3GPP TR 33.816 V10.0.0 (2011-03)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Feasibility study on LTE relay node security
Release 10

Keywords

Security, LTE, Relay, authentication

3GPP

Postal address

3GPP support office address

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

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Report 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

The present document provides an analysis of the security issues by including Relay Nodes (RN) into the LTE network. Furthermore it contains several solutions to provide security for the relay architecture chosen by the RAN groups. It also provides a comparison between those solution and the reasoning why a particular solution was chosen.

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 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

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

[4] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[5] NIST Special Publication 800-56B: " Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography", August 2009.

[6] RFC 5296 The Transport Layer Security (TLS) Protocol Version 1.2

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

[8] 3GPP TS 33.110: "Key establishment between a UICC and a terminal".

[9] 3GPP TS 31.116: "Remote APDU Structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications".

[10] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[11] 3GPP TS 33.220: Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[12] ETSI TS 102 484: "Secure channel between a UICC and an end-point terminal".

[13] RFC 4366 Transport Layer Security (TLS) Extensions

[14] 3GPP TS 33.102: "3G Security; Security architecture".

[15] 3GPP TS 31.101: "UICC-terminal interface; Physical and logical characteristics".

[16] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[17] RFC 2560: "Online Certificate Status Protocol - OCSP".

[18] RFC 5705 Keying Material Exporters for Transport Layer Security (TLS)

[19]	RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

3 Definitions, symbols 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].

RN subscription authentication: This form of authentication is performed between the RN in its role as a UE and the MME-RN. It is performed using the EPS AKA protocol as defined in TS 33.401 [2] and involves a USIM on a UICC inserted in the RN.

RN platform authentication: This form of authentication is performed between a secure environment in the RN platform and a network entity. For the purpose of this definition, the RN platform encompasses both the ME functionality of the RN and the eNB functionality of the RN. As a result of this authentication the network entity (e.g. Donor eNB, HSS or MME-RN) has verified that the secure environment in the RN is in possession of a secret key associated with the RN. RN platform authentication is intended to additionally provide implicit proof of the integrity of the RN platform to the network entity. This is achieved by assuming that the secure environment in the RN engages in RN platform authentication only after a successful autonomous RN platform validation has been performed by the secure environment.

Editor's Note: The definition of the term "platform validation" may need further refinement.

RN-UICC secure channel authentication: This is any authentication performed as part of the set up of a secure channel between an RN and a UICC, for example according to ETSI TS 102 484 "Smart cards; Secure channel between a UICC and an end-point terminal" where the "end-point terminal" is the RN. The RN-UICC secure channel terminates in the RN secure environment.

NOTE 1: Although RN-UICC secure channel authentication also presupposes a secure environment in the RN platform we deliberately distinguish it terminologically from the authentication of the RN platform to the network to make it easier to discuss these forms of authentication separately.

RN management authentication: This form of authentication is performed between a secure environment in the RN platform and a network management entity. For the purpose of this definition, the RN platform encompasses the RN management functionality of the RN. As a result of this authentication a network management entity has verified that the secure environment in the RN is in possession of a secret key associated with the RN. RN management authentication is intended to additionally provide implicit proof of the integrity of the RN platform's management capability to a network management entity. This is achieved by assuming that a secure environment in the RN engages in RN management authentication only after a successful autonomous RN validation of the management capabilities has been performed by the secure environment.

NOTE 2: We deliberately distinguish RN management authentication terminologically from RN platform authentication to make it easier to discuss configuration and remediation capabilities separately.

RN authentication: This term is an umbrella term for the above forms of RN authentication.

NOTE 3: In many cases, it may be necessary to say explicitly which form of RN authentication is meant, so this term should be used with restraint.

Platform Secure Environment: This follows the definition and requirements as specified in 5.3.5 of TS33.401 [2].

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].

DeNB	Donor eNB

MME-RN	MME serving the RN
MME-UE	MME serving the UE
RN	Relay Node
P-GW-RN	P-GW serving the RN
S-GW-RN	S-GW serving the RN

4 Relay Architecture

This clause aims to provide some brief details of this architecture chosen for relays as background to the rest of the analysis in this document. A more complete description of architecture is covered in TR36.300 [4].

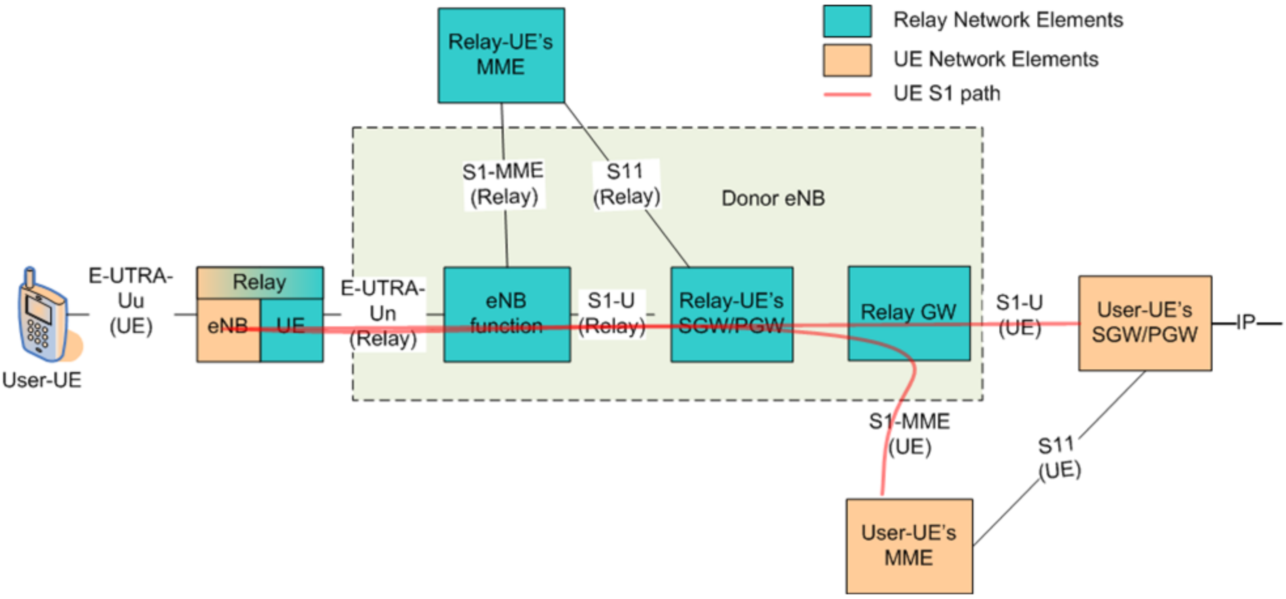


Figure 4-1: Relay Architecture

The DeNB contains the S-GW/P-GW functionality for the RN in addition to the radio aspects. It may also contain some Relay GW functionality.

The user plane is moved from GTP tunnel to another one at the DeNB. This is illustrated in figure 4-2.

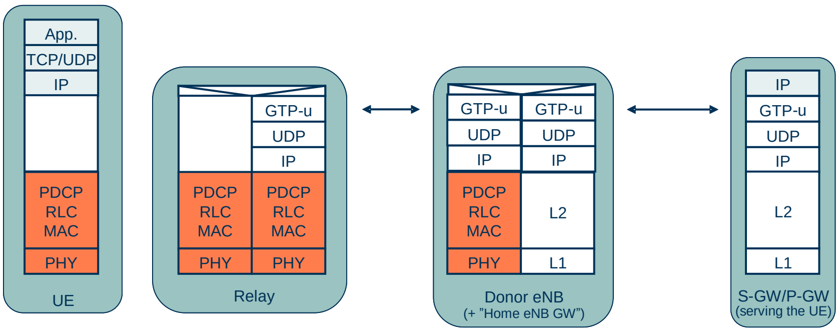


Figure 4-2: User plane protocol stack

Similarly the DeNB does not pass the S1-AP signalling traffic directly between the MME-UE and the RN. The DeNB acts as a proxy between the RN and MME-UEand changes the S1-AP UE IDs in the messages but leaves the other part of the message the same. This is illustrated in figure 4-3.

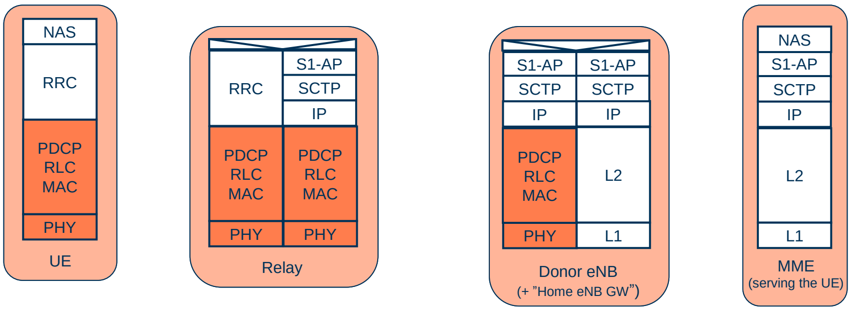


Figure 4-3: Control plane protocol stack

RAN2/3 have agreed a two phase start-up procedure for RNs. This is illustrated in figure 4-4.

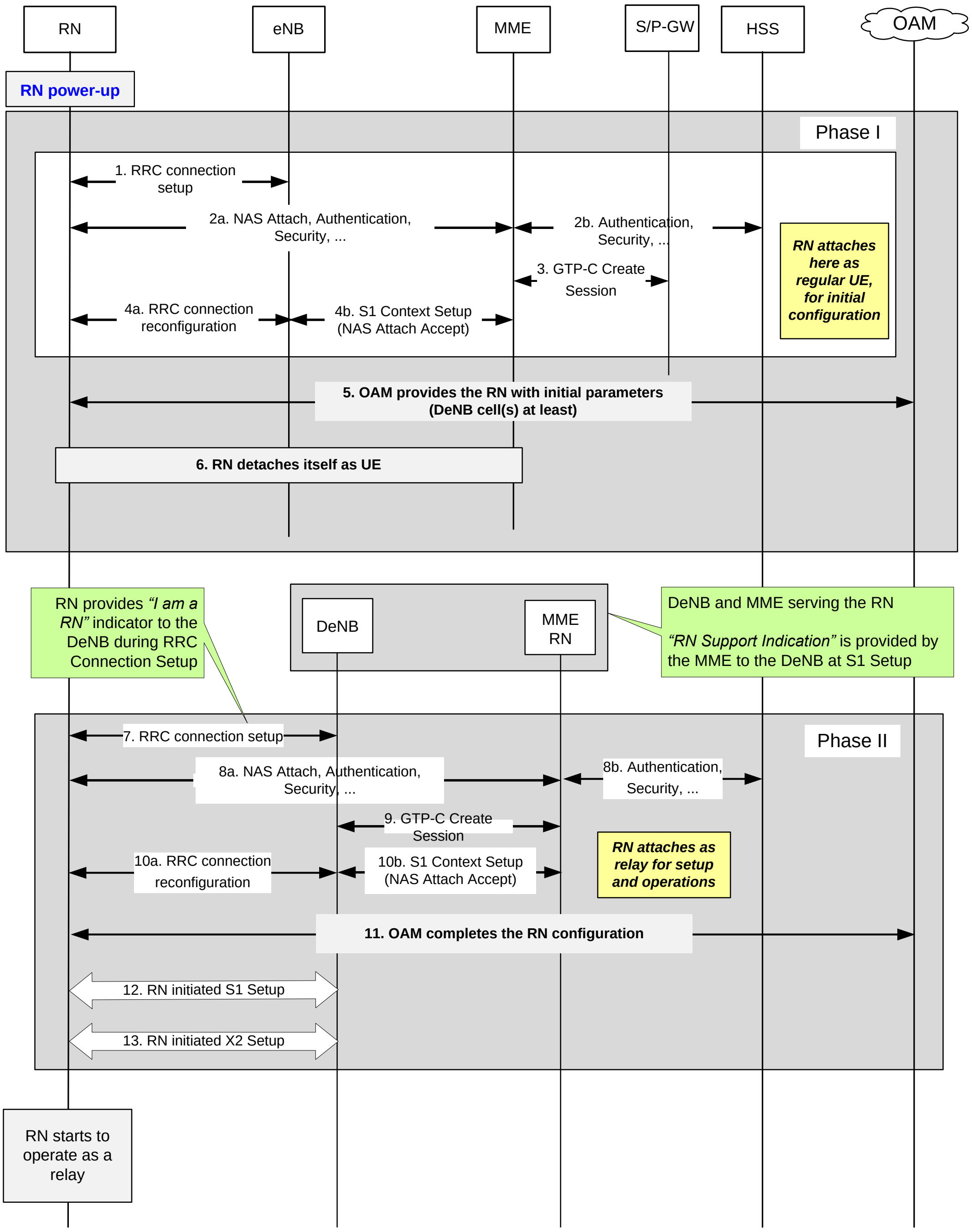

RN
eNB
MME
S/P-GW
HSS
OAM
RN power-up
Phase I
1. RRC connection setup
2a. NAS Attach, Authentication, Security, ...
2b. Authentication, Security, ...
3. GTP-C Create Session
4a. RRC connection reconfiguration
4b. S1 Context Setup (NAS Attach Accept)
RN attaches here as regular UE, for initial configuration
5. OAM provides the RN with initial parameters (DeNB cell(s) at least)
6. RN detaches itself as UE
RN provides "I am a RN" indicator to the DeNB during RRC Connection Setup
DeNB
MME RN
DeNB and MME serving the RN
"RN Support Indication" is provided by the MME to the DeNB at S1 Setup
Phase II
7. RRC connection setup
8a. NAS Attach, Authentication, Security, ...
8b. Authentication, Security, ...
9. GTP-C Create Session
10a. RRC connection reconfiguration
10b. S1 Context Setup (NAS Attach Accept)
RN attaches as relay for setup and operations
11. OAM completes the RN configuration
12. RN initiated S1 Setup
13. RN initiated X2 Setup
RN starts to operate as a relay

Figure 4-4: Two phase start-up procedure

5 Threats

5.1 General

Threats can be considered at several stages of the development of a security architecture. General threats apply when no security mechanisms are in place yet; residual threats still apply with certain security mechanisms already in place. General threats are handled in this clause; residual threats are addressed in clause 8 on security procedures.

5.2 Assumptions for threat analysis

As the relay architecture is based on the already existing LTE architecture, the following assumptions are made when analysing the security threats to the relay architecture:

- A removable UICC is inserted into the RN to provide authentication between itself and the network to establish the bearer(s).

Editor's note: if the UICC is not removeable, the applicability of threats is FFS. The acceptability of non-removeable UICC is FFS.

- AS level encryption is switched on between the RN and DeNB.
- The DeNB will have some secure environment that is assumed that an attacker will not compromise
- Everything from the DeNB upwards (towards the network) is secure and will use macro network security mechanisms (such as NDS/IP).

These assumptions are made purely for the purposes of understanding the security threats and any solution is not restricted to follow these assumptions.

5.3 Security threats

Despite the security assumptions made in the previous section, the introduction of a RN into the network introduces some new security threats to E-UTRAN, namely:

- Impersonation of a RN to attack the user(s) attached to the RN
- Attacks on the Un interface between RN and DeNB
- Inserting a MitM
- Attacking the traffic
- Impersonation of a RN to attack the network
- Attacks on the interface between the RN and UICC
- Attacks on the RN itself
- DoS Attacks
- RN stays as UE after initial attach
- Attacks on NAS signalling and AS traffic

1 Impersonation of a RN to attack user attached to RN

To perform the attack, the attacker removes the UICC from a real RN and inserts it into their own Rogue RN as shown in the below figure. As there is no authentication of the RN as a device (only the subscription that is inserted in the RN), the network can not detect the Rogue RN, and hence keys related to the user-UE will be passed to the Rogue RN. This enables a user to attach to the Rogue RN and hence the user's security will be compromised. This shows that it is essential to perform some type of device authentication of the RN.

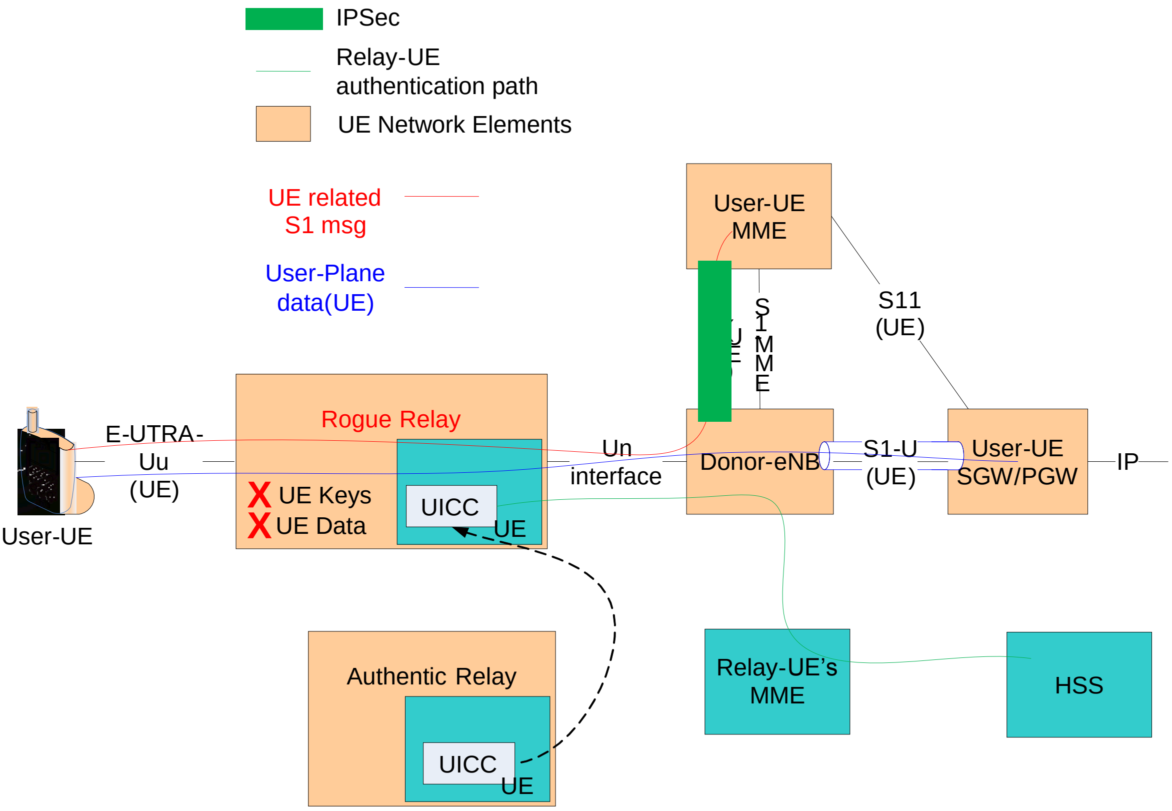


Figure 5-1: Impersonation of a RN to attack user attached to RN

2 MitM on the Un interface between RN and DeNB

This can be considered to be a variant of the above attack, but it is essential to consider as it illustrates that some care must be taken on the method of authenticating the RN device. In this attack, an MitM Node is inserted in between the RN and DeNB. This MitM node is created by taking a real UICC from a real RN and replacing it with a fake UICC for which the attacker has the root key. It also requires inserting the real UICC into the MitM node. This is illustrated in the below figure.

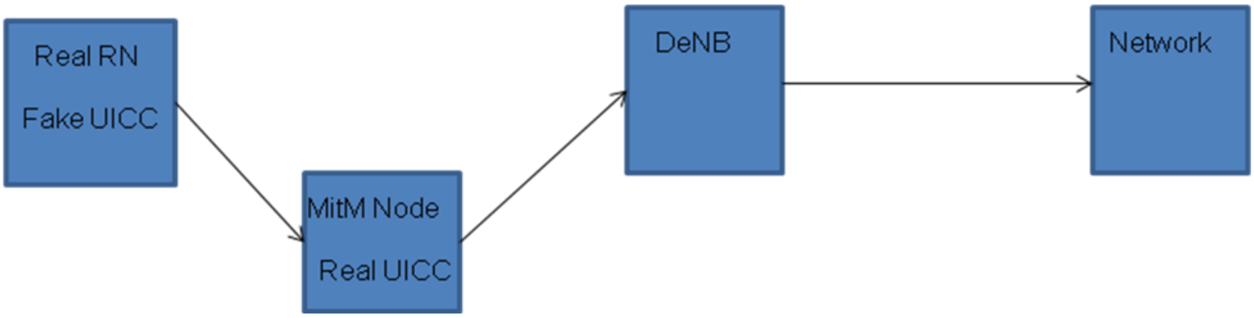


Figure 5-2: Man-in-the-Middle (MitM) Node

The real RN will connect to the MitM node and the MitM node can connect to the real DeNB. The MitM node can transparently transmit, receive, view, and modify the traffic between the real RN and the DeNB without either of those nodes being aware of it. Hence the security of any user connected to the real RN is compromised. The MitM can eavesdrop on, modify, and inject user traffic even if the user related keys are protected by IPsec between the MME-UE and the RN. The important security point illustrated by this attack is that not only is it essential to perform device authentication of the RN, it is important to ensure that all security tunnels from the RN terminate in the real network instead of in a MitM node.

Editor's Note: Whether the attack described above is feasible to launch is FFS.

3 Attacking the traffic on the Un interface between RN and DeNB

The interface between the RN and DeNB is based on the standard E-UTRAN air interface. This provides optional confidentiality for all traffic between the EN and DeNB, but all the non-RRC signalling traffic between the RN and DeNB is not integrity protected. The confidentilaity protection could be used to encrypt the traffic on this interface, but if this security is not available for RN's node, then some other method of providing confidentiality will be needed.

If there is no integrity protection for the interface between RN and DeNB, an attacker could modify the traffic over this interface.

For user UE traffic, this would be the content as well as the protocol headers of the communication. By changing GTP protocol headers of user traffic over Un, it could be possible to redirect traffic bound for one (victim) UE to another (attacker) UE. This attacker UE would receive the data encrypted with its own UPenc key. In uplink, this may allow IP address spoofing.

Editor's Note: The impact of this threat is FFS.

For signalling traffic, this is S1-AP traffic and X2-AP traffic.

While this may be accepteable for user traffic from the UE, this may not be acceptable for signalling traffic (either S1-AP or X2-AP) from RN to network. This means that either the Un interface may to enhanced from a standard E-UTRAN UE-eNB interface or some other method of protecting the S1-AP and X2-AP signalling across the Un interface needs to be used.

4 Impersonation of a RN to attack the network

A Rogue RN (as described in Threat 1) could insert essentially four types of traffic into the network:

a NAS signalling towards the MME-RN – the same attacks could be done with a Rogue UE so are not important for the RN security analysis

b S1-AP or X2-AP signalling

c Insert data on behalf of a user

d User plane traffic to get free IP connectivity

This threats could be mitigated by ensuring RN platform authentication of the RN before such traffic is accepted or being aware of such threats and mitigating them in other ways.

Before RN platform authentication has taken place the network cannot distinguish between a RN and a rouge RN. Hence, there is still a risk for similar attacks.

5 Attacks on the interface between the RN and the UICC

The data that travels across the RN to UICC interface is not protected. This means that while an attacker may not be able to compromise the behaviour of a RN, it may be possible for the attacker to get hold of the keying material that is transferred across this interface. Access to these keys would provide the attacker with access any data protected by these keys and also allow the attacker to insert data that would be protected using these keys. In particular the attacker could set up a MitM node as described in threat 2.

6 Control of the RN platform

All traffic, apart from NAS-UE signalling between UE and MME-UE, is available inside the RN platform in the clear. So, when an attacker controls the RN platform eavesdropping and modification of this traffic is possible.

7 DoS type attacks

When the attacker removes the UICC, RN without UICC can't be authenticated by the network. So the legal RN can't connect to network and provide services. The attacker could also insert the UICC into another RN, then the topology of access network will be changed and cause interference problem to other eNB.

8 RN stays as UE after initial attach

In this attack, a false RN stays as UE even after RN subscription authentication by not performing detach and also not initiating the S1 interface setup procedure. As a result, the network can not authenticate the RN as an eNB and the RN acts as UE to receive or request services in the network. This will lead to free charging problem even when the network knows the attached user is an RN.

9 Attacks on NAS signalling and AS traffic

In this attack an attacker intercepts/modifies/injects messages on the UICC RN interface. In Phase 1 and possibly part of Phase II signalling NAS and AS traffic will be protected with keys that can be derived from information intercepted on the UICC RN interface. It is noted that the attack cannot be stopped, assuming that the RN should be able to attach as UE using legacy eNB and MME in Phase 1.

NOTE: This threat implies that all services in Phase I need to be protected on application level. Currently enrolment of certificates and connections to OAM are specified.

The effects of attacks on NAS signalling has to be evaluated and possible restrictions prescribed, see clause 8.10.

6 Requirements

6.1 General Requirements

The AKA credentials shall be stored on a removable UICC.

Editor's note: The requirements on extending sessions and starting or continuing emergency calls outside normal RN operating conditions, e.g. when the UICC is removed, are FFS.

6.2 Security Requirements

If end to end protection between the RN and the core network is needed, then the same solution as for backhaul protection should be considered.

Integrity protection and confidentiality protection for the S1 control plane traffic shall be mandatory. The S1 control plane traffic between RN and MME-UE shall be integrity protected between the DeNB and the MME-UE with the same strength as in the current EPS architecture. Only hop by hop protection between RN and MME-UE shall be considered as the DeNB acts as an S1-proxy in the solution selected by RAN. The S1 control plane traffic between DeNB and MME-RN shall be integrity protected with the same strength as in the current EPS architecture.

NOTE: If NULL encryption algorithm is used, it is essentially the same as providing no confidentiality protection to the S1 control plane traffic.

Editor's note: The need for confidentiality and replay protection of the S1 control plane traffic between DeNB and MME-RN are FFS.

Integrity protection for the X2 control plane traffic over the Un shall be mandatory. The X2 control plane traffic between RN and eNB/RN shall be integrity protected between the DeNB and the eNB/RN with at least the same strength as in the current EPS architecture. Only hop by hop protection between RN and eNB/RN shall be considered as the DeNB acts as an X2-proxy in the solution selected by RAN.

Integrity protection for the S11 control plane traffic between DeNB and MME-RN shall be mandatory.

Editor's note: The need for confidentiality and replay protection between DeNB and MME-RN are FFS.

Mutual authentication between RN and network shall be supported.

Relay node platform authentication is mandatory.

Editor's note: There are many different solutions for meeting this requirement.

The certificates used for the relay node platform authentication shall be validated.

Certificates used for the relay node management authentication shall be validated.

The DeNB shall not accept or send S1-AP and X2-AP message from/to the RN until a successful relay node platform authentication has happened.

A certificate in the relay node used for platform authentication shall be provided by a CA trusted by the operator, e.g. the CA of the operator or by another party trusted by the operator. Certificate enrolment, if any, should follow TS 33.310 [7] as much as possible.

The wireless resource: security shall be able to prevent misuse by identifying whether the attached terminal is a UE or a RN. The identification could be implicit.

The connection between relay and network should be confidentiality protected. Confidential protection for the S1/X2 user plane traffic over the Un should provide protection as same as the user plane data transferred on Uu interface, i.e. provide optional confidentiality protection on Un interface.

Editor's Note: It remains to be seen whether the previous sentence can be aligned with the integrity protection requirements.

Both user plane and control plane must be considered as they may not require the same level of protection.

Editor's note: Forward security and backward security in handover procedure needs further study.

Editor's note: For AS security aspects of Un interface, the key lifetime management should be considered based on existing LTE UE AS key time management for the Uu interface. It should be studied whether the impact of UE data aggregation on the Un interface requires more frequent key change due to the increased traffic. The Security Association life time management for the IPsec tunnel should be considered. And all aspects of interaction between the key lifetime management and the respective security mechanism to be specified should be considered. The aspect of minimizing the effect to the ongoing service for the UE attached to the Relay-Node should be considered.

The RN platform shall protect from reading and/or modification of security parameters and security functions by unauthorized parties (platform security).

The integrity of the RN platform shall be validated as part of the RN start up procedure.

RN specific device security features, e.g. security storage of sensitive data, device integrity check, UICC aspects, shall be considered.

Editor's Note: Platform security requirements should be considered in more detail.

Editor's Note:It is FFS if the security of the DeNB needs to be greater than a macro eNB.

6.3 Requirements on enrolment and RN start-up procedure

6.3.1 General

The parts of the requirements relating to certificate based IKEv2 and IPsec are of course only applicable for the solutions where these protocols are used.

6.3.2 Enrolment

Requirement 1: Before step 12 in Phase II it is necessary that the RN is able to contact its certificate enrolment server.

Rationale: In step 12 of Phase II, the RN establishes S1-MME connections which are proxied by the DeNB. Since keys for real UEs are passed over the S1-MME interface, the DeNB must be ensured that the RN platform is properly authenticated. Since RN platform authentication is based on certificates requirement 1 follows.

6.3.3 Start of IPsec

Requirement 2: Between steps 10 and 12 in Phase II, solutions based on IPsec to protect the S1/X2 reference points must have run IKEv2 to establish SAs and started to protect the IP traffic over Un.

Rationale: If IPsec is not enabled between steps 10 and 12, the UE keys sent over Un will be unprotected. Depending on what data the RN needs to collect from the O&M system, IPsec may be enabled before the communication with O&M or after.

6.4 Access restrictions for the RN

Requirement 3: During Phase I, the RN shall only be allowed IP access for specific purposes, for example to enable download of configuration data, and to access certificate validation servers and certificate enrolment servers. All other access (including general Internet access) shall be denied.

Rationale: Principle of least privileges. If the RN is able to access Internet it could be used for general free internet access if broken into.

Editor's Note: Potentially, enrolment servers could be accessed via other networks, e.g., the Internet, and in this case Requirement 3 must be modified so that the RN is allowed access to the O&M network and the Internet. This needs to be discussed by SA3.

Requirement 4: During Phase II, the RN shall only be allowed IP access for specific purposes, for example to enable download of configuration data, and to access certificate validation servers and certificate enrolment servers. For IPsec based solutions, the RN shall also be allowed to run IKEv2 and IPsec to/from the DeNB. All other access (including general Internet access) shall be denied.

Rationale: Principle of least privileges. If the RN is able to access Internet it could be used for general free internet access if broken into.

Comment: The requirement 3 for Phase I is almost the same. The only difference is that for Phase II the RN is required to run IKEv2/IPsec, so this must be allowed for some of the proposed solutions.

6.5 RN Management

Editor’s Note: RN configuration may need to be download from corresponding mangement entity, this procedures should be secure.

Security of RN Management shall be guaranteed. RN should have separate security model for OAM configuration data.

Communication between RN and OAM system shall be protected by end-to-end model, for example, TLS.

The OAM system and the RN shall be able to mutually authenticate each other.

The ability of the OAM to configure a RN shall not depend on the ability of the RN to perform RN Platform Authentication.

The OAM system should be able to (re)configure the RN remotely. Under certain fault conditions the re-configuration will fail (e.g. if the RN is not capable of connecting to the OAM system).

The capabilities of the RN to perform OAM procedures needed for trustworthy operation shall be assured by the RN platform secure environment.

7 Security Architecture

7.1 Security protection type for relay node on User UE’s S1 interface and X2 interface

7.1.1 Analysis

In the architecture which is selected by RAN2/RAN3, there are 2 kinds of GTP tunnels exists: the tunnel between RN and DeNB and the tunnel between DeNB and core network. DeNB should decompress the message from one tunnel and switch them to the other. So if the data is encrypted, DeNB needs to decrypt the data first.

When User UE’s signaling or user data transferred to relay node, there are 2 kinds of protections between relay node and core network entities for S1 interface and X2 interface: end to end protection and hop by hop protection

- When E2E protection is used to protect UE's message between relay node and MME-UE/SGW-UE in S1 interface, or between relay node and another eNB during User UE's handover, User UE's messages are transferred directly from relay node to MME-UE/SGW-UE which are transparent to the DeNB. So DeNB cannot compose the messages in this assumption.
- When H2H protection is used to protect UE's message between relay node and MME-UE/SGW-UE, or between relay node and another eNB during User UE's handover. The protection will be applied into 2 hops separately. One hop is between relay node and DeNB, and the other is between DeNB and network entities(MME-UE/SGW-UE or another eNB). Under this assumption, DeNB should decrypt data from one link then switch the plain data to another link. So DeNB can compose message in this case.

So hop by hop protection is proper to be used in relay's alternative 2 architecture.

7.1.2 Security protection architecture

Then, based on the analysis above, when the protection is applied to relay node and network entities, hop by hop protection model shall be used in the relay architecture

7.2 Security protection type for relay node about OAM communication

7.2.1 Analysis

If we want to reuse this hop-by-hop protection mechanism described in section 4.1.2 on the communication between RN and OAM system, there is a security issue that exists for the communication.

In RN's alternative 2 architecture, DeNB acts as a proxy and can get all communication data between RN and OAM. When OAM sends software or configuration data like configuration parameters to the RN, DeNB will get these parameters because it will switch them from the link between OAM and DeNB to the link between RN and DeNB.

If the RN and DeNB are provided by different vendors, one vendor's privacy about RN's configuration data and preference will be possible known by another vendor who made this DeNB.

This risk is raised because DeNB will get the communication data between RN and OAM. So the simplest solution for this problem is to provide an end-to-end confidentiality protection between RN and OAM. As there are IPsec tunnels that exist between RN and DeNB, TLS tunnel should be used for protecting the communication between RN and OAM system. For this, the RN and the RN OAM system should be able to authenticate each other.

If TLS is used to protect OAM traffic, a TLS tunnel should be used between RN and OAM server to secure step 5 in Phase 1 and step 11 in Phase 2 of figure 4-4.

The ability of the OAM to configure a RN should not depend on the ability of the RN to authenticate as device.

Furthermore, there may be cases where the RN is in certain fault conditions (e.g. if the RN fails device authentication a number of times consecutively, etc) and needs to be reconfigured remotely. Therefore, the RN OAM should be able to at least attempt to (re)configure the RN under these fault conditions.

7.2.2 Security protection architecture

Based on the analysis above, End-to-end protection model shall be used in the relay architecture for OAM communication.

8 Security Procedures

8.1 Analysis of Un interface security

Editor's Note: General: Multi-hop relaying and mobile relays were not considered in the comments. They may require additional considerations.

8.1.1 General aspect on Un security for Relay architecture

Relaying functionalities shall support the TNL of S1-MME and S1-U interface, and hence a function to ensure the secure transport over the Un interface needs to be defined. Since it is considered that a RN can be seen both as a UE and as an eNB in the network, for Un interface, AS security provided by PDCP [2], or network domain security provided by NDS/IP [7] or their combination could be applied. In the typical network deployment, the SEG within the operator network is implemented as standalone node in order to gain the concentration effect. In this document SEG to secure DeNB and the EPC node is named 'native SEG'.

Editor's Note: It is assumed that the native SEG is the one that would be present anyhow according to the current EPS security architecture in TS 33.401 [2] when the DeNB would not serve any RN.

Therefore, based on the abovementioned RN roles, the security over the Un interface is ensured by AS security and/or NDS/IP, respectively in the different layer illustrated in Figure 8.1.1-1.

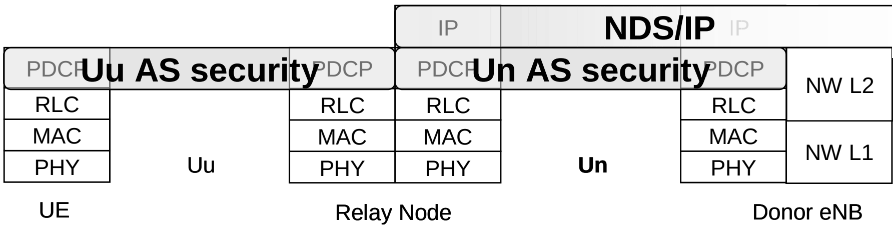
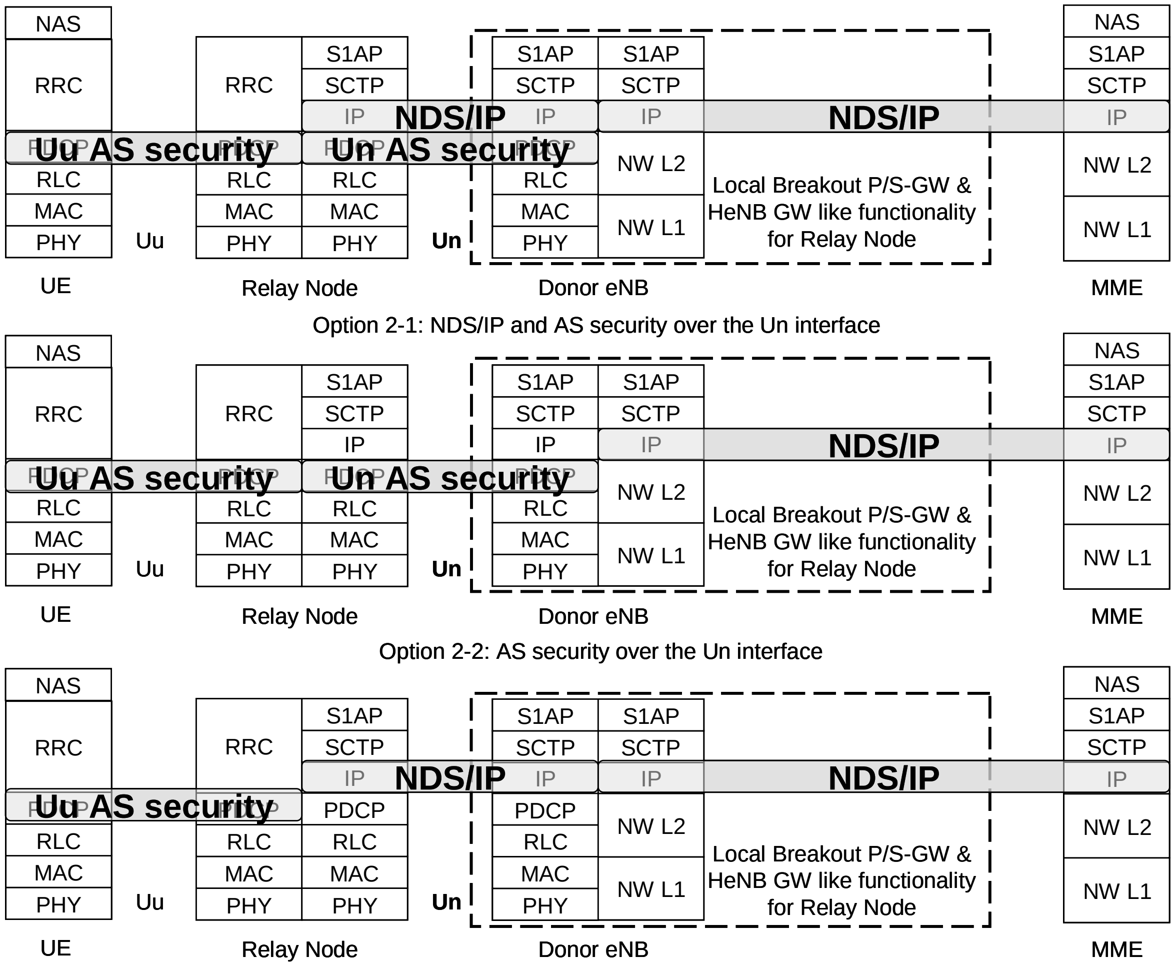


Figure 8.1.1-1: General aspect on Un security

8.1.2 Analysis of options for Un interface security

Figure 8.1.2-1 shows possible options on the Un interface security in the architectural alternative selected by RAN. In this alternative, the native SEG is responsible for the secure transport between the DeNB and the MME.



Option 2-1: NDS/IP and AS security over the Un interface

Option 2-2: AS security over the Un interface

Option 2-3: NDS/IP over the Un interface

Figure 8.1.2-1: Un interface security options

8.1.2.1 Option 1: NDS/IP and AS security over the Un interface

8.1.2.1.1 General

Editor's Note: It needs to be clarified whether all traffic over the Un user plane, or only S1 signalling traffic, is to be protected by NDS/IP, e.g. for performance reasons. If the latter applies then appropriate mapping of parameters identifying S1 signalling traffic to IPsec selectors (IP addresses, ports, transport protocol) would have to be performed.

Editor's Note: The enrolment process for credentials to set up backhaul link security between RN and MME-RN, and RN and S-/P-GW-RN (i.e. distribution of IPsec certificates and set up of IPsec tunnel) needs to be studied.

In this option, Un PDCP provides AS security for upper layers. In addition, IP transport provides TNL security between the RN and the DeNB, and the DeNB and the MME utilizing NDS/IP.

Although the native SEG can be reused for NDS/IP traffic between the DeNB and the MME, another SEG is needed to process the IPsec between the RN and the DeNB.

8.1.2.1.2 Residual Threats for Option 1

8.1.2.1.2.1 NDS/IP for all user plane traffic on Un

Assumption: AS security is established between RN and DeNB as part of the RN attachment involving the UICC-RN and the MME-RN. As soon as the Data Radio Bearers (DRBs – Un user plane) have been established, one or several IP security associations are established between RN and DeNB. As part of this process, the integrity of the RN platform is validated by the network. **All** traffic over DRBs is protected by IPsec.

Analysis: IPsec for all user plane traffic, the most benefit is it can provide integrity protection for UE's user data in Un interface as it can be seen as backhaul link for UE. On the other hand, the disadvantage comes from the integrity protection on UE's user data. It will cause low efficiency on Un traffic. Further more, because the integrity protection of user data on radio bearer is not needed, so the integrity protection for UE's user data traffice in Un interface is not necessary.

Residual Threat: threats of eavesdropping on and modification of traffic of DRBs is satisfactorily addressed by platform integrity and use of IPsec. As RRC traffic cannot be protected by IPsec it needs to be considered separately. The main threat to RRC seems to be that an attacker modifies bearers on Un. This seems to be possible when an attacker knows the RRC integrity key.

Editor's Note: threats to AS security for RRC over Un need further study. In particular: how can an attacker obtain knowledge of the RRC integrity key?

The AS security provided to DRBs does not harm, but does not seem to provide an additional advantage either.

8.1.2.1.2.2 NDS/IP for part of the user plane traffic on Un

Assumption: same as for 5.1.2.1.2.1 except that **not all, but only S1-UE**, traffic over DRBs is protected by IPsec.

Analysis: IPsec only for S1-UE signalling in Un user plane traffic, the most advantage is to limit IPsec impact on radio perform in an negligible degree. Although this alternative can't provide IPsec confidential protection for UE's user plane traffic, the traffic can be confidential protected in PDCP layer

Residual Threat: neither RRC nor UP-UE traffic are protected by IPsec. (UP-UE = user plane data sent by UE.) In addition to the remarks made on RRC in 8.1.2.1.2.1, the attacker could eavesdrop on UP-UE. An attacker could e.g. fraudulently establish an RN-DeNB radio connection via a MitM as described for threat 2 in clause 5.

Depending on the way in which the attacker obtains knowledge of the keys it may not be enough to ascertain that the IPsec SAs and AS security have the same endpoints, i.e. that all security tunnels from the RN terminate in the real network instead of in a MitM node may not be sufficient. It may neither be sufficient to bind the USIM to the RN, e.g. by using EAP-AKA inside IKEv2 in the way done for HeNBs.

Editor's Note: threats to AS security for RRC and UP-UE over Un need further study.

8.1.2.1.2.3 Conclusion of option 1

Conclusions: In radio bearer, the performance is very important and shall be considered when a security mechanism will be applied to. So based on the analysis above, it is proposed to take the working assumption to apply NDS/IP for part of the user plane in the Un and rule out alternative 1 of option 1

8.1.2.2 Option 2: AS security over the Un interface

8.1.2.2.1 General

The main issue with this approach is that S1 signalling packets are delivered over the Un user plane, which does not provide integrity protection. But integrity protection for S1 signalling is mandatory, so Option 2 must be ruled out unless Un security is modified such that integrity protection is provided in the Un user plane at least for PDCP PDUs carrying S1 signalling. This may, however, run counter to the intention to re-use the Uu protocol for Un.

An issue with this alternative is that it may require strong assurance of a binding of USIM and RN. Current eNBs do not provide this binding feature while they do currently allow to anchor IPsec credentials in the secure part of the eNB platform, thus providing a secure anchor for NDS/IP.

In this option, link by link security is provided by Un PDCP between the RN and the DeNB, and NDS/IP between the DeNB and the MME.

The native SEG can be reused for NDS/IP traffic between the DeNB and the MME.

8.1.2.2.2 Residual Threats for Option 2

Assumption: all traffic over Un is protected only by AS security.

Residual Threat: as already noted in 8.1.1, integrity protection of S1-UE is required, but can be only guaranteed if the AS security mechanisms on Un are modified with respect to Uu as Uu does not provide integrity on DRBs. Furthermore, all threats that apply to RRC and UP-UE in case 8.1.2.2.2 now apply to all traffic over Un.

Editor's Note: threats to AS security for all traffic over Un need further study. Integrity protection for S1-UE traffic needs further study.

8.1.2.3 Option 3: NDS/IP over the Un interface

8.1.2.3.1 General

At least RRC traffic needs to be protected by AS level security and cannot be protected by NDS/IP. If a part of the traffic on the Un interface is to be protected by AS security, then RAN3 should be aware that the same algorithms must be chosen both for DRB and SRBs based on the current AS security mode procedure. In particular, if you have non-NULL ciphering on RRC then you cannot switch off ciphering in the user plane at the same time, cf. 33.401 [2], 7.2.4.2.1. This could imply that you would need a relay-specific AS Security Mode Command procedure for Un.

In this option, the secure IP transport is provided by NDS/IP between the RN and the DeNB, and the DeNB and the MME.

Additionally, secure IP transport would have to be provided for UE user packets between the DeNB and the S-/P-GW (UE). The DeNB could use the different destination IP addresses as selectors in this case.

Therefore, the secure transport over the Un interface relies on upper layer function (NDS/IP), since Un PDCP does not provide AS security for upper layers.

This would imply that the outer IP headers would not be protected.

Editor's Note: While this requires some further study, we have so far not identified a problem with this.

For the same reason as option 1, the native SEG and another SEG are needed.

Editor's Note: The enrolment process for credentials to set up backhaul link security between RN and MME-RN, and RN and S-/P-GW-RN (i.e. distribution of IPsec certificates and set up of IPsec tunnel) needs to be studied.

8.1.2.3.2 Residual Threats for Option 3

Assumption: all user plane traffic over Un is protected only by NDS/IP security.

Residual Threat: as already noted in 8.1.1 AS security is needed at least for RRC. In order to be able to switch off AS security for DRBs, while still maintain confidentiality for RRC, a modification of Un with respect to Uu would be needed. Apart from this, the same considerations as for 8.1.2.1 apply.

Editor's Note: threats to AS security for RRC over Un need further study.

8.1.3 Comparison of Options

For radio network performance impact, using NDS/IP on all Un user plane data is low efficiency, and for this reason, Option 2 may be better. If only S1 signalling traffic applies NDS protection, the performance degradation of option 1 is insignificant.

If NDS/IP is not adopted at all, the Un security has to be modified to provide integrity protection in the Un user plane at least for the PDCP PDUs including S1 signalling, which may bring changes to Un PDCP protocol. This method has the following advantages:

- For device authentication methods that enable the choice between enhanced AS security and IPsec for integrity protection of S1 signalling over Un, the AS security setup does not involve extra round trips beyond the ones needed for existing Attach, compared with IPSec which needs its own handshakes in addition to the radio level attach.

- AS security could make a transition to mobile RNs simpler as it could be automatically established at handovers, although this is not a major consideration at this point.
- Less overhead than IPsec method

With regard to option 3, NDS/IP protection will not only bring more overhead, but also cause too much complexity for the PDCP header compression (i.e. ROHC) Also, if a part of the traffic on the Un interface is to be protected by AS security, the impact to the current AS security mechanism will be quite large.

So option 3 will bring more impact to the LTE system compare to other options. The reason is as below. Firstly, comparing with option 1, option 3 will not only bring IPsec overhead similar to option 1, but also requires changes to the current RRC protocol(SMC) that makes it possible to enable ciphering of the control plane only (leaving the user plane NULL ciphering). Note, LTE currently requires that the same ciphering algorithm is used for control plane and for user plane. Secondly, option 3 requires DeNB to identify which security scheme to use by this different AS security because RN and normal UE needs different negotiation functions. Then it needs to bring security negotiation command on the specific security scheme. Thirdly, compared with option 2, even though they also needs to impact the protocol, option 2 has no IPSec overhead problem. What is more, applying IPsec to ALL traffic is generating significant overhead.

Based on the analysis and comparison above, option 3 is not recommended and shall be ruled out. .

8.2 Security for the RN NAS traffic

The security for the NAS traffic between the RN and the MME-RN shall be established and maintained as for any UE accessing LTE. built in security of the NAS layer shall provide ciphering and integrity protection for the NAS traffic.

8.3 Security for the RN RRC traffic

The security for the RRC traffic between the RN and the DeNB over Un may be established and maintained as for any RRC connection over Uu.

8.4 Mutual Authentication

Editor’s Note: Mutual authentication between RN and network should be considered.

8.5 Enrolment procedures for RNs

Assuming that a USIM is available in the RN, this USIM can be used to authenticate the RN to the MME and the RN can be granted IP connectivity via a DeNB, any other eNB, or a fixed network access, e.g. at the operator’s premises. If the access provided by the DeNB is a general purpose access, it could potentially be used to get service from the network which could be misused. Therefore the MME should inform the DeNB that this RN is a only allowed restricted access. That is, the RN is only allowed to communicate with a server in the O&M network. Access restrictions could potentially also be enforced in the S-GW or PDN-GW.

Once IP connectivity to the enrolment server is established, the same procedure used for macro eNBs can be used to enrol an operator certificate in the RN. The RN has been provisioned with a vendor certificate and corresponding private key in the factory, and uses the procedures defined in TS 33.310 [7] to enrol the operator certificate. This gives the benefit that the certificate handling can be exactly the same as for macro eNBs and no additional procedures needs to be specified and implemented/tested.

There are two issues that need to be addressed for the above setup to work: how to ensure that the RN is only allowed to access the O&M network before it is enrolled and how to make the USIM available in the RN.

The first issue can for instance be solved by checking if the DeNB can or cannot establish the required IPsec tunnel to the RN (assuming an IPsec tunnel is used to provide integrity protection for the S1/X2 signalling). When the DeNB notices that a tunnel cannot be established, it only gives the RN IP connectivity to the server in the O&M network. Other possibilities may exist. The problem is solvable. It is noted that the MME does not have access to any information regarding if the RN has enrolled an operator certificate or not and hence cannot provide this information to the DeNB in the S1 setup for the RN (unless additional certificate based authentication is added to the NAS signalling).

The second issue regarding how a USIM can be made available to the RN is more complex. There are several possibilities:

1. The USIM credentials are hard coded in the RN's secure environment in the factory.
2. The USIM is physically made part of the secure environment in the factory, e.g., soldered in place and the connection between the USIM and the secure environment is physically protected from access..
3. The USIM is inserted by a field engineer and is physically made part of the secure environment. A mechanical/gluing solution would be required to guarantee that the USIM integration into the secure environment.
4. The USIM is inserted by a field engineer when the RN is deployed and is not made part of the secure environment. The interface between the UISM and the secure environment may be protected or not.

It is noted that the first and second methods makes it impossible to get a late binding between the USIM identity and the RN device identity, the location of the RN, which operator owns the credentials on the USIM etc. It is FFS how this should be resolved and if it needs to be resolved.

The third method does not allow the USIM to be removed from the RN. Requiring that the field engineer shall be able to securely make the USIM part of the secure environment puts very high demands on the competence of the field engineer and also on the trust that must be put in the field engineer. During the work on deployment of macro eNBs it was clear that there were use cases where the field engineer could not be trusted by the operator with credentials. Hence the field engineer should probably not be trusted to perform this type of operation either.

The fourth method only relies on the field engineer inserts a USIM into the RN. The USIM may be removable. If a secure channel between the USIM and the secure environment is required this infers requirements on the RN and the UICC to support such functionality, including handling and holding of the required credentials.

If a field engineer provisions the USIM during installation of the RN, there is an opportunity to include other data on the USIM as well, such as the address or identity of the enrolment server, etc.

8.6 Location verification

Editor’s Note: The location of RN has effect on network performance and RN configuration. So the location e.g. Geographical information, surrounding radio environment, needs to be varified.

Editor’s Note: The need for location security if FFS.

8.7 Security handling in handover

8.7.1 UE Handover scenario

Generally, there are two additional types of handover scenario compared to HO scenario in legacy LTE system.

- UE handover from RN. Based on the target node type, more detailed scenarios are:
  - ✓ From RN to DeNB;
  - ✓ From RN to neighbor RN under the same DeNB;
  - ✓ From RN to neighbor eNB;
  - ✓ From RN to neighbor RN under another DeNB;
- UE handover to RN, additional details are:
  - ✓ From DeNB to RN;
  - ✓ From DeNB to RN under neighbor DeNB;

8.7.2 Security handling for UE Handover from/to RN

8.7.2.1 General

R8 UE can also access to RN, the security handling for UE handover from/to RN shall be compatible with legacy LTE UEs.

8.7.2.2 Security handling on the source node

If the souce node is a normal eNB, the same security handling as legacy LTE is applied.

If the source nodes are RN and its DeNB, either RN or DeNB may take the role of calculating keys for target cell and reestalishment cell or forwarding {NCC, NH} to target eNB. There are some differences between the two cases.

In case of source RN deriving keys for target node, the RN should forward the HANDOVER REQUEST message with security parameters, e.g. KeNB*s, algorithm used in source cell, UE security capability, NCC, to source DeNB.Then the DeNB reads the target cell ID from the message, finds the target eNB corresponding to the target cell ID, and forwards the X2 message toward the target eNB.

The DeNB has proxy function for all the S1/X2 messages terminated in RN and is able to obtain the security parameters used to update the keys during handover procedure. If the DeNB is responsible for caculating the keys, the source RN will forward HANDOVER REQUEST to DeNB without KeNB*s. The source RN has no knowledge of the KeNB*s used by target cell and cells for reestablishment, this has the effect of separating keys between source RN and target RN/eNB. While backward security is not affected, one-hop forward security is achieved by RN (forward security is not affected in the DeNB).

Editor's Note: How source DeNB learns about the KeNB that is used to calculate the key material for the target after RN has performed intra-cell HO or key-change-on-the-fly is FFS.

8.7.2.3 Security handling on the target node

In case that target node is a normal eNB, key handling in target side will be the same as described in 7.2.4.2.2 (X2 HO) or 7.2.4.2.3(S1 HO), TS 33.401 [2].

As RAN3 has come to an agreement that RN eNB id is equal to DeNB id, the source node can not differentiate the cells of RN and cells of DeNB from the detected cell ID. Cells under both nodes may be selected as target cell and cell for reestablishment. Following is the two detailed scenarioes.

1. Target cell in RN

The target cell and cells for reestablishment may be in different nodes, If target cell is under target RN while cells for reestablishment is under target DeNB, DeNB should extract security parameter prepared for cells of reestablishment under DeNB, e.g. KeNB*, NCC, algorithm used in source node and UE security capability, from the message sent by source DeNB, and then forward the message with security parameter,e.g.KeNB*,UE security capability,to target cell.

{NCC, NH} pair is used to separate keys between source node and target node and MME is responsible to update the {NCC, NH} in legacy LTE system.The same logic should be adopted in RN involved system for backward compatibility. However as the middle node between MME and target RN, the target DeNB may decide whether it will forward the {NCC, NH} pair to target RN. If the DeNB decide to locally keep a copy of {NCC, NH}, then it is possible for DeNB to calculate keys for target node in UE's next handover procedure.

2. Target cell in DeNB

When the target cell is under DeNB and there is cell for establishment under the RN.Still the DeNB should remove security information prepared for the DeNB cells and leave only the necessary information (e.g. UE security capability , NCC, KeNB*) in the X2 message to be transffered to target RN.

8.8 Analysis of key interaction on Un interface

8.8.1 Key relationship on Un interface

There are three options for the relationships of the keys on Un interface security:

- Scheme A: Device related keys and AS keys are independently generated
- Scheme B: IPsec keys are derived by AS keys
- Scheme C: AS keys are bound to RN device related keys

The schemes mapped into the remaining solutions under consideration as shown in table 8.8.1-1.

Table 8.8.1-1 Mapping relation between the schemes and solutions

scheme	mapped solution
scheme A	solution 4,solution 11,solution 12
schemeB	solution 7a
scheme C	solution 5,solution 8,solution 9

8.8.2 Analysis of the key interaction on Un interface

For scheme A, AS keys are derived from key generated in EPS-AKA. IPsec keys are generated during IKEv2 SA setup. IPsec key lifetime depends on SA lifetime. If lifetime of an SA expires, SA rekeying needs to be executed. The rekeying is implemented by creating new child SA to replace the expired SA and this rekeying procedure will not impact the service of existing IPsec tunnel.AS key updating will be executed indenpendently.There is no interaction between AS key updating and SA rekeying and therefore there is no need to synchronise between updating the keys on the two different layers. The following two requirements shall be satisfied.

1.Interface between UICC and RN-ME shall be secured;

2.AS keys shall be saved and processed in secured environment.

For scheme B, IPsec keys are based on keys from an AKA run. If interface between RN-ME and UICC is not secure, attackers can obtain AS keys and IPsec keys which are used to protect Un interface. The following two requirements shall be satisfied.

1. Interface between UICC and RN-ME shall be secured;

2. AS keys shall be saved and processed in secured environment.

If PDCP COUNT wraps round, AS keys could be updated by triggering an intra-cell handover procedure. The new AS key will introduce new either key K_{IKE} for IPsec or new key K_{IPSEC} for IKE that in turn generates new key for IPsec. IPsec rekeying is implemented by re-establishing security associations to take the place of ones that expire. The K_{IKE} may also be used as the new pre-shared key of the new SA. The SA rekeying may in reverse impact AS keys from key synchronization perspective.

For scheme C, the AS keys are the product of binding UICC authentication and RN platform authentication. If interface between RN-ME and UICC is not secure, the attackers still can not know AS keys which are used to protect Un interface, even in case that only AS security is used for Un security.

8.9 Differentiation the RN and UE by the DeNB

The donor eNB must know if a particular subscription is a RN subscription or a UE subscription so the donor eNB must know if it is authorised to pass S1-AP traffic to the RN. SA3's current preferred solution is the following:

Subscription type (e.g. RN or UE) can be added in the subscription data in the HSS. Then the MME can get the subscription type from the HSS and send it to the Donor eNB in a S1-AP message. For this solution,

- No specific IMSI range should be reserved. It can reduce operators management cost.

- The protocol between HSS and MME may need to be changed to transfer this subscription type. It will influence interface, i.e.S6a. It also needs standardization in other groups.

- MME should be also able to differentiate RN and UE when it received UE's subscription type, which is prior to the IP establishment.

8.10 NAS signalling security

In Phase I of RN attach the RN will attach as a legacy UE and Phase I attach should be possible against legacy eNB's and MME's. This means that all solutions relying on an unprotected interface between RN and UICC for Phase I attach will be susceptible to attacks on NAS signalling as the keys used for NAS protection could be derived from information intercepted on the RN UICC interface. For most of the existing NAS procedures (TS 24.301 [10]), an attack would at most lead to a recoverable DoS attack. Attacks on the NAS Security Mode Control procedure could lead to a bidding-down attack on AS and NAS algorithm; this could be a serious attack if the selected algorithms are used also after Phase I. Attacks on the EMM information procedure (optional) may lead to intercept/injection/ modification of information sent from the network to the RN. Attacks on the Generic transport of NAS messages procedure may lead to intercept/injection/modification of higher layer messages to/from the MME/UE.

This is acceptable because the Un is an operator internal interface acting as a backhaul. The RN (and DeNB) should thus be provisioned with the allowed sets of algorithms from the O&M system and these sets should only contain strong algorithms. The situation is the same as that for the backhaul protection for eNBs. There IPSec is used and an operator would not allow use of weak algorithms and the means to enforce this is to remove the weak algorithms from the set of negotiable algorithms in IKE.

For EMM and the Generic transport of NAS messages procedure restrictions may be required.

Editor's Note: It is for further study if there should be restrictions on use of EMM and the Generic transport of NAS messages procedures; this depends on their use in RN deployments.

8.11 Algorithm negotiation for RBs on Un interface

There are three types of RBs on Un interface.It has been decided that SRBs/DRBs of UE signaling plane shall be integrity protected.The confidentiality protection for DRBs of UE signaling plane may be mandatory.

1. S1/X2-AP protected by IPsec

In the case that S1/X2-AP messages are protected by IPsec, algorithms are selected during IPsec SA establishment.The SRBs and DRBs of UE user plane may select the same integrity algorithm and encryption algorithm.

As the integrity protection for SRBs is mandatory while integrity protection for DRBs of UE user plane is optional, there should be an indicator to switch the integrity protection for all DRBs of UE user plane on/off. This indicator may be carried in AS SMC. Or an indicator is prepared for each DRB of UE user plane when the DRB is established. This will bring more flexibility to DRB security configuration.

The confidentiality protection for SRBs and DRBs of UE user plane is optional. In the case that only one type of the RBs needs confidentiality protection according to the operator policy, there should be an indicator to switch the confidentiality protection for the other type of RBs off. For DRBs of UE user plane the confidentiality protection may be configured on per RB granularity.

Editor's Note: How IPsec interacts with lower layer is FFS.

2. S1/X2-AP protected in PDCP

In this case, all data transmitted on Un interface is protected in PDCP while different types of RBs have different security requirements.Algorithm selection scheme for all three types of RBs can be based on one of the following depending on operator policy/preference and/or network impact:

A. The same integrity algorithm and same encryption algorithm may be negotiated for data on all the three types of RBs on Un interface.The selected algorithms can be informed to RN by AS SMC. An indicator may be carried in AS SMC to enable/disable integrity protection and/or encryption protection DRBs of UE user plane.

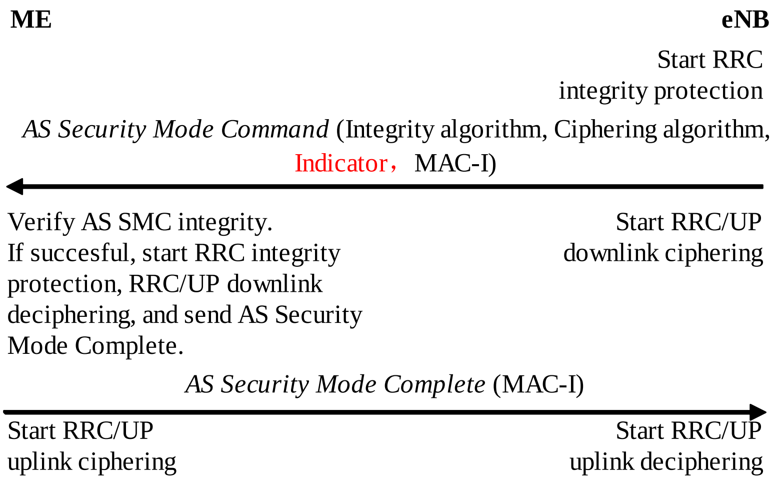

ME
eNB
Start RRC
integrity protection
AS Security Mode Command (Integrity algorithm, Ciphering algorithm,
Indicator， MAC-I)
Verify AS SMC integrity.
If succesful, start RRC integrity
protection, RRC/UP downlink
deciphering, and send AS Security
Mode Complete.
Start RRC/UP
downlink ciphering
AS Security Mode Complete (MAC-I)
Start RRC/UP
uplink ciphering
Start RRC/UP
uplink deciphering

Figure 8.11-1: AS SMC procedure

Alternatively, integrity protection and encryption protection of DRBs of UE user plane may be indicated during the DRB estabishment procedure.An indicator can be carried in the DRB establishment message.

B. Integrity algorithm and encryption algorithm for SRBs and DRBs of UE signalling plane are the same and both will be indicated in AS SMC.Algorithms for DRBs of UE user plane may configured when each DRB is established. For an example, drb-int-alg (indicated as integrity algorithm) and drb-enc-alg (indicated as encryption algorithm) may be captured as new configuration parameters in the establishment message for DRB. The appearance of the algorithm parameters may be used to switch protection of specific DRB on/off. In case either of the algorithm parameter does not appear in the establishment message for DRB of UE user plane, it means that the corresponding protection is disabled.

C. Algorithms are negotiated according to security requirements of each RB type. Integrity algorithm for SRBs and DRBs of UE signalling plane is the same. Integrity algorithm for DRBs of UE user plane is selected independently. Encryption algorithm for SRB and DRB of UE user plane is the same while encryption algorithm for DRB of UE signalling plane is selected independently.All of the above algorithms may be informed to RN by AS SMC. Integrity algorithm for DRBs of UE user plane and encryption algorithm for SRB and DRB of UE user plane may be set to specific value to disable the corresponding protection.

A is the easiest to be standardized and has least impact on legacy mechanism.Through this method operator can configure all DRBs of UE user plane to switch on/off integrity protection or encryption protection.

B has little impact on legacy mechanism. Operator can configure integrity algorithm or encryption algorithm for each DRB of UE user plane and enable/disable the protection for each DRB of UE user plane.

C has little impact on legacy mechanism while operator can configure security flexibly according to security requirement of each RB type.

Editor's Note: Algorithm negotiation and selection needs to be coordinated with RAN2.

9 Device Security

9.1 Security requirements on Relay Nodes

Editor's Note: RN sensitive data, such as IPsec certificates and pre-shared keys, need to be stored in a secure way.

The requirements related to device security in clause 5.3.5 of TS 33.401 [2] apply to Relay Nodes.

Editor's note: If is FFS whether further requirements are needed.

9.2 Device Integrity check

Editor's Note: Upon booting or before connecting to the network, the device integiry check may need to be performed, for the sake of RN validation.

The Relay Node should perform a device integrity check. The process of device integrity check should be protected from tampering or unauthorized execution.

The requirements 3,4 and 5 in 5.3.2 of TS 33.401 [2] apply here.

Editor's Note: The need for further requirements is FFS.

Editor's note: The following requirements are FFS. A failed device integrity check should be reported to the network (if the relay node is capable). A relay node which fails integrity checks for some components could allow for remote and secure recovery procedures, which restore device integrity (e.g. via software/firmware upgrade) according to operator policy

9.3 RN Platform Validation

The RN platform secure environment shall prevent the RN from attaching as RN to the network if the RN platform integrity is not assured by RN platform secure environment beforehand (i.e. integrity check is unsuccessful).

9.4 UICC aspects

Editor's Note: A UICC in a UE provides security under quite different assumptions from a UICC in an RN. What would happen if a UICC was removed from a genuine RN and inserted into a false RN? Is binding of USIM and RN in some way required? This should be considered.

Editor's note: Keeping the ongoing service of the UE attached to the Relay-Node even when UISM card was removed from the Relay-Node should be considered for emergency and priority service only

When RN attaches to the network via the RN attach procedure defined in TS 36.300 [4] a legacy UICC shall be used in authentication as defined in 3GPP TS 33.401 [2]. Preventing the attacks on removable UICC in RN needs to be considered. Possible methods of preventing this attack include physically integrating the RN and UICC together, a logical binding for example using a secure channel between the RN and UICC or some other binding method that is not between the RN or USIM.

Editor's Note: No decisions have yet been taken on the viability of these methods.

In the following, we discuss countermeasures against threat 5 of section 2 entitled "Attacks on the interface between the RN and the UICC" in more detail. Suitable countermeasures must ensure that attackers cannot obtain any advantage by listening on the interface between UICC and RN. If attackers could to this the attacker would know the keys sent across the interface between UICC and RN. For solutions that this is a problem, the following countermeasures may be used. The issue of binding particular USIMs and RNs is different and is not necessarily addressed by the same countermeasures.

Countermeasure 1):

Protect all traffic by security mechanisms residing above the AS layer.

With this countermeasure, the RN security architecture is designed such that AS security on the Un interface is not important for the overall security of the system. This would be the case if all traffic on Un was protected by IPsec, or even higher layer protocols. While this would provide good security it would be likely to have a quite negative effect on performance as the overhead created by protecting the UE user traffic by IPsec would be quite significant, both in terms of bandwidth and processing power. This solution is therefore not considered here any further.

Countermeasure 2):

Physical integration of RN and a non-removable UICC.

Such a solution would face two challenges: a) making the integrated RN / USIM hardware tamper-resistant such that the interface between RN and USIM cannot be attacked. This seems not easy, but doable. Cost would warrant a separate consideration, and it should be noted that such an approach would imply a significant deviation from the HW design of eNBs, something which may be considered undesirable. b) personalizing the USIM at the right point in time during the deployment process. Personalization in the factory seems undesirable as it limits the commercial flexibility, while personalization in the field would meet with the difficulties, technical and otherwise, encountered during the discussions on remote USIM management. This solution is therefore not considered here any further.

Countermeasure 3):

Physical protection of the interface between an RN and a removable UICC.

It would be sufficient to prevent eavesdropping on this interface while the USIM on the UICC was activated. Certainly, a suitable RN design could make it difficult for an attacker to access this interface. But the very fact that the UICC shall be removable means that the interface must be somehow exposed and exhibit electrical contacts. This may be exploited by an attacker while the RN is switched off and/or the USIM is deactivated, e.g. by establishing thin electrical wires leading from the contacts to the surface of the device. Of course, ingenious designs preventing this cannot be ruled out, but it may be quite difficult to prove the security of such a design. In view of these difficulties, further study on the viability of this countermeasure should not be precluded.

Countermeasure 4):

Logical protection of the interface between an RN and a removable UICC.

A standardized solution is available from ETSI TS 102 484 "Smart cards; Secure channel between a UICC and an end-point terminal". This TS contains three mechanisms for providing mutual authentication, confidentiality and integrity, namely a method called "Secured APDU" (Application Data Protocol Unit), TLS and IPsec. While the first mechanism works only with pre-shared keys, both TLS and IKE may be used with both, pre-shared keys or certificates. Pre-shared keys may be established using GBA as defined in 3GPP TS 33.110 [8], or in a proprietary way. The protection may be provided at the level of application, e.g USIM application, (TLS and Secured APDU), platform, i.e. UICC, (Secured APDU), or USB class (IPsec, for a definition of USB class cf. the reference in ETSI TS 102 484 [12]). The use of a secure channel between the UICC/USIM and the RN pre-supposes the existence of a secure environment on the RN in which the secure channel terminates.

The suitability of the mechanisms offered by ETSI TS 102 484 [12] for RN security is discussed in the following. While all these mechanisms seem feasible to apply in the RN context, they show differences in the complexity of the required changes.

Regarding key management

- A certificate-based solution seems to require relatively little extra effort as a certificate is to be available in the RN anyhow, e.g. if IPsec is selected to protect at least a part of the traffic on the Un interface. The certificate in the RN could be enrolled automatically, and the corresponding mechanisms for RN should be similar to enrolment procedures for eNBs defined in TS 33.310 [7]. UICCs, on the other hand, are under full control of the operator anyhow, and a certificate could be installed on a UICC e.g. when the applications on the UICC are personalized (e.g. when the permanent keys are installed on a USIM). This solution would affect only the UICC and the RN.

- A pre-shared-key-based solution using GBA according to TS 33.110 [8] would require additional functional entities currently not present in the EPS architecture, namely a BSF and a NAF Key Centre. This seems to add considerable complexity to the EPS architecture. Furthermore, certificates would be required in the RN and the NAF Key Centre for establishing the TLS connection between them.

- A pre-shared-key-based solution using a proprietary key management could, in principle, be realized by manually installing keys. But this should be ruled out as the deployment of RNs is likely to need an even higher degree of automation than that of ordinary eNBs. A proprietary key management according to ETSI TS 102 484 [12] could also be realized by a key management solution defined in another standard. In particular, 3GPP could define their own key management solution for this purpose, e.g. by exploiting the mechanisms of the EPS security architecture already available. But any such a solution would be likely to entail modifications to various functional entities defined for EPS today. It is difficult to conceive of such a solution affecting only the UICC and the RN.

Conclusion: if the secure channel method is adopted then a certificate-based solution is preferred as it seems to have the least impact on the existing EPS architecture.

Regarding the mechanism for authentication, confidentiality and integrity

- With the preference for a certificate-based solution expressed in the previous paragraph, of the mechanisms defined in ETSI TS 102 484 [12] only TLS and IPsec remain. Support for both, IPsec (for backhaul link protection) and TLS (for protecting the management connection to the OAM server), is available in present eNBs, and therefore implementing them in RNs would not mean a big change to the base station architecture. On the other hand, IKE/IPsec has a bigger footprint than TLS and could be less favourable for implementation on smart cards. Furthermore, TLS offers the possibility to selectively establish a secure channel between a single application on a UICC, e.g. a particular USIM, and the UICC-hosting device, i.e. in this case the RN, while IPsec does not offer this possibility.

Conclusion: if the secure channel method is adopted then TLS with mutual certificates is the preferred mechanism.

Editor's Note: Further study on the preferred mechanism is required if the secure channel method is adopted.

Editor's note: The above analysis was performed assuming a many to many relationships between RNs and UICCs was sufficient. If a solution requires a one-to-one relationship at the time of establishment of the secure channel then further analysis may be necessary.

10 Proposed Solutions

10.1 Solution 1 – IPsec for control and user plane

Editor's Note: Entities affected by security for relays (e.g. termination points of security protocols, entities with additional relay-related functionality) should be considered

10.1.1 General

This solution proposes to use IPsec between the RN and DeNB to protect both the user plane and control plane signalling. In many ways, this is the default option as it matches the standardised solution in the macro network.

10.1.2 Security Procedures

IPsec will be used to protect the S1-AP/X2-AP interface between the RN and DeNB exactly as for eNBs as described in clause 11 of TS 33.401 [2]. This prevents attacks 1, 3 and 4b. The overhead caused by the IPsec would be negligble as there is little signalling compared to user plane traffic.

The S1-U and X2-U interfaces are protected by IPsec as described in clause 12 of TS 33.401 [2]. While this might not be suitable for all deployments due to the overhead of using IPsec on small user plane packets, it is resaonable solution for the deployments when media traffic such as RTP will not be carried over LTE. It also has the advantage of requiring no protocol enhancements over the macro network. Using IPsec for both control plane and user plane solves attack 2 in the sense that while there could still be a MitM node, all the genuine UE related traffic available in the MitM node is protected.

Threat 4c is solved as the DeNB is the endpoint of the IPsec tunnels and hence there is no way a MitM could data on behalf of the user.

The risk of threat 5 is at least partially eliminated as the keys from the UICC will not be used to protect an data from a geniune UE or S1-AP/X2-AP signalling related to a UE.

10.1.3 UICC Aspects in RN scenarios

Editor's Note: A UICCin a UE provides security under quite different assumptions from a UICC in an RN. What would happen if a UICC was removed from a genuine RN and inserted into a false RN? Is binding of USIM and RN in some way required? This should be considered.

10.1.4 Enrolment procedures for RNs for backhaul link security

Editor's Note: Currently SA3 works on enrolment procedures for macro eNBs. It needs to be studied whether the same procedures apply to RNs. It should be considered how initial connectivity for enrolment would be provided?

10.1.5 Analysis of Solution 1

This solution is not sufficient. It only mentioned how the IPsec is used to protect the UE's CP and UP. But it is not clear on how to perform the AS security and what to do. However, one may assume that AS security is supposed to be used in solution 1 as for Rel-8.

What is more, it is not explicit on the security procedure to authenticate the RN and how to protect the RN's itself RRC and NAS signaling. But the main objection to solution 1 is the big overhead created by using IPsec for all traffic. This is probably not acceptable.

10.2 Solution 2 – IPsec for control and user plane with certificate and AKA authentication in IKE

Editor's Note: Entities affected by security for relays (e.g. termination points of security protocols, entities with additional relay-related functionality) should be considered

10.2.1 General

This solution uses IPsec to protect the signalling traffic over the Un interface and the AS level security to protect the user plane. In addition while using IKE to establish the IPsec, EAP-AKA is run in addition to the certificate based authentications as described from the H(e)NB cases.

Editor's Note: Additional criteria are needed to ensure that the binding between AKA and certificate based authentication ensures tha security of AS level commuication, e.g. the same USIM is used in both authentications.

10.2.2 Security Procedures

In this solution, when IPsec for S1-AP is being established, an EAP-AKA is run in addition to the certificate based authentication exactly as has been described in clause 7.3 of TS 33.320 [3]. This has the effect of binding the RN device authentication to the RN subcription authentication. It is not necessary for the network to keep track of the pairings between UICCs and RNs. Successful completion of this combined authentication assures both the network and RN that a geniune UICC is inserted in the RN. Hence the endpoint of both secure tunnels from the RN must be a node in the genuine network.

IPsec will be used to protect the S1-AP/X2-AP interface between the RN and DeNB exactly as for eNBs as described in clause 11 of TS 33.401 [2]. This prevents attacks 1, 3 and 4b. The overhead caused by the IPsec would be negligble as there is little signalling compared to user plane traffic.

This solution prevents attack 2 from working as the RN will not attach to the MitM node.

Attack 4c can be prevented as the is aware of which UE are attached to which RNs and hence it can prevent a rogue RN from inserting traffic belonging to the UE that is not connected to it.

10.2.3 UICC Aspects in RN scenarios

Editor's Note: A UICC in a UE provides security under quite different assumptions from a UICC in an RN. What would happen if a UICC was removed from a genuine RN and inserted into a false RN? Is binding of USIM and RN in some way required? This should be considered.

10.2.4 Enrolment procedures for RNs for backhaul link security

Editor's Note: Currently SA3 works on enrolment procedures for macro eNBs. It needs to be studied whether the same procedures apply to RNs. It should be considered how initial connectivity for enrolment would be provided?

10.2.5 Analysis of Solution 2

This solution is not sufficient. The security mechanism and procedure did not mention AS level security when RN acts as a UE. If the AS level security is not applied, RN should not be authenticated, and RRC and NAS signalings generated by RN are not protected, so threats 4a is not addressed. Even though it can assume that the intention is to use the normal EPS AKA and AS level security for RN's signaling protection..

This proposal is not explicit and also it did not say when the AKA is run.

And also for this solution, we think that there is an AKA run on the NAS layer first like a normal UE, then IP connection can be established and IKE can be performed. But it said in addition to this AKA on the NAS layer there is another EAP-AKA run in the IKE procedure. The purpose of running EAP AKA is not clear.

And also the EAP AKA cannot implement the binding between the RN and the UICC. So it is not considered how to bind UICC and device together.

There is no clear text on whom EAP AKA is used to authenticate. If it is used for authenticating the UICC, then there is a duplication for authenticating UICC. UICC shall be authenticated in AS security procedure It causes additional roundtrips and authentication vector consumption in the core network by running both EPS-AKA and EAP-AKA. It is a waste to radio bearer.

And also it is not clear on whether or not to use UICC for this EAP AKA, so there is threat on the local interface security as shown in the threat 5 in section 2.

10.3 Solution 3 – AKA credentials embedded in RN

Editor's Note: Entities affected by security for relays (e.g. termination points of security protocols, entities with additional relay-related functionality) should be considered

10.3.1 General

In this solution, the AKA credentials used to establish the AS level security between the RN and DeNB are embedded directly into the RN (e.g. in the secure environment of the RN). This means that there is no UICC required.

Either IPsec or enhanced AS security could be used to protect the S1-AP and X2-AP across the Un interface. AS level security is used to protect the user plane.

10.3.2 Security Procedures

Either enhanced AS or IPsec exactly as for eNBs as described in clause 11 of TS 33.401 [2] will be used to protect the S1-AP/X2-AP interface between the RN and DeNB. The use of IPsec or enhanced AS level security established from credentials directly on the RN prevents attacks 1, 3 and 4b. If IPsec is used, the overhead caused by the IPsec would be negligble as there is little signalling compared to user plane traffic.

As the AS level security is established from credential directly on the RN, this means that the RN is device authenticated at the network access layer and hence all of the threats 2, 4c, 4d are mitigated. Threat 5 is not a problem as that interface does not exist in this solution.

10.3.3 UICC Aspects in RN scenarios

None as there is no UICC.

10.3.4 Enrolment procedures for RNs for backhaul link security

This solution requires the RN to enroll a device certificate as with macro eNBs.

AKA credentials also need to be provisioned into the RN.

10.3.5 Analysis of Solution 3

This solution precondition is that AKA credential is embedded into device for this solution. Based on the requirement in clause 3.2.1, it is concluded AKA credential cannot not be embedded into device. So this solution shall be ruled out.

10.4 Solution 4 – IPsec for control plane and secure channel between RN and USIM with AKA credentials stored in UICC

10.4.1 General

The main features of this solution are: (1) Autonomous validation of the RN platform; (2) Secure Channel between USIM-RN and RN; (3) certificate validation client on the UICC; (4) IPsec integrity for S1/X2; (5) Use of a second USIM, called USIM-INI, for initial IP connectivity purposes prior to RN attachment.

The solution is further characterized by the fact that the MME-RN delegates the platform authentication of the RN to the UICC and trusts that the USIM-RN on the UICC engages in an AKA run only after successful platform authentication of the RN, cf. clause 10.4.8.1. A second layer of protection is inherent in this proposal be the use of IKEv2 between the RN and DeNB to establish IPsec integrity.

The overhead caused by IPsec may be considered negligble as there is little signalling traffic compared to user plane traffic. The overhead may be further reduced by the use of IPsec ESP in transport mode instead of tunnel mode. The choice of transport mode is possible here as the DeNB is the first IP hop from the RN.

Clauses 10.4.2 through 10.4.6 describe the solution with all its options. This description is closely aligned with that of solution 11.

Clauses 10.4.7.1 and 10.4.7.2 describe two profiles of solution 4, profiles 4A and 4B. It would be sufficient to standardize only one of these profiles.

In profile 4B, the certificate-checking requirements on the UICC are reduced by adding some requirement on the binding of the USIM-RN to an RN.

10.4.2 Security Procedures

The start-up of an RN proceeds in the following steps. If one of the steps fails in any of the involved entities the procedure is aborted by that entity.

Phase I: Procedures prior to the RN attach procedure

E1. The RN performs an autonomous validation of the RN platform.

E2. The RN attaches as a UE using USIM-INI to be prepared for performing steps E5. and, optionally, E3.

E3. The RN optionally obtains an operator certificate through the enrolment procedures defined in TS 33.310 [7]. Details can be found in clause 10.4.4. The RN optionally establishes a secure connection to an OAM server. Details can be found in clause 10.4.5.

E4. Then the RN platform secure environment and the UICC establish a Secure Channel between RN and USIM-RN according to ETSI TS 102 484 [12] clause 7 “Secured APDU” with TLS handshake. This TLS handshake shall be initiated by the UICC and use certificates on both sides. The RN uses a pre-established certificate or the certificate enrolled in step E3. The UICC verifies that this certificate is limited to use with relay nodes. The UICC is pre-provisioned with an operator root certificate to verify the RN certificate. The UICC certificate needs to be pre-installed in the UICC by the operator. The RN is pre-provisioned with a root certificate to verify the UICC certificate.

NOTE 1: The root certificate, and potentially other data required e.g. according to profile 4B, that need to be stored in the UICC could be provisioned in the UICC during its personalization. The operator provides to smartcard manufacturer a list of data (e.g. IMSI, key K, etc) to be provisioned in the UICC during its personalization phase, before issuance of the UICC. The root certificate, and potentially other data, could be provided by the operator as part of the data to be personalized in the UICC by the smartcard manufacturer. In the field, the root certificate, and potentially other data, could also be updated by OTA means, if needed.

The private key corresponding to the RN certificate and the root certificate used to verify the UICC certificate are stored in the secure environment of the RN platform validated in step E1, and the TLS handshake terminates there. From the completion of this step onwards, all communication between the USIM-RN and the RN is protected by the Secure Channel. The USIM-RN shall not engage in any AKA-related communication prior to the establishment of the Secure Channel and a successful certificate validation check, cf. step E.5.

NOTE 2: Certificate use restriction may be made possible e.g. through a suitable name structure, or a particular intermediate CA in the verification path, or policy information terms, e.g. by a suitable object identifier (OID) in the certificate policies extension.

NOTE 3: The USIM-RN is activated after the completion of the secure channel set-up, cf. ETSI TS 102 484 [12].

E5. A certificate validation client on the UICC checks the validity of RN certificate used in the secure channel set-up with a certificate validation server. The check of revocation status and expiry time may be omitted when there are additional restrictions on the binding between the USIM-RN and the RN, cf. profile 4B in clause 10.4.7.2, while the verification of the signatures in the certificate chain up to the root certificate shall be performed in any case. A certificate validation client on the RN checks the validity of UICC certificate used in the secure channel set-up with a certificate validation server. Details can be found in clause 10.4.6.

E6. The RN detaches from the network if it has attached for performing steps E2, E3, or E5.

NOTE 4: ETSI TS 102 484 [12] states in clause 6.2.2: "The UICC may present a self-signed certificate. The terminal or terminal application should temporarily accept such a certificate during the TLS handshake protocol, if it is able to establish by other means (e.g. successful network authentication) that the handshake protocol is conducted with an authentic UICC." And in the present solution for relay node security, the RN indeed verifies the authenticity of the USIM-RN by means of a successful RN attach procedure. However, the use of a self-signed UICC certificate, or no UICC certificate at all, would weaken network-to-RN authentication in cases where both the interfaces of the RN with the UICC and the network were under the control of an attacker. (Think of a stolen RN in a rogue environment.) Then the RN would happily use any key fed to it over the interface with a fake UICC and use this key in the communication with a fake network. The use of a UICC certificate prevents this threat as no rogue UICC can set up a secure channel with the RN. Similar considerations apply when the method in ETSI TS 102 484 [12] in clause 7 "Secured APDU" with TLS handshake is used.

NOTE 5: ETSI TS 102 484 [12] states in clause 6.2: "Both the terminal or the UICC shall be able to initiate a TLS secure channel." It is proposed here that the UICC assumes the role of TLS client for the following reason: the certificate validation cf. step E.5, can be integrated with TLS according to RFC 4366 [13], otherwise the certificate validation would have to be a separate procedure following the TLS procedure. When the method in ETSI TS 102 484 [12] in clause 7 "Secured APDU" with TLS handshake is used this requires an addition to the TS.

NOTE6: One may want to limit the lifetime of a secure channel between USIM-RN and RN for security reasons. Suitable counters providing such a limit include a record counter, cf. clause 6.4 of ETSI TS 102 484 [12], or a transaction counter, cf. clause 7 of ETSI TS 102 484 [12], or a counter on the AUTHENTICATE commands received over the secure channel. To disallow the resumption of TLS session, and to enforce a new TLS handshake on each RN attach, the USIM-RN may be configured accordingly, if necessary.

NOTE 7: Having two USIMs on one UICC is a standard feature available today (but only one USIM can be active at a time in current 3GPP specifications). The set-up of the secure channel between USIM-RN and RN causes the USIM-RN to be activated, but the connectivity and the security context established by means of USIM-INI may continue to be used. TS 33.401 [2], clause 6.4, requires the deletion of an EPS security context only when the UICC changes.

NOTE 8: The RN could distinguish a USIM-RN from a USIM-INI e.g by the use of so-called "labels" for UICC applications; cf. TS 31.101 [15] for the definition and TS 33.220 [11] for an example where such labels are used in 3GPP security specifications.

Phase II: RN attach procedure

The RN performs the RN attach procedure for EPS as defined in TS 36.300 [4]. From a security point of view, this involves the following steps:

A1. If the USIM-RN is not already active the RN activates it and resumes or re-establishes the secure channel. The RN activates the USIM-RN and invalidates any EPS security context on the USIM-RN. The RN uses the IMSI (or a related GUTI) pertaining to the USIM-RN in the RN attach procedure.

NOTE 9: This IMSI differs from the one pertaining to the USIM-INI, therefore the network can distinguish the handling of the two USIMs.

A2. The MME-RN runs EPS AKA with the RN and the USIM-RN and establishes NAS security. The RN shall use only keys in an RN attach procedure that were received from the USIM-RN over the Secure Channel.

A3. The MME-RN checks from the RN-specific subscription data received from the HSS that the USIM-RN is dedicated to the use in RN attach procedures. The MME-RN communicates the fact that the attachment is for relay nodes to the DeNB in an extended S1 INITIAL CONTEXT SETUP message.

A4. Upon receipt of the extended S1 INITIAL CONTEXT SETUP message the DeNB sets up AS security over Un as defined for Rel-8. The DeNB initiates certificate based IKEv2 to establish an IPsec ESP security association with the RN. Both IPsec in transport and tunnel mode are possible, but transport mode offers better performance. The IPsec traffic selectors are to be chosen such that precisely S1 and X2 traffic is protected by this security association. Only integrity protection (message authentication) is required, for encryption the NULL transform shall be used. The DeNB rejects any attach request by relay nodes for which no confirmation has been received from the MME-RN that the attachment is for relay nodes. The DeNB and the RN shall check the validity of each others' certificates by means of CRLs.

The RN start-up is now complete from a security point of view, and UEs can start attaching to the RN.

10.4.3 UICC Binding Aspects in RN scenarios

The requirement of restricting the possible combinations of particular RNs and particular USIMs is ffs, cf. clause 9.4. If such restrictions are required then authorization is required that could be enforced in at least one of the following ways:

(1) The RN enforces the allowed combinations.
The RN verifies the IMSI pertaining to the USIM-RN through the successful RN attach procedure. The RN can then learn about the allowed combinations of USIM-RN and RN as follows:

- (1a) The RN knows the authorized USIM-RNs by configuration;
- (1b) The OAM server with which a secure connection was established in step E.3 tells the RN the authorized identities;

NOTE: The check whether the binding between RN and USIM-RN is authorized can be entrusted to an RN with a validated platform. But only such RNs are able to establish a secure channel with a USIM-RN, which in turn is a pre-requisite for a successful RN attachment to the network, cf. clause 10.4.2. Hence the network can trust that the RN performs the check faithfully.

(2) The UICC enforces the allowed combinations.
The UICC verifies the RN identity through the TLS handshake in the secure channel set-up. The UICC knows the authorized RNs by configuration. The standard secure OTA mechanisms (TS 31.116 [9]) can be used to update the configuration of UICC and renew the stored identities if required.

(3) The MME enforces the allowed combinations.
The MME-RN may learn the RN device identity in a way similar to an MME learning the IMEI of a UE. Alternatively, the DeNB sends the RN device identity in a new S1 message to the MME-RN. The MME-RN then performs the check whether this combination of USIM and RN is authorized. The MME-RN may obtain the authorization information from the HSS.

Editor's Note: It is ffs whether the IMEI could serve as the RN device identity. If not a new NAS message or message field for sending the RN device identity may be required. In profiles 4A and 4B the sending of an RN device identity to the MME is not required.

10.4.4 Enrolment procedures for RNs

The RN may enroll a device certificate as with macro eNBs according to TS 33.310 [8] prior to the RN attach procedure with the DeNB. This certificate may then be used for running IKEv2 with the DeNB and, additionally, for establishing the secure channel between RN and USIM.

The certificate enrolment procedure does not rely on the security at the AS level, but is secured at the application layer. It can be therefore executed before security on the Un interface has been established. However, the RN requires IP connectivity for the enrolment procedure to be able to reach the Registration Authority RA. The IP connectivity could be established in various ways:

(1) The RN attaches to a fixed network for enrolment purposes. No USIM is required.

(2) The RN attaches to an eNB like a normal UE using a USIM, called USIM-INI, different from the one used in the RN attach procedure to the DeNB, called USIM-RN. No secure channel between RN and USIM-INI is required..

In both cases, the network must ensure that the destinations the RN can reach are restricted, e.g. to only the PDN(s) where the RA, the OAM server and the certificate validation server are located. In case (2) this could be ensured e.g. by restricting IP traffic originating from the RN and sent over PDCP without integrity protection to only certain destinations (APNs). The restrictions are assumed to be part of the profile relating to the subscription associated with the USIM-INI.

10.4.5 Secure management procedures for RNs

The RN may establish a secure connection to an OAM server.

The OAM procedure does not rely on the security at the AS level. It can therefore be executed before security on the Un interface has been established. If no security on lower layers is available the communication between RN and OAM server would be typically secured using TLS. The RN requires IP connectivity for this procedure to be able to reach the OAM server. The IP connectivity established for enrolment purposes according to clause 10.4.4 could be re-used, or, if not available, it could be established in the same ways as described in clause 10.4.4.

Restrictions on the destinations the RN can reach must apply if the communication with the OAM server occurs prior to the RN attach procedure. It can be realized similar to what is described in clause 10.4.4.

10.4.6 Certificate validation

The solution in this clause requires the UICC and the RN to perform certificate validation of the RN certificate and the UICC certificate respectively used for the set up of the secure channel prior to the RN attach procedure with the DeNB unless additional restrictions, as for profile 4B, cf. 10.4.7.2, apply . The certificate validation protocol shall be self-secured and can therefore be executed over unsecured links. The client on the UICC needs to send and receive the certificate validation data via the RN if a certificate status check is required according to the selected profile of solution 4, cf. clause 10.4.2, step E5.The RN requires IP connectivity for the certificate validation messages to be able to reach the certificate validation server. The IP connectivity, and the restrictions on permitted destinations, can be established in the same ways as described in clause 10.4.4 case (2). The certificate validation in step E5. of clause 10.4.2, shall be integrated with the TLS handshake performed in step E4., according to RFC 4366 [13].

If certificate validation is required then OCSP, cf. RFC 2560 [17], shall be used for certificate validation in the following way: the UICC shall generate a nonce. This nonce is sent as part of the TLS client hello, as described in RFC 4366 [13]. The RN, acting as the OCSP client, shall form an OCSP request including this nonce in a requestExtension, as defined in RFC 2560 [17]. The signed response of the OCSP responder then also includes this nonce, according to RFC 2560 [17]. Furthermore, this signed response mandatorily includes a “producedAt” field, indicating the time at which the OCSP responder signed the response. The RN forwards the signed response of the OCSP responder as part of the TLS handshake to the UICC, as described in RFC 4366 [13]. The UICC then checks the CertStatus and that the expiry time of the RN certificate is later than the producedAt-time in the signed response of the OCSP responder.

NOTE: The above expiry time checking procedure ensures the UICC that the RN certificate was valid at the time the UICC started the TLS handshake. As the UICC has no clock the UICC cannot control the duration of the TLS handshake. In case this is a concern methods to enforce TLS handshakes, and hence OCSP checks, at defined events controlled by the network, e.g. AKA runs, may be used. An example is given in profile 11A, cf. clause 10.11.7.1.

10.4.7 Profiles of solution 4

This clause describes two profiles of solution 11, profile 11A in clause 10.4.7.1 and profile 11B in clause 10.4.7.2.

10.4.7.1 Solution profile 4A

10.4.7.1.1 General

The UICC inserted in the RN contains two USIMs: a USIM-RN which shall communicate with the RN only via a secure channel, and a USIM-INI communicating with the RN without secure channel and used for initial IP connectivity purposes prior to RN attachment.

USIM-INI and USIM-RN could be functionally identical to Rel-99 USIMs. But a restriction of the command set, compared to a Rel-99 USIM, may be appropriate. In addition there will be other requirement on the UICC to perform the TLS handshake (BIP-UICC server mode or UICC USB).

NOTE: The proposed solution with USIM-INI and USIM-RN does not imply new functionality on Rel-99 USIM. Only additional files may be needed, e.g. for RN profile. The secure channel features are at the UICC platform level and Rel-x UICC implementing the secure channel could contain Rel-99 USIM.

No particular binding of RN and USIM-RN is required. But the UICC shall check in the secure channel set-up that the RN certificate is dedicated to use with RNs.

10.4.7.1.2 Security Procedures

The start-up of an RN proceeds in the following steps. If one of the steps fails in any of the involved entities the procedure is aborted by that entity.

Phase I: Procedures prior to the RN attach procedure

E1. The RN performs an autonomous validation of the RN platform.

E2. The RN attaches as a UE using USIM-INI.

E3. The RN optionally obtains an operator certificate through the enrolment procedures defined in TS 33.310 [7]. Details can be found in clause 10.4.7.1.4. The RN optionally establishes a secure connection to an OAM server. Details can be found in clause 10.4.7.1.5. The RN shall retrieve a CRL from a suitable server.

E4.Then the RN platform secure environment and the UICC establish a Secure Channel between RN and USIM-RN according to ETSI TS 102 484 [12] clause 7 “Secured APDU” with TLS handshake. This TLS handshake shall be initiated by the UICC and use certificates on both sides. The RN uses a pre-established certificate or the certificate enrolled in step E3. The UICC verifies that this certificate is limited to use with relay nodes. The UICC is pre-provisioned with an operator root certificate to verify the RN certificate. The UICC certificate needs to be pre-installed in the UICC by the operator. The RN is provisioned with a root certificate to verify the UICC certificate.

The private key corresponding to the RN certificate and the root certificate used to verify the UICC certificate are stored in the secure environment of the RN platform validated in step E1, and the TLS handshake terminates there. From the completion of this step onwards, all communication between the USIM-RN and the RN is protected by the Secure Channel. The USIM-RN shall not engage in any AKA-related communication prior to the establishment of the Secure Channel and a successful certificate validation check, cf. step E.5.

The UICC shall re-establish the Secure Channel including a new certificate validation according to clause 10.4.6 after every AUTHENTICATE command exchanged between RN and USIM-RN.

NOTE: TS 33.310 [7] mandates the use of the same key for digitalSignature and keyEncipherment, e.g. clause 6.1.3 for SEG certificate profile.

E5. A certificate validation client on the UICC checks the validity of RN certificate used in the secure channel set-up with a certificate validation server. The verification of the signatures in the certificate chain up to the root certificate shall be performed. A certificate validation client on the RN checks the validity of UICC certificate used in the secure channel set-up with a certificate validation server. Details can be found in clause 10.4.7.1.6.

E6. The RN detaches from the network if it has attached for performing steps E2, E3, or E5.

Phase II: RN attach procedure

The RN performs the RN attach procedure for EPS as defined in TS 36.300 [4]. From a security point of view, this involves the following steps:

A1. If the USIM-RN is not already active the RN activates it and resumes or re-establishes the secure channel. The RN invalidates any EPS security context on the USIM-RN. The RN uses the IMSI (or a related GUTI) pertaining to the USIM-RN in the RN attach procedure. The RN shall request access only to the default APN. The default APN allows access to only the OCSP server.

NOTE 1: A Default APN is defined as the APN which is marked as default in the subscription data and used during the Attach procedure and the UE requested PDN connectivity procedure when no APN is provided by the UE, cf. 23.401 [16], clause 3.

A2. The MME-RN runs EPS AKA with the RN and the USIM-RN and establishes NAS security. The RN shall use only keys in an RN attach procedure that were received from the USIM-RN over the Secure Channel.

A3. The MME-RN checks from the RN-specific subscription data received from the HSS that the USIM-RN is dedicated to the use in RN attach procedures. If the RN requested access to an APN other than the default APN the MME shall reject the request. The MME-RN communicates the fact that the attachment is for relay nodes to the DeNB in an extended S1 INITIAL CONTEXT SETUP message.

A4. Upon receipt of the extended S1 INITIAL CONTEXT SETUP message the DeNB sets up AS security over Un as defined for Rel-8. The DeNB initiates certificate based IKEv2 to establish an IPsec ESP security association with the RN in transport mode. The IPsec traffic selectors are to be chosen such that precisely S1 and X2 traffic is protected by this security association. Only integrity protection (message authentication) is required, for encryption the NULL transform shall be used. The DeNB rejects any attach request by relay nodes for which no confirmation has been received from the MME-RN that the attachment is for relay nodes. The DeNB and the RN shall check the validity of each others' certificates by means of CRLs.

A5. According to step E4., a new TLS handshake including certificate validation according to E.5 is performed. The RN uses the IP connectivity of the RN to the default APN establishes in step A4 to communicate with the server providing certificate validation information.

A6. The RN sends a PDN connectivity request for the APNs required for performing its function as a relay node. The MME shall challenge this request by sending an Authentication request. After successful completion of the authentication procedure and a corresponding key-change-on-the-fly, the MME shall establish the requested PDN connectivity for the RN. The MME shall control the time elapsed between steps A2 and A6 by setting a suitable timer.

The RN start-up is now complete from a security point of view, and UEs can start attaching to the RN.

NOTE 2: The above procedure ensures that a certificate validation check is completed by the UICC during the RN attach procedure. This ensures in turn that the RN certificate has not expired, for details cf. 10.4.7.1.6.

10.4.7.1.3 USIM Binding Aspects in RN scenarios

For this profile, no particular binding between USIM and RN is required.

10.4.7.1.4 Enrolment procedures for RNs

No change from 10.4.4.

10.4.7.1.5 Secure management procedures for RNs

No change from 10.4.5.

10.4.7.1.6 Certificate validation

Profile 4A requires the UICC and the RN to perform certificate validation as described in clause 10.4.6.

10.4.7.2 Solution profile 4B

10.4.7.2.1 General

The UICC inserted in the RN contains two USIMs: a USIM-RN which shall communicate with the RN only via a secure channel, and a USIM-INI communicating with the RN without secure channel and used for initial IP connectivity purposes prior to RN attachment.

USIM-INI and USIM-RN could be functionally identical to Rel-99 USIMs. But a restriction of the command set, compared to a Rel-99 USIM, may be appropriate. In addition there will be other requirement on the UICC to perform the TLS handshake (BIP-UICC server mode or UICC USB).

NOTE: The proposed solution with USIM-INI and USIM-RN does not imply new functionality on Rel-99 USIM. Only additional files may be needed, e.g. for RN profile. The secure channel features are at the UICC platform level and Rel-x UICC implementing the secure channel could contain Rel-99 USIM.

The basic idea of profile 4B is that, once the USIM-RN has established a secure channel to one RN, it cannot establish further secure channels, simultaneously or consecutively, to other RNs (e.g. as represented by the subject name in the certificate) until reset by administrative procedures. There is no need to pre-establish the relationship between USIM-RN and RN.

10.4.7.2.2 Security Procedures

The start-up of an RN proceeds in the following steps. If one of the steps fails in any of the involved entities the procedure is aborted by that entity.

Phase I: Procedures prior to the RN attach procedure

E1. The RN performs an autonomous validation of the RN platform.

E2. The RN attaches as a UE using USIM-INI.

E3. The RN optionally obtains an operator certificate through the enrolment procedure defined in TS 33.310 [7]. Details can be found in clause 10.4.7.2.4. The RN optionally establishes a secure connection to an OAM server. Details can be found in clause 10.4.7.2.5. The RN shall retrieve a CRL from a suitable server.

E4. The RN platform secure environment and the UICC establish a Secure Channel between RN and USIM-RN according to ETSI TS 102 484 [12] clause 7 "Secured APDU" with TLS handshake. This TLS handshake shall be initiated by the UICC and use certificates on both sides. The RN either uses a pre-established certificate or the certificate enrolled in step E3. The UICC verifies that this certificate is limited to use with relay nodes. The UICC is pre-provisioned with an operator root certificate to verify the RN certificate. The UICC certificate needs to be pre-installed in the UICC by the operator. The RN is provisioned with a root certificate to verify the UICC certificate.

The private key corresponding to the RN certificate and the root certificate used to verify the UICC certificate are stored in the secure environment of the RN platform validated in step E1, and the TLS connection terminates there. From the completion of this step onwards, all communication between the USIM-RN and the RN is protected by the Secure Channel. The USIM-RN shall not engage in any AKA-related communication prior to the establishment of the Secure Channel.

The lifetime of the secure channel between USIM-RN and RN shall be limited by a transaction counter, cf. clause 7 of ETSI TS 102 484 [12].

E5. A certificate validation client on the UICC shall verify the signatures in the RN certificate chain up to the root certificate. The check of revocation status and expiry time is omitted. A certificate validation client on the RN shall check the verification of the signatures in the RN certificate chain up to the root certificate as well as the revocation status and expiry time. Details can be found in clause 10.4.7.2.6.

E6. The RN detaches from the network.

Phase II: RN attach procedure

The RN performs the RN attach procedure for EPS as defined in TS36.300 [4]. From a security point of view, this involves the following steps:

A1. If the USIM-RN is not already active the RN activates it and resumes or re-establishes the secure channel by a new TLS handshake. The RN invalidates any EPS security context on the USIM-RN. The RN uses the IMSI (or a related GUTI) pertaining to the USIM-RN in the RN attach procedure.

A2. The MME-RN runs EPS AKA with the RN and the USIM-RN and establishes NAS security. The RN shall use only keys in an RN attach procedure that were received from the USIM-RN over the Secure Channel.

A3. The MME-RN checks from the RN-specific subscription data received from the HSS that the USIM-RN is dedicated to the use in RN attach procedures. The MME-RN communicates the fact that the attachment is for relay nodes to the DeNB in an extended S1 INITIAL CONTEXT SETUP message.

A4. Upon receipt of the extended S1 INITIAL CONTEXT SETUP message the DeNB sets up AS security over Un as defined for Rel-8. The DenB initiates certificate based IKEv2 to establish an IPsec ESP security association with the RN in transport mode. The IPsec traffic selectors are to be chosen such that precisely S1 and X2 traffic is protected by this security association. Only integrity protection (message authentication) is required, for encryption the NULL transform shall be used. The DeNB rejects any attach request by relay nodes for which no confirmation has been received from the MME-RN that the attachment is for relay nodes. The DeNB and the RN shall check the validity of each others' certificates by means of CRLs. In addition, the DeNB verifies that the certificate presented by the RN is limited to use with relay nodes.

The RN start-up is now complete from a security point of view, and UEs can start attaching to the RN.

10.4.7.2.3 USIM Binding Aspects

For the security of this profile 4B, a USIM-RN need not be configured with an identity of an RN to which it is allowed to attach. The USIM-RN may establish a secure channel with any RN, with which the procedure in 10.4.7.2.2 can be successfully performed. But the UICC shall store the identity of this RN (e.g. as represented by the subject name in the certificate) and shall not engage in a secure channel set-up with any other RN until reset by administrative procedures. A suitable procedure could be the entry of a super-PIN by a field engineer.

NOTE 1: Setting up a secure channel with another RN would imply that the UICC would be inserted in a different RN, hence manual intervention would be required anyhow.

NOTE 2: As solution 4 and solution 11 (see clause 10.11) both provide comparable profiles A and B, it is stated here explicitly for clarity, that contrary to profile 11B (see clause 10.11.7.2.3) profile 4B does not require the configuration of the UICC with an identity of an allowed RN.

10.4.7.2.4 Enrolment procedures for RNs

No change from 10.4.4.

10.4.7.2.5 Secure management procedures for RNs

No change from 10.4.5.

10.4.7.2.6 Certificate and subscription handling

As described in clause 10.4.7.2.2, step E5, the certificate validation client on the UICC verifies the signatures in the RN certificate chain up to the root certificate, but omits the check of revocation status and expiry time. A certificate validation client on the RN shall check the verification of the signatures in the RN certificate chain up to the root certificate as well as the revocation status and expiry time. The revocation status of the UICC certificate is checked by means of the CRL obtained by the RN in 10.4.7.2.2, step E3. Consequently, no OCSP server is needed in profile 4B.

Further considerations on certificate and subscription handling for profile 4B:

The requirement that the USIM-RN is allowed to establish a secure channel to only one RN until reset by administrative means obviates the need for OCSP checking of the RN certificate by the UICC because the RN certificate is later checked by the DeNB during the IKEv2 run. If the USIM-RN happened to set up a secure channel with a compromised RN (known as such to the operator) then this compromised RN would fail the RN attach procedure due to the failed IKEv2 set-up, and the USIM-RN bound to it could not be used in RN attach procedures. And once the USIM-RN has set up a secure channel with a genuine RN it will not set up a secure channel with any different RN any more, in particular not to a compromised RN. Hence, no compromised RN could get access to any keys generated by a USIM-RN once attached to a genuine RN.

10.4.8 Analysis of Solution 4

10.4.8.1 How does solution 4 address the threats in clause 5?

1) NOTE: this text is aligned with 10.11.8.1.

Threat 1: Impersonation of a RN to attack user attached to RN

The text in clause 5.3 states that threat 1 can be countered by device authentication. By the definition in clause 3.1, platform authentication "is performed between a secure environment in the RN platform and a network entity". No such protocol between a secure environment in the RN platform and a network entity is run in solution 4, but nevertheless solution 4 implicitly provides the same assurances to the MME-RN as platform authentication would provide, as can be seen from the following reasoning, in which we repeatedly refer to the elements of the definition in clause 3.1 We can therefore say that solution 4 provides implicit platform authentication to the MME-RN.

Definition from clause 3.1: "…the network entity has verified that the secure environment in the RN is in possession of a secret key associated with the RN."

Solution in clause 10.11: In short, the MME-RN delegates the platform authentication of the RN to the UICC and trusts that the USIM-RN on the UICC engages in an AKA run only after successful platform authentication of the RN. In more detail: The MME-RN successfully runs EPS AKA with the RN and USIM-RN. This is only possible when the USIM-RN engages in AKA-related communication with the terminal (i.e. here: the RN) in which it is inserted. The MME-RN knows that the USIM-RN is dedicated to be used in RN attach procedures and that such USIMs communicate with terminals only over secure channels. Furthermore, they do so only after they checked the validity of the terminal (i.e. here: the RN) certificate by means of certificate validation and that the certificate is limited to use with relay nodes, cf. clause 10.4.2. Hence the MME-RN concludes that the UICC has successfully checked that the RN has a valid certificate and the corresponding private key. But an RN private key corresponding to a valid certificate limited to use with relay nodes resides in the secure environment of a relay node. The RN attach procedure hence tells the MME-RN that the attached entity indeed resides on an RN platform, but it does not provide the MME-RN yet with a verified identity of an individual device. If the latter is also desired the RN can send the IMEI or another suitable identity via the NAS protocol to the MME-RN, as explained in clause 10.4.3. This completes the argument. For profile 4B of solution 4, the argument slightly varies in that the certificate expiry and revocation check is performed as part of the IKEv2 run, which prevents effective further use of the AS keys when the check fails.

Definition from clause 3.1: "RN platform authentication is intended to additionally provide implicit proof of the integrity of the RN platform to the network entity. This is achieved by assuming that the secure environment in the RN engages in RN platform authentication only after a successful autonomous RN platform validation has been performed."

Solution in clause 10.11: A secure environment in a genuine RN engages in the set-up of a secure channel with the USIM-RN only after a successful autonomous RN platform validation has been performed, and the USIM-RN verifies that it has set up a secure channel with a genuine RN, cf. clause 10.11.2. As the MME-RN learnt in the previous step that such a secure channel was successfully established the MME-RN can also conclude that a successful autonomous RN platform validation has been performed.

Threat 2: MitM on the Un interface between RN and DeNB

The description of threat 2 in clause 5.3 requires inserting the real UICC into the MitM node. This is prevented by the fact that the USIM-RN on the UICC checks whether the secure channel with a real RN has been set up successfully before engaging in AKA-related communication. The necessary validity check of the RN certificate is performed differently in profiles 4A and 4B.

In profile 4A according to clause 10.4.7.1the UICC performs a complete validity check of the RN certificate including check of expiry and revocation status.

In profile 4B according to clause 10.4.7.2 the UICC only performs a check of the signature chain up to the root certificate, thus validating that the certificate chain really extends to the preconfigured root certificate. Expiry and revocation check in the UICC is replaced by the later complete validity check of the RN certificate in the DeNB. In this case a USIM-RN would still establish a secure channel with a RN presenting an expired or revoked certificate, but the RN would not be able to attach to the DeNB as RN. Further security details are described in clause 10.4.7.2.6.

In addition, the description of threat 2 in clause 5.3 assumes that a fake UICC can be inserted in a real RN. This is prevented by the fact that the RN checks whether the secure channel with the USIM has been set up successfully before performing the RN attach procedure. **Threat 3: Attacking the traffic on the Un interface between RN and DeNB**

Integrity protection of S1-AP and X2-AP signalling across the Un interface is provided by an IPsec security association between RN and DeNB. Other traffic over Un is sufficiently protected by AS security.

Threat 4: Impersonation of a RN to attack the network

The description of threat 4 in clause 5.3 states that threat 4 could be mitigated by ensuring device authentication of the RN. But device authentication is provided, cf. response to threat 1. Access of the RN to the network needs to be restricted until the device authentication is successful.

Threat 5: Attacks on the interface between the RN and the UICC

The attacks are prevented by the secure channel between the USIM and the RN. More precisely: as stated in clause 10.4, it is ensured that no NAS security context exists in the RN or the USIM immediately prior to the set-up of the secure channel between USIM and RN. The RN attach procedure happens only after the secure channel between USIM and RN has been set up. In this way, the RN ensures that the keys sent from the USIM to the RN from which the AS security context on Un is derived were received by the RN through the secure channel. The DeNB checks through device authentication that the integrity of the platform of the RN attempting to attach is guaranteed. Hence the DeNB knows that this RN has checked that the secure channel was in place before the start of the RN attach procedure, so the AS keys are not compromised by attacks on the interface between RN and UICC.

Threat 6: Control of the RN platform

This threat is prevented by autonomous validation and device authentication, cf. response to threat 1.

Threat 7: DoS type attacks

The description of this threat has two parts:

a) From clause 5.3: "When the attacker removes the USIM, RN without USIM can't be authenticated by the network. So the legal RN can't connect to network and provide services."
Response: An attacker removing a USIM could just as easily physically destroy the RN so this type of DoS cannot be prevented.

b) From clause 5.3: "The attacker could also insert the USIM into another RN, then the topology of access network will be changed and cause interference problem to other eNB."
Response: If the other RN is a fake then the threat is the same as threat 1. If the other RN is genuine then there are several solutions on top of solution 4 for ensuring that the binding between USIM and RN is authorized. Possible solutions are listed in clause 10.4.3.

10.4.8.2 How does solution 4 fulfil the requirements in clause 6?

We quote text from clause 6.

"If end to end protection between the RN and the core network is needed, then the same solution as for backhaul protection should be considered."

Response: But e2e protection is not possible due to the chosen architecture alternative, as stated in the next paragraph, so this sentence should be removed.

"Integrity protection for the S1 control plane traffic over the Un shall be mandatory."

Response: This is provided in solution 4 by the mandatory IPsec security association between RN and DeNB.

"The S1 control plane traffic between RN and MME-UE shall be integrity protected between the DeNB and the MME-UE with at least the same strength as in the current EPS architecture."

Response: This requirement seems compatible with all solutions described in clause 7. It is addressed as in clause 11 of TS 33.401 [2] today.

"Integrity protection for the X2 control plane traffic over the Un shall be mandatory. The X2 control plane traffic between RN and eNB/RN shall be integrity protected between the DeNB and the eNB/RN with at least the same strength as in the current EPS architecture."

Response: same as for S1 traffic.

"Mutual authentication between RN and network shall be supported."

Response: This is a bit vague as the authenticating network entity is not mentioned. Mutual authentication between RN and MME-RN is provided by EPS AKA performed according to TS 33.401 [2]. Mutual authentication between RN and DeNB is provided by IKEv2 with mutual certificates according to solution 4.

"Relay device authentication is mandatory."

Response: solution 4 provides this, cf. response in clause 10.4.8.1 to threat 1.

"The DeNB shall not accept or send S1-AP and X2-AP message from/to the RN until a successful Relay device authentication has happened."

Response: cf. response in clause 10.4.8.1 to threat 1 where it is explained that platform authentication is provided as part of the RN attach procedure.

"Security of RN Management shall be guaranteed."

Response: this requirement seems compatible with all solutions described in clause 7. Either a separate TLS connection is set up to the OAM server, or, after the successful completion of the RN attach procedure, the management traffic is secured hop-by-hop

"The wireless resource: security shall be able to prevent misuse by identifying whether the attached terminal is a UE or a RN. The identification could be implicit."

Response: this requirement is addressed by step A.3 in clause 10.4.2: the MME-RN "checks from the RN-specific subscription data received from the HSS that the USIM-RN is dedicated to the use in RN attach procedures.".

"The connection between relay and network should be confidentiality protected. Confidential protection for the S1/X2 user plane traffic over the Un should provide protection as same as the user plane data transferred on Uu interface, i.e. provide optional confidentiality protection on Un interface."

Response: solution 4 uses IPsec for integrity of S1 and X2, and AS security otherwise.

"Both user plane and control plane must be considered as they may not require the same level of protection."

Response: solution 4 satifies this requirement.

"The RN platform shall protect from reading and/or modification of security parameters and security functions by unauthorized parties (platform security). The integrity of the RN platform shall be validated as part of the RN start up procedure."

Response: solution 4 requires platform integrity and device authentication as part of the start-up procedure.

"RN specific device security features, e.g. security storage of sensitive data, device integrity check, USIM aspects, shall be considered."

Response: for secure storage and device integrity cf. the preceding response, for USIM aspects a secure channel is provided in solution 4, and the binding aspects between particular USIMS and RNs have been considered in clause 10.4.3.

10.4.8.3 How does solution 4 address the general Editor's notes and the residual threats in clause 8.1.2.1?

Solution 4 is a more detailed version of Option 1 "NDS/IP and AS security over the Un interface" described in clause 8.1.2.1. We quote from clause 8.1.2.1.

"Editor's Note: It needs to be clarified whether all traffic over the Un user plane, or only S1 signalling traffic, is to be protected by NDS/IP, e.g. for performance reasons. If the latter applies then appropriate mapping of parameters identifying S1 signalling traffic to IPsec selectors (IP addresses, ports, transport protocol) would have to be performed."

Response: Solution 4 opts for protecting only S1 and X2 traffic by means of IPsec for performance reasons. The traffic selectors are ffs, but are believed not to be a fundamental obstacle.

"Editor's Note: The enrolment process for credentials to set up backhaul link security between RN and MME-RN, and RN and S-/P-GW-RN (i.e. distribution of IPsec certificates and set up of IPsec tunnel) needs to be studied."

Response: the enrolment phase is taken care of in solution 4.

"Editor's Note: The following is for further study: The donor eNB must know if a particular subscription is a RN subscription or a UE subscription so the donor eNB must know if it is authorised to pass S1-AP traffic to the RN. It requires further study whether this requirement can be supported using the current S1-AP protocol and/or core network procedures. Furthermore the donor eNB must know that it has to apply the Un security procedures which are by assumption different to the Uu procedures."

Response: according to solution 4, the DeNB obtains this information from the MME-RN, cf. step A.3 in clause 10.4.2.

"**Residual Threat:** threats of eavesdropping on and modification of traffic of DRBs is satisfactorily addressed by platform integrity and use of IPsec. As RRC traffic cannot be protected by IPsec it needs to be considered separately. The main threat to RRC seems to be that an attacker modifies bearers on Un. This seems to be possible when an attacker knows the RRC integrity key.
Editor's Note: threats to AS security for RRC over Un need further study. In particular: how can an attacker obtain knowledge of the RRC integrity key? "

Response: in solution 4 the attacker cannot obtain the RRC integrity key, cf. response in clause 10.4.8.1 to threat 5.

"**Residual Threat:** neither RRC nor UP-UE traffic are protected by IPsec. (UP-UE = user plane data sent by UE.) In addition to the remarks made on RRC in 5.1.2.1.2.1, the attacker could eavesdrop on UP-UE. An attacker could e.g. fraudulently establish an RN-DeNB radio connection via a MitM as described for threat 2 in section 1.
Depending on the way in which the attacker obtains knowledge of the keys it may not be enough to ascertain that the IPsec SAs and AS security have the same endpoints, i.e. that all security tunnels from the RN terminate in the real network instead of in a MitM node may not be sufficient. It may neither be sufficient to bind the USIM to the RN, e.g. by using EAP-AKA inside IKEv2 in the way done for HeNBs.

Editor's Note: threats to AS security for RRC and UP-UE over Un need further study."

Response: in solution 4 the attacker cannot obtain the UP-UE encryption key, cf. *responses in clause 10.4.8.1* to threats 2 and 5.

10.5 Solution 5 – Enhanced AKA to include device authentication

10.5.1 General

In this solution, the authentication procedures are enhanced between the network and RN in order to provide authentication based on credentials stored on the RN. Either enhanced AS or IPsec is used to protect the control plane signalling. The user plane traffic will be protected by the AS level security.

10.5.2 Security Procedures

10.5.2.1 General

Using either IPsec exactly as for eNBs as described in clause 11 of TS 33.401 [2] or enhanced AS security to protect the S1-AP/X2-AP interface between the RN and DeNB will prevent attacks 1, 3 and 4b. The overhead caused by the IPsec would be negligible as there is little signalling compared to user plane traffic.

The user plane data is protected by the AS level security. The EPS AKA procedure is run to authenticate the UICC in the RN and the network. The AKA run also provides the keying material for the AS level security. Additional IEs are included in some NAS messages in order to provide authentication between the RN and network based on credentials stored on the RN.. This would prevent threats 2, 4c and 4d.. Threat 5 is mitigated by using keys for the E-UTRAN that result from both the AKA and authentication based on credentials on the relay node.

10.5.2.2 Enhanced AKA authentication

10.5.2.2.1 High level description

In this solution, the device authentication is proposed to work in conjunction with the standard EPS AKA access authentication. The solution assumes that the device has been provisioned with a *device_root_key* that can be used to send encrypted traffic to the device and that is uniquely associated to the *device_identity*. The *device_identity* is assumed to be the IMEI of the device. The *device_root_key* is a public key of the device certificate. The associated private key(s) of the device are stored securely in the device. In the following descriptions, the *device_credentials* are the device certificate (an alternative approach would be a pointer to the certificate (e.g., *device_identity*)). This public/private key pair and certificate is in addition to any that the Relay Node may use for signing.

The *device_credentials* allow a network entity to form the *device_challenge* (see below) and to check the revocation status of the device (e.g., check whether the device credentials have been compromised). It is further assumed that a secure part of the device stores the sensitive device keys such as the private key associated with the certificate. Furthermore, it is assumed that the secure part of the relay node performs all cryptographic operations that make use of these sensitive keys.

Whenever the network wishes to perform device authentication, it creates a *device_challenge* and sends it to the device in a relevant NAS message. The device computes the *device_response* and returns it to the network in a response NAS message. The device uses the data in *device_challenge* and *device_response* to calculate K_{ASME_D}. K_{ASME_D} is the equivalent key to K_{ASME} defined in E-UTRAN (see TS 33.401 [2]) except that it is bound to the device (more specifically, the *device_root_key*) as well to the $\mathrm{K}_{\mathrm{ASME}}$ resulting from EPS AKA authentication. If the network receives a valid *device_response*, the network also calculates K_{ASME_D}.

The calculation of *device_challenge*, *device_response* and K_{ASME_D} are as follows:

$$device\_challenge = E_{device\_root\_key}\ (device\_temp\_key),\ network\_nonce$$

where $E_K(data)$ means *data* encrypted with key *K*, and *network_nonce* is a 128-bit random number chosen by the network. The *device_temp_key* is a 256-bit random number chosen by the network.

Both the Relay Node and MME keep *device_temp_key* while it has an EPS security context whose K_{ASME_D} was derived from it. This means that $E_{device\_root\_key}\ (device\_temp\_key)$ is optional to send in the case that the MME knows the current EPS NAS security context being used by the Relay Node has a K_{ASME_D} as root key and hence the Relay Node has a *device_temp_key* stored and the MME is willing to re-use that key.

device_response is calculated as

$$device\_response = device\_nonce,\ device\_res$$

where *device_nonce* is a 128-bit random number (e.g., 128 bits) chosen by the device; and *device_res* is a 128-bit number that is calculated as follows:

$$device\_res = \mathrm{KDF}\ (device\_temp\_key,\ network\_nonce \parallel device\_nonce)$$

where KDF is a suitable pseudo-random function.

Finally, the calculation of K_{ASME_D} is as follows:

$$K_{ASME\_D} = \mathrm{KDF}\ (device\_temp\_key \parallel K_{ASME},\ network\ nonce \parallel device\_nonce)$$

where K_{ASME} is the one freshly generated as part of the EPS AKA authentication. Note that the device authentication process here is running in the same NAS messages as those used for the AKA procedure.

K_{ASME_D} is treated same as the K_{ASME} in E-UTRAN, except that K_{ASME_D} is bound to the Relay Node device authentication and the EPS security context resulting from $\mathrm{K}_{\mathrm{ASME\_D}}$ is always stored in the Relay Node and not on a UICC.

10.5.2.2.2 Security Analysis

From the DeNB and rest of the network's perspective, the Relay Node has been successfully authenticated and hence it is acceptable to authorise the DeNB to enable relay functionality, e.g. to send user keys to the Relay and allow it to send/receive user data.

The Relay Node is effectively a slave of the DeNB and network, and it can only serve users for whom the network provides keys. Because of this, there are no security concerns for the Relay Node regarding sending data to a network which has provided the keys used to communicate with that user.

The authentication of the Relay Node in the E-UTRAN signalling happens by the Relay Node being able to successfully decrypt the *device_temp_key* that was sent to it by the MME. From this the MME and RN generated a root key for a new EPS security context using the exchanged nonces. This protocol follows the use of RSA Key Exchange in TLS[6]

Like RSA Key Exchange in TLS this protocol provides only authentication of the RN to the MME while authentication of the network to the RN is not ensured by cryptographic means without securing the UICC-RN interface as shown by the following observations:

The following analysis only applies when AS security is used to provide the integrity protection for S1-AP and X2-AP traffic. For a rogue network, it has to be assumed that the attacker has control over the network entity to which the RN is attaching. Furthermore, in the threat scenarios in clause 2, it is assumed that the attacker may have control over an unprotected interface between RN and UICC, cf. e.g. the text for threat 2 "…taking a real UICC from a real RN and replacing it with a fake UICC for which the attacker has the root key" or threat 5 "Attacks on the interface between the RN and the UICC". Under these assumptions, the protocol in solution 5 does not even have the weaker network authentication properties of UMTS AKA (as described in clause 5.1.2 of TS 33.102 [14]), as can be inferred from the following observations.

The protocol described in clause 10.5.2.2.1 has no provisions for protecting the UICC-RN interface. This means that it may be assumed that an attacker having access to this interface can transfer keys to the RN over this interface without the RN having the possibility to verify the origin of these keys. Or, as a minimum, it may be assumed that eavesdropping on the UICC-RN interface is possible.

The formula in clause 10.5.2.2.1 for the new intermediate EPS key, from which all keys for AS and NAS protection are ultimately derived, is:

$$K_{ASME\_D} = \mathrm{KDF}\ (\mathit{device\_temp\_key} \mid\mid K_{ASME}\ , \mathit{network\ nonce} \parallel \mathit{device\_nonce})$$

Network_nonce and device_nonce are public information. By our assumptions, the attacker controlling a (rogue) network entity to which the RN is attaching can know K_{ASME} by eavesdropping on CK, IK sent on the interface between UICC and RN. So, the only value the attacker needs to know in addition for being able to compute K_{ASME_D} is *device_temp_key*. This parameter *device_temp_key* is sent to the RN as part of the *device_challenge* encrypted as $E_{device\_root\_key}$ *(device_temp_key, A)*, where the additional input A is the old *device_temp_key* if the authentication is not part of the attach procedure and is the empty string otherwise. Hence, as the *device_root_key* is the public key of the RN and thus known to the attacker, the attacker can choose a *device_temp_key* of his own and send it to the RN in a *device_challenge* in attach procedures. For non-attach procedures, he needs to additionally know the old *device_temp_key*. Then the attacker can compute K_{ASME_D} and impersonate a genuine network. The attacker has two possibilities for obtaining the EPS AKA challenge RAND || AUTN to be sent to the RN from the rogue network: if the attacker can only eavesdrop on the UICC-RN interface the attacker obtains a valid RAND || AUTN from a genuine network in a response to an unprotected RN attach request; if the attacker can fully control the UICC-RN interface he can choose any challenge RAND || AUTN and transfer any keys CK, IK to the RN over the UICC-RN interface under his control.

The root cause of this lack of network-to-RN authentication seems to be that the public key-based part of the protocol from clause 7.6.2.2.1 provides only RN-to-network authentication while EPS AKA, which does provide mutual authentication, is executed on the UICC, which is not securely bound to the RN platform. In more detail: the *device_challenge* lacks freshness and origin authentication. The EPS AKA challenge RAND || AUTN has both, freshness and origin authentication, through the use of the sequence number and the MAC. However, this does not help to guarantee network-to-RN authentication because SQN and MAC in EPS AKA can only be checked by the UICC on behalf of the RN and the RN has no secure connection to the UICC.

The above attack scenario is only applicable for the case that AS security is used to integrity protect the S1-AP/X2-AP signalling. The threat identified for the case of using AS security to integrity protect the S1-AP/X2-AP traffic only relates to stealing the RN for use in another network and not on actually attacking user(s) connected to that RN.

In order to prevent the RN being stolen and used continually in a rogue network, the RN could be required to periodically attach to the management system in order to keep functioning as a RN.

10.5.2.2.3 Attach flow and rekeying E-UTRAN keys

The flow in figure 10.5.2.2.3-1 shows the Attach procedures for a Relay Node using NAS messages used for EPS AKA enhanced to support the device authentication as described in this contribution. It is assumed that presenting the device identity upfront will not lead to any privacy issues for relay nodes. This flow assumes that the RN has been already provisioned by the operator and has *device_credentials* that the MME will accept (more discussion of this issue is contained in the management of the RN section) but does not have an E-UTRAN security context that the MME is willing to use. The description of the flows only notes where the new IEs are sent.

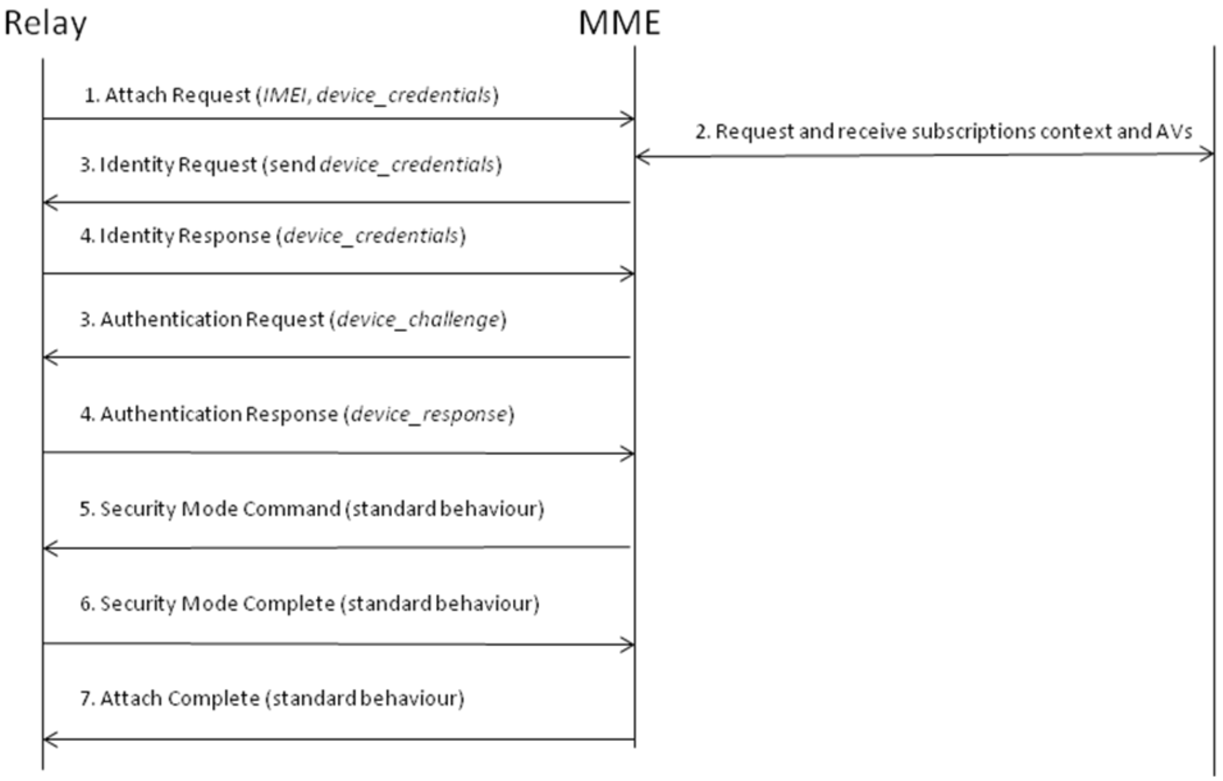

Relay
MME
1. Attach Request (*IMEI, device_credentials*)
2. Request and receive subscriptions context and AVs
3. Identity Request (send *device_credentials*)
4. Identity Response (*device_credentials*)
3. Authentication Request (*device_challenge*)
4. Authentication Response (*device_response*)
5. Security Mode Command (standard behaviour)
6. Security Mode Complete (standard behaviour)
7. Attach Complete (standard behaviour)

Figure 10.5.2.2.3-1: Enhanced AKA during an Attach procedure

1. Relay sends the Attach Request message
2. The MME requests the device's certificate in the Identity Request message
3. The RN sends its certificate to the MME in the Identity Response message
4. MME fetches RN subscription and authentication information from HSS
5. MME sends Authentication Request including *device_challenge*
6. Relay responds with Authentication Response including *device_response*. Relay and MME can also calculate K_{ASME_D} at this point
7. MME sends NAS Security Mode Command to start using the security context based on K_{ASME_D}
8. Relay responds with NAS Security Mode Complete
9. MME sends Attach Complete

When the MME wishes to re-key the E-UTRAN level keys, it uses the flow given in figure 10.5.2.2.3-2. The flow assumes that the MME already has the RN's device certificate.

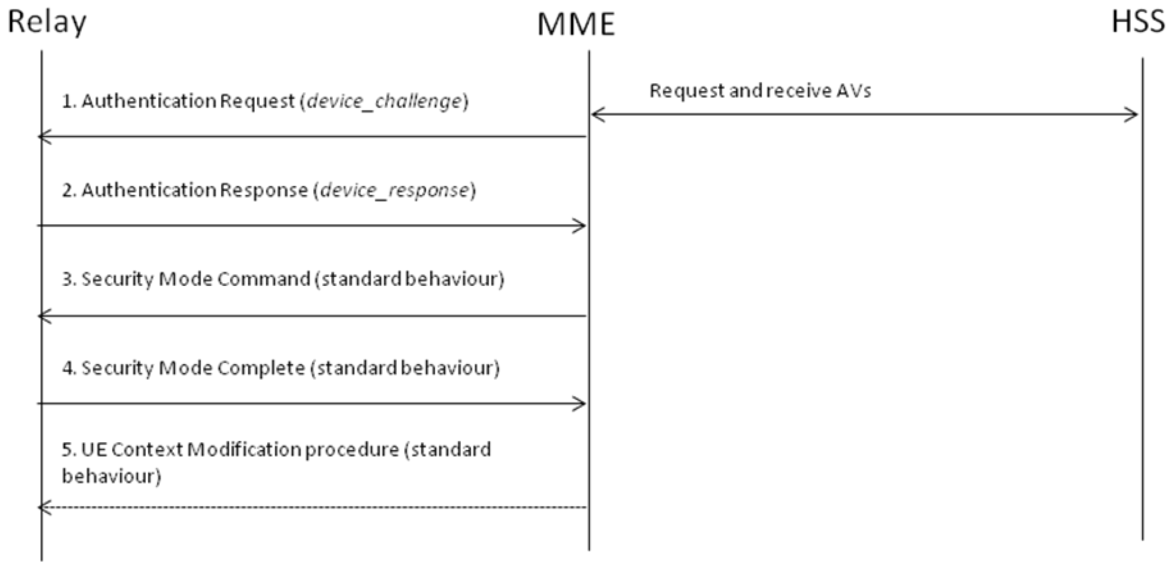

Relay
MME
HSS
Request and receive AVs
1. Authentication Request (*device_challenge*)
2. Authentication Response (*device_response*)
3. Security Mode Command (standard behaviour)
4. Security Mode Complete (standard behaviour)
5. UE Context Modification procedure (standard behaviour)

Figure 10.5.2.2.3-2: Rekeying using enhanced AKA

Steps 1 to 4 are the same as steps 5 to 8 above with the following exception:

- If the Relay Node's current EPS NAS security context has a K_{ASME_D} as it root key and the MME is willing to re-use that *device_temp_key* that generated K_{ASME_D} then $E_{device\_root\_key}$ *(device_temp_key)* is not included in step 4. In this case the RN and MME use the exisiting *device_temp_key* to generate the new K_{ASME_D}.
- Note: *network_nonce* is always included in step 1 and *device_nonce* is always included in step 2

Step 5: If the Relay Node has an established AS security context, then the MME initiates a UE Context Modification to change the AS level keys

10.5.2.2.4 Changes to NAS messages

The following changes will be needed to NAS messages to support this solution for Relay Nodes.

Authentication Request

Modified or new IE(s) to carry *device_challenge* = [$E_{device\_root\_key}$ *(device_temp_key)*], *network_nonce*

Authentication Response

Modified or new IE(s) for *device_response = device_nonce, device_res*

Identity Request:

Modified or new IE(s) to request the *device_credentials*, i.e. the device's certificate

Identity Response:

Modified or new IE(s) to carry *device_credentials*

1) NOTE: The requirement in this solution is for the device certificate to be available in the MME before the Authentication message is sent. This could be done using the above changes to Identity Request/Response or by some other method if CT1 prefers a different solution.

10.5.2.2.5 Profiles of Cryptographic Functions

RSA-OEAP as described in [5] is used to encrypt the *device_temp_key* when it is sent from the MME to the RN according to the following profile:

HASH function = SHA-256

The additional input A = empty string if the authentication is part of the attach procedure and the user authentication will be/ was sent unprotected and the old device_temp_key otherwise

For encryption, the MME-RN shall use the public key of the RN

For decryption, C is the $E_{device\_root\_key}$ *(device_temp_key)* that was sent to the RN

For decryption, the RN uses its private key

The generation of K_{ASME_D} and *device_res* shall use profiles the KDF used in TS 33.401 [2] as follows:

K_{ASME_D} = KDF(*device_temp_key* || K_{ASME}, *network_nonce*, *device_nonce*)

device_res = KDF(*device_temp_key, network_nonce, device_nonce*)

where || means concatenation

10.5.2.2.6 Error cases

In the case that the MME-RN considers the certificate provided by the RN to be unacceptable for access, the MME-RN shall reject the EPS attach request by the RN. This rejection shall not prevent the RN trying a phase I connection with the network.

If the RN receives a non-enhanced AKA challenge, i.e., one not including network_nonce, when it is trying to attach for a phase II connection or it receives an enhanced authentication challenge that was incorrect (e.g. the old device_temp_key included was incorrect), the RN shall respond with the error message to indicate an incorrect enhanced authentication.

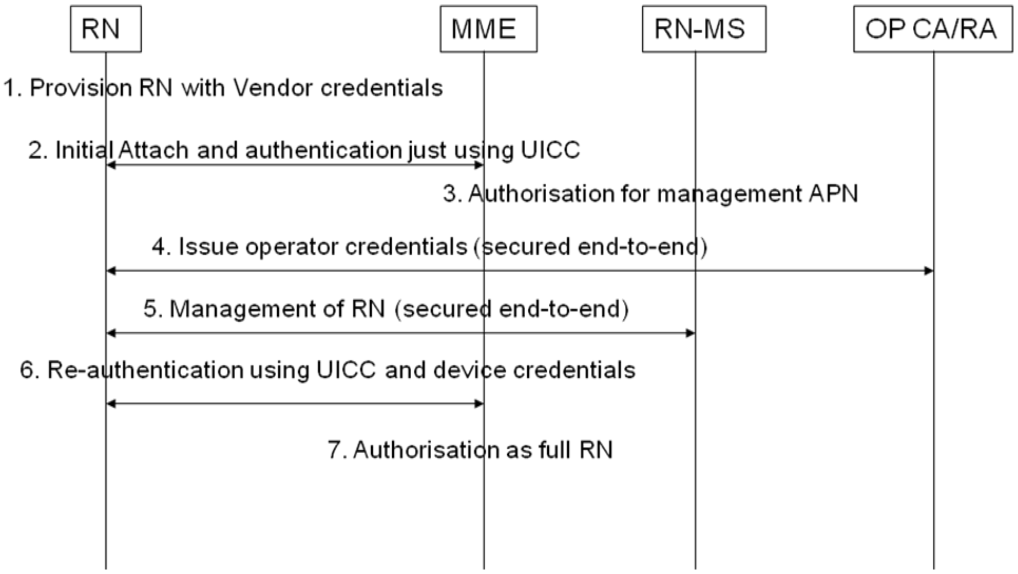
If the MME receives an incorrect device_res from the RN, it shall treat the RN as though it has returned an incorrect RES (i.e., it may re-try authentication after checking it had the correct parameters for the RN before sending an authentication reject to the RN). This rejection shall not prevent the RN from trying a phase I connection with the network.

10.5.3 UICC Aspects in RN scenarios

A standard UICC could be used and as the K_{ASME_D} is bound to the Relay Node, then there is no need to protect the Relay Node to UICC interface.

10.5.4 Enrolment procedures for RNs for backhaul link security

An advantage of this proposal comes in the management of the Relay Node. It is shown in the below call flow that a Relay Node can be managed exactly like any other eNB. This is achieved by allowing the Relay Node access to the management boxes based on the EPS AKA credentials only and then issuing a certificate for the *device_root_key*. The below flow assumes that the RN does not have a *device_credential* that the MME is willing to accept (e.g., device only has vendor credentials, but the network requires the operator issued credentials).


RN
MME
RN-MS
OP CA/RA
1. Provision RN with Vendor credentials
2. Initial Attach and authentication just using UICC
3. Authorisation for management APN
4. Issue operator credentials (secured end-to-end)
5. Management of RN (secured end-to-end)
6. Re-authentication using UICC and device credentials
7. Authorisation as full RN

1. The Relay Node is provisioned with manufacturer- or vendor-supplied credentials.
2. The Relay Node and MME performs a standard EPS AKA, just as a normal UE would, i.e. at this stage the Relay Node does not have a *device_credential* the MME is willing to accept.
3. The subscription information retrieved by the MME indicates that the authenticating UE is actually a Relay Node. As a result, the MME authorizes the RN to only sets up a bearer to allow the Relay to communicate with management nodes.
4. The Relay Node uses the credentials provided in step 1 to authenticate to the operator CA/RA and set up a secure connection with it. The operator CA/RA creates any associated certificates and sends them to the Relay Node over this secure connection.
5. The Relay Node connects to an OA&M node for further configuration and provisioning. Once the management operators are completed, the OA&M system may issue a management command to re-attach/restart the Relay Node.
6. The Relay Node and MME performs a re-authentication using the enhanced device authentication as described above.
7. The MME authorizes the Relay Node to provide service to UEs.

10.5.5 Analysis of Solution 5

10.5.5.1 How does solution 5 address the threats in clause 5?

Threat 1: Impersonation of a RN to attack user attached to RN

All secure tunnels from the RN are established using some form of device authentication, hence it is not possible to impersonate a RN

Threat 2: MitM on the Un interface between RN and DeNB

All secure tunnels from DeNB to RN in solution 5 are known to terminate in a valid RN as the RN is device authenticated when establishing such tunnels. Hence it is not possible to insert a MitM between the DeNB and RN

Threat 3: Attacking the traffic on the Un interface between RN and DeNB

Integrity protection of S1-AP and X2-AP signalling across the Un interface is provided by an IPsec security association or enhanced AS security between RN and DeNB. Other traffic over Un is sufficiently protected by AS security.

Threat 4: Impersonation of a RN to attack the network

The RN is device authenticated as it attaches to the network.

Threat 5: Attacks on the interface between the RN and the UICC

The security of solution 5 does not rely on the security of any traffic passed across this interface

Editor's Note: the lack of protection of the UICC-RN interface is one of the causes for the lack of network-to-RN authentication in the case of using AS security for integrity protecting the S1-AP and X2-AP messages. It is ffs whether the lack of network-to-RN authentication leads to relevant threats.

Threat 6: Control of the RN platform

This threat is prevented by autonomous validation and device authentication.

Threat 7: DoS type attacks

The description of this threat has two parts:

a) From clause 5.3: "When the attacker removes the USIM, RN without USIM can't be authenticated by the network. So the legal RN can't connect to network and provide services."
Response: An attacker removing a USIM could just as easily physically destroy the RN so this type of DoS cannot be prevented.

b) From clause 5.3: "The attacker could also insert the USIM into another RN, then the topology of access network will be changed and cause interference problem to other eNB."
Response: The threat is not completely clear but solution 5 could bind a USIM with a RN in the MME as the MME authenticates both these entities.

10.5.5.2 How does solution 5 fulfil the requirements in clause 6?

We quote text from clause 6.

"If end to end protection between the RN and the core network is needed, then the same solution as for backhaul protection should be considered."

Response: But e2e protection is not possible due to the chosen architecture alternative, as stated in the next paragraph, so this sentence should be removed.

"Integrity protection for the S1 control plane traffic over the Un shall be mandatory."

Response: This is provided in solution 4 by the mandatory IPsec security association or enhanced AS security between RN and DeNB.

"The S1 control plane traffic between RN and MME-UE shall be integrity protected between the DeNB and the MME-UE with at least the same strength as in the current EPS architecture."

Response: This requirement seems compatible with all solutions described in clause 7. It is addressed as in clause 11 of TS 33.401 [2] today.

"Integrity protection for the X2 control plane traffic over the Un shall be mandatory. The X2 control plane traffic between RN and eNB/RN shall be integrity protected between the DeNB and the eNB/RN with at least the same strength as in the current EPS architecture."

Response: same as for S1 traffic.

"Mutual authentication between RN and network shall be supported."

Response: Mutual authentication between RN and MME-RN is provided by EPS AKA performed according to TS 33.401 [2].

Editor's Note: authentication from RN to MME-RN is provided. Network-to-RN authentication is not provided in the case that AS security is used to protect the S1-AP and X2-AP traffic.

"Relay device authentication is mandatory."

Response: solution 5 provides this during the E-UTRAN access

“The DeNB shall not accept or send S1-AP and X2-AP message from/to the RN until a successful Relay device authentication has happened.”

Response: this requirement seems compatible with all solutions described in clause 7.

“Security of RN Management shall be guaranteed.”

Response: this requirement seems compatible with all solutions described in clause 7. Either a separate TLS connection is set up to the OAM server, or, after the successful completion of the RN attach procedure, the management traffic is secured hop-by-hop

“The wireless resource: security shall be able to prevent misuse by identifying whether the attached terminal is a UE or a RN. The identification could be implicit.”

Response: Solution 5 prevents a UE acting like a RN as it will not be able to device authenticate the MME.

“The connection between relay and network should be confidentiality protected. Confidential protection for the S1/X2 user plane traffic over the Un should provide protection as same as the user plane data transferred on Uu interface, i.e. provide optional confidentiality protection on Un interface.”

Response: solution 5 uses IPsec or enhanced AS security for integrity of S1 and X2, and AS security otherwise.

“Both user plane and control plane must be considered as they may not require the same level of protection.”

Response: solution 5 satisfies this requirement.

“The RN platform shall protect from reading and/or modification of security parameters and security functions by unauthorized parties (platform security). The integrity of the RN platform shall be validated as part of the RN start up procedure.”

Response: solution5 requires platform integrity and device authentication as part of the start-up procedure.

“RN specific device security features, e.g. security storage of sensitive data, device integrity check, USIM aspects, shall be considered.”

Response: for secure storage and device integrity cf. the preceding response.

10.5.5.3 How does solution 5 address the general Editor’s notes and the residual threats in clause 8.1.2.1?

This clause is only appropriate if the version of solution 5 using IPsec to integrity protect the S1 and X2 signalling is chosen. We quote from clause 8.1.2.1.

“Editor’s Note: It needs to be clarified whether all traffic over the Un user plane, or only S1 signalling traffic, is to be protected by NDS/IP, e.g. for performance reasons. If the latter applies then appropriate mapping of parameters identifying S1 signalling traffic to IPsec selectors (IP addresses, ports, transport protocol) would have to be performed.”

Response: Solution 5 opts for protecting only S1 and X2 signalling traffic by means of IPsec. The traffic selectors are ffs, but are believed not to be a fundamental obstacle.

“Editor’s Note: The enrolment process for credentials to set up backhaul link security between RN and MME-RN, and RN and S-/P-GW-RN (i.e. distribution of IPsec certificates and set up of IPsec tunnel) needs to be studied.”

Response: the enrolment phase is taken care of in solution 5.

“Editor’s Note: The following is for further study: The donor eNB must know if a particular subscription is a RN subscription or a UE subscription so the donor eNB must know if it is authorised to pass S1-AP traffic to the RN. It requires further study whether this requirement can be supported using the current S1-AP protocol and/or core network procedures. Furthermore the donor eNB must know that it has to apply the Un security procedures which are by assumption different to the Uu procedures.”

Response: In solution 5, the MME authenticates the RN and hence can inform the DeNB to treat the RN as a RN.

“**Residual Threat:** threats of eavesdropping on and modification of traffic of DRBs is satisfactorily addressed by platform integrity and use of IPsec. As RRC traffic cannot be protected by IPsec it needs to be considered separately.

The main threat to RRC seems to be that an attacker modifies bearers on Un. This seems to be possible when an attacker knows the RRC integrity key.
Editor's Note: threats to AS security for RRC over Un need further study. In particular: how can an attacker obtain knowledge of the RRC integrity key? "

Response: in solution 5 the attacker cannot obtain the RRC integrity key.

"**Residual Threat:** neither RRC nor UP-UE traffic are protected by IPsec. (UP-UE = user plane data sent by UE.) In addition to the remarks made on RRC in 5.1.2.1.2.1, the attacker could eavesdrop on UP-UE. An attacker could e.g. fraudulently establish an RN-DeNB radio connection via a MitM as described for threat 2 in section 1.
Depending on the way in which the attacker obtains knowledge of the keys it may not be enough to ascertain that the IPsec SAs and AS security have the same endpoints, i.e. that all security tunnels from the RN terminate in the real network instead of in a MitM node may not be sufficient. It may neither be sufficient to bind the USIM to the RN, e.g. by using EAP-AKA inside IKEv2 in the way done for HeNBs.
Editor's Note: threats to AS security for RRC and UP-UE over Un need further study."

Response: in solution 5 the attacker cannot obtain the UP-UE encryption key.

10.5.5.4 How does solution 5 address the general Editor's notes and the residual threats in clause 8.1.2.2?

This clause is only appropriate if the version of solution 5 using enhanced AS security to integrity protect the S1 and X2 signalling is chosen. We quote from clause 8.1.2.2.2.

"**Residual Threat:** as already noted in 8.1.1, integrity protection of S1-UE is required, but can be only guaranteed if the AS security mechanisms on Un are modified with respect to Uu as Uu does not provide integrity on DRBs. Furthermore, all threats that apply to RRC and UP-UE in case 5.1.2.2.2 now apply to all traffic over Un."

Response: in solution 5, the attacker cannot obtain the RRC integrity key or the UP-UE encryption key.

10.5.5.5 Analysis of solution 5 not related to threats

In this solution, it modified the LTE existing attach procedure. A device-credential (either the device certificate or a pointer to it (e.g., *device_identity*)) is used binding with IMSI. The authentication request/response message should be extended to take device_chanllenge and device_response, So there are some impacts on original attach procedure and Solution 5 implies the following changes to the NAS signalling:

1. Additional message exchanges are needed for the certificate validation

2. The authentication message should be specific and different with original authentication request/response. It also changes signaling in attach procedure.

3. The MME has to generate random number to calculate device_challenge and K_{ASME_D}. It modifies key generation function in attach procedure.

Editor's note: The acceptability of the NAS changes need to be checked

10.6 Solution 6: AKA for Relay Node UE authentication and secure channel between RN and USIM

10.6.1 General

In this solution, AKA is performed for mutual authentication between Relay Node and core network, which generate keys for AS communication and IP communication. Certificate based IKE authentication is not needed. IPsec is used to protect the S1 and X2 control plane signalling. The user plane traffic will be protected by the AS level security.

10.6.2 Security Procedures

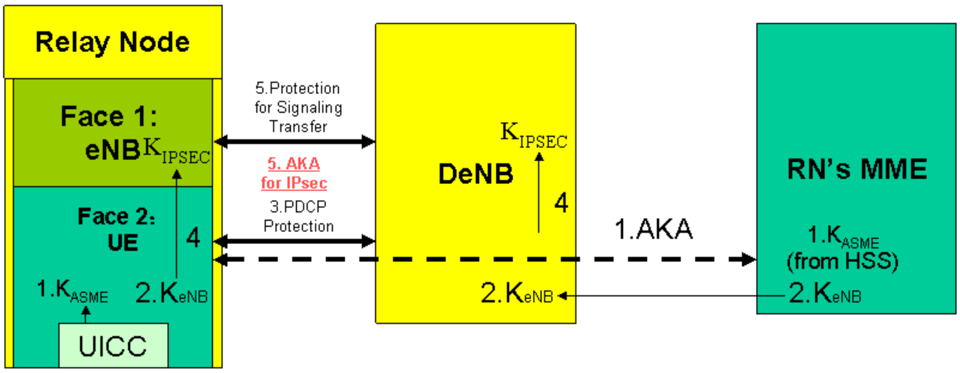


Figure 10.6.2-1: AKA for IPSec

The EPS AKA procedure is run to authenticate the UICC in the Relay Node and core network as shown in the figure above.

1. When RE connects network as a legacy UE, AKA shall be performed, and K_{ASME} is generated by Relay Node and its HSS. MME will get K_{ASME} from HSS.

2. RN and MME generate the K_{eNB} independently, MME send the K_{eNB} to DeNB, then both RN and DeNB share K_{eNB} and related keys like K_{RRCenc}, K_{RRCint}, etc.

3. SMC negotiation is complete between RN and core network. And PDCP bearer will be generated and protected

4. A special K_{IPSEC} will be generated by K_{eNB} in RN and RN's DeNB simultaneously. A new K_{IPSEC} will be generated when K_{eNB} has rekeyed.

5. IPsec protection can be established between RN and DeNB by using K_{IPSEC}.

Editor's note: How the other parameters for the IPsec connection are established is FFS

After that, AS security communication and IPsec communication are all set up. Then AS security can be used to protect user plane data and IPsec can be used to protect control plane data between RN and DeNB.

10.6.3 UICC Aspects in RN scenarios

It uses the USIM, and there are the following ways to make sure it is secure binding between the USIM and RN.

Secure channel mechanism shall be used between the UICC and the Relay Node as described in ETSI TS 102 484 [12]. A pre-shared key can be pre-installed into RN automatically or by using GBA.

10.6.4 Enrolment procedures for RNs for backhaul link security

Editor's note: Enrollment procedures are FFS

10.7 Solution 7: AKA for Relay Node UE authentication and IPSec protection

10.7.1 General

In this solution, AKA is performed for mutual authentication between Relay Node and core network, and generate keys for AS communication and IP communication. IPsec is used to protect the S1 and X2 control plane signalling. The user plane traffic will be protected by the AS level security. We use IKE and AKA key will be used as the pre-shared key to the IKE, because it can provide more dynamic configuration and negotiation on the security parameters.

Solution 7 actually includes secure channel (PSK) + IPsec tunnel (PSK).

10.7.2 Security Procedures

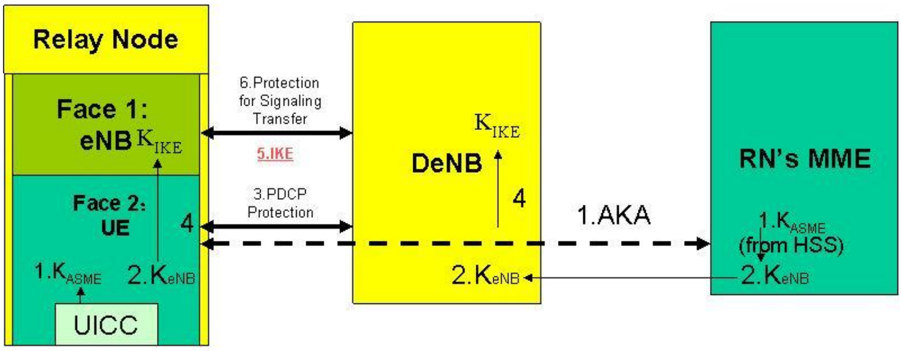


Figure 10.7.2-1: AKA for IKE

The EPS AKA procedure is performed to authenticate the UICC in the Relay Node and core network.

1. When RN connects network as a legacy UE, AKA shall be performed, and K_{ASME} is generated by Relay Node and its HSS. MME will get K_{ASME} from HSS. At the same time, RN provide "I'm an RN" indicator to DeNB.
2. RN and MME generate the K_{eNB} independently, MME send the K_{eNB} to DeNB, then both RN and DeNB share K_{eNB} and related keys like K_{RRCenc}, K_{RRCint}, etc.
3. NAS SMC negotiation is complete between RN and core network at first. Then a special AS SMC negotiation should be performed between RN and DeNB. As DeNB received "RN" indicator in step 1, it can derive a special key Kup_int for user data integrity protection based on K_{eNB} and send a special security mode command with additional algorithm selected for UE's UP integrity. RN derives this Kup-int as well and apply selected algorithm on UE's UP integrity protection. As a result, PDCP bearer will be generated and protected
4. A special K_{IKE} will be generated from K_{eNB} in RN and RN's DeNB simultaneously.
5. The key K_{IKE} can be used for IKE authentication pre-share key instead of certificate.
6. A standard IKE negotiation procedure with pre-share key can be performed. IPsec tunnel will be generated by IKE and protection will be activated. What is more, IPsec can be updated by using standard IKE procedure.

After that, AS security communication and IPsec communication are all set up. Then AS security can be used to protect user plane data and IPsec can be used to protect control plane data between RN and DeNB.

10.7.3 UICC Aspects in RN scenarios

It uses the USIM with the following way to make the secure binding between the USIM and RN.

Secure channel mechanism shall be used between the UICC and the Relay Node as described in ETSI TS 102 484 [12].The UICC shall not disclose AKA related sensitive information before the secure channel establishment. The mechanism can be applied as below.

1. A pre-shared key can be pre-installed into RN.

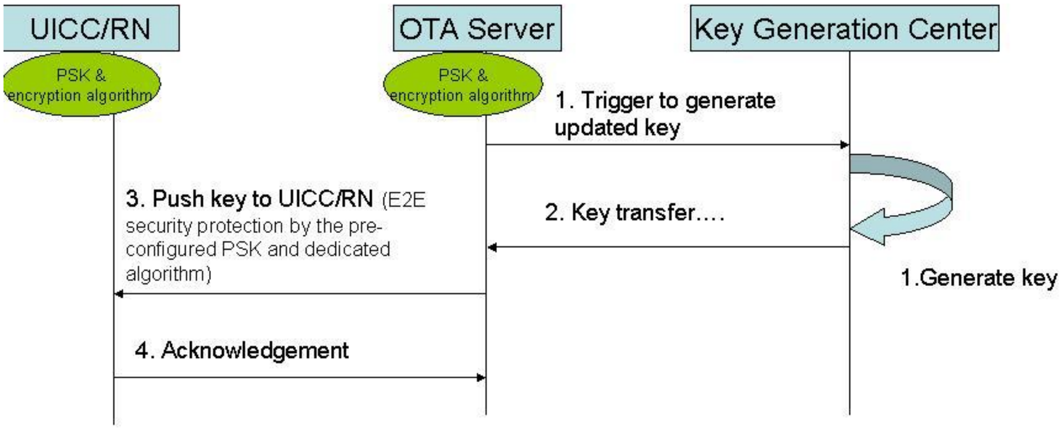
10.7.4 Pre-shared Key Enrolment procedures for RNs for backhaul link security

Before the RN and UICC are deployed, a pre-shared key will be generated and installed in RN and UICC manually.

If re-key of the PSK is necessary, OTA mechanism can fulfill the update as below.

- The update can be performed as following: Firstly OTA server triggers the key generation center to generate the updated PSK. Secondly, this key is transferred to OTA server which is also inner operator's domain. Thirdly, OTA server can initiate the key transfer to the RN and UICC. Fourth, RN/UICC confirms the update. This mostly happens at the application layer. It can be executed in this 3GPP scope.

NOTE: this update does not happen frequently, it is only performed when necessary.


UICC/RN
OTA Server
Key Generation Center
PSK & encryption algorithm
PSK & encryption algorithm
1. Trigger to generate updated key
1.Generate key
2. Key transfer....
3. Push key to UICC/RN (E2E security protection by the pre-configured PSK and dedicated algorithm)
4. Acknowledgement

- As for the protection on the OTA messages, at the very beginning, a shared pre-configured key or certificate can be installed between UICC and OTA server as well as the same requirement between RN and OTA server. A pre-defined algorithm was selected and implemented in all related devices. After that, the key can be transferred from OTA server to UICC securely and OTA transmissions can be protected. E2e security protection based on the pre-configued PSK or equipment certificate can be applied.

The relevant standard here can check OTA standard 3GPP TS 31.116 [9] which have defined all the commands and modules. It uses the same commands and modules to the terminal in this solution.

And the procedures above can be based on the platform validation or integrity check which has certificate to make sure this device security. But platform validation is independent procedure and shall be applied into every solution. So here it is not described.

10.7.5 Analysis of Solution 7

10.7.5.1 Countermeasures for the threats in clause 5

1) Impersonation of a RN to attack user attached to RN

As this attack will be perfomed by removing the UICC from a real RN and inserts it into their own Rogue RN, and the objective is to perform the device authentication for this threat. But Solution 7 uses secure binding between the UICC and device. So this attack can be prevented by the secure channel between UICC and RN, the legal UICC can't be inserted to another RN. So this attack can't be made.

2) MitM on the Un interface between RN and DeNB

This attack can also prevented by the following ways. Firstly, there is secure channel between UICC and RN. A UICC for RN can only be inserted into a specified RN. In this situation, attacker can't get root key by fake RN. Secondly, there is keys negotiation closely associated with RN authentication to be used to the integrity and encryption of IPSec or AS. So there will be no MitM attack.

3) Attacking the traffic on the Un interface between RN and DeNB

RN's AS level security is provided to protect RN's singling and User's user plane data. IPsec security is used to provide integrity protection of User's Control plane signaling.

4) Impersonation of a RN to attack the network

Same to 1)

5)Attacks on the interface between the RN and the UICC

This attack can be eliminated by binding between UICC and the RN.

6)DoS type attacks

For DoS attacking that attacker inserts the UICC into another RN to cause the interference problem, it can be prevented by secure channel between UICC and RN(binding).

10.7.5.2 How does solution 7 fulfil the requirements in clause 6

1)"If end to end protection between the RN and the core network is needed, then the same solution as for backhaul protection should be considered."

> *For User UE 's S1 and X2 interface, hop by hop protection is used, so this requirement is not applied for these interfaces. For OAM communication, e2e protection is used. Mutual authentication between RN and OAM system is required. This requirement is fulfilled.*

2) "Integrity protection for the S1 control plane traffic over the Un shall be mandatory."

IPsec is used to provide integrity protection for S1 control plane traffic over Un.

3)"The S1 control plane traffic between RN and MME-UE shall be integrity protected between the DeNB and the MME-UE with at least the same strength as in the current EPS architecture."

It can be addressed by TS 33.401 [2].

4)"Integrity protection for the X2 control plane traffic over the Un shall be mandatory. The X2 control plane traffic between RN and eNB/RN shall be integrity protected between the DeNB and the eNB/RN with at least the same strength as in the current EPS architecture."

It is addressed by TS 33.401 [2].

5)"Mutual authentication between RN and network shall be supported."

Mutual authentication between UICC(binding with RN) and network is supported.

6) "The DeNB shall not accept or send S1-AP and X2-AP message from/to the RN until a successful Relay device authentication has happened."

This requirement seems compatible with all solutions described in clause 7.

7)"Security of RN Management shall be guaranteed. RN should have separate security model for OAM configuration data."

Solution 6 does not deal with OAM security. So we meet this requirement .

8)"The wireless resource: security shall be able to prevent misuse by identifying whether the attached terminal is a UE or a RN. The identification could be implicit."

There are some solutions to prevent misuse which are described in section 8.1.2.1.1. Although there is no final decision to select which solution should be used, all these solutions can be used to resolve this requirement.

9)"The connection between relay and network should be confidentiality protected. Confidential protection for the S1/X2 user plane traffic over the Un should provide protection as same as the user plane data transferred on Uu interface, i.e. provide optional confidentiality protection on Un interface."

AS level security mechanisms are used in this solution to protect S1/X2 user plane traffic confidentiality.

10)"Both user plane and control plane must be considered as they may not require the same level of protection."

It has been considered.

10.7.5.3 Benefits of PSK based IPsec tunnel in solution 7

In solution 7, IPsec tunnel is used to protect the S1 and X2 control plane signalling. And it uses IKE mechanism and AKA key (KeNB) will be used as the pre-shared key to the IKE. There are many benefits using PSK (KeNB) mechanism to establish the IPsec secure tunnel.

From the point of cost, RN and DeNB use KeNB which is from AKA as the pre-shared key to establish the IPsec tunnel, so it does't need to add new mechanisms to provide other kind of preshared keys (e.g. GBA) or certificates for the establishment of IPsec. Because KeNB can be updated by performing an intra-eNB handover when it is needed, there is no need to add new mechanisms to update pre-shared key (KeNB) for IKE. So it reduces device complexity.

Besides, when compared to certificates based IPsec establishing method, there is no need to make certificates validation with CRL or OCSP for KeNB during IKE.

10.8 Solution 8 – Enhancing AKA to include device authentication via symmetric key in RN and HSS/MME

Editor's Note: Entities affected by security for relays (e.g. termination points of security protocols, entities with additional relay-related functionality) should be considered

10.8.1 General

In this solution, either IPsec or enhanced AS security is used to protect the control plane signalling. However, this solution is optimal for use with enhanced AS security, as the AS security context to be used to protect the PDCP layer is not made available on any of the relay-node physical interfaces (i.e. the interface with the UICC). The user plane traffic will be protected by the AS level security with the authentication procedures enhanced between the network and RN in order to provide mutual authentication based on credentials stored on the RN.

10.8.2 Security Procedures

10.8.2.1 General

Using either IPsec exactly as for eNBs as described in clause 11 of TS 33.401 [2] or enhanced AS security to protect the S1-AP/X2-AP interface between the RN and DeNB will prevent attacks 1, 3 and 4b. The overhead caused by the IPsec would be negligible as there is little signalling compared to user plane traffic, however, this little overhead can still be avoided if enhanced AS security is used (i.e. using integrity protection of S1 and X2 signalling in the PDCP layer).

The user plane data is protected by the AS level security. In 10.8.2.2, the EPS AKA procedure is extended and run to mutually authenticate the UICC in the RN and the network (RN subscription authentication), and to authenticate the RN device to the network (RN platform authentication). The enhanced AKA run also provides the keying material for the AS level security. This would prevent threats 2, 4c and 4d, but without further security mechanisms, threat 5 could be used to launch similar attacks.

In 10.8.2.3, an improvement with enhanced authentication data is proposed: the enhanced authentication data are protected with the secret key of the RN platform, so that the authentication data used in the AKA procedure can not be got by false RN.

No changes in NAS messages and interface and any other signalling messages and interface are needed to run this enhanced authentication procedure.

NOTE: some changes are still needed on the key derivation procedures run in the relay node and the HSS.

10.8.2.2 Enhanced EPS-AKA using a relay-node device secret key

Editor's note: More analysis of the security of the proposed solution is needed

In order to authenticate the relay-node platform in addition to the RN subscription during the attachment of the relay to the network, the following enhancement can be made to the existing EAP-AKA procedure.

A device symmetric secret key K_{relay} must be securely stored in the relay device and in the network side (HSS or MME-RN).

Editor's note: More details on the provisioning of K_{relay} is needed

This key can be used to sign the authentication challenge RAND and derive further the (expected) response to the authentication challenge (X)RES and the EPS master session key K_{ASME} with a suitable Key Derivation Function, such as the KDF defined in TS 33.220 [11].

- RES_{relay} = KDF(K_{relay}, RAND || RES || IDx || … other parameters …) in the relay node, IDx being the specific identifier for this KDF.
- Same derivation procedure should apply to $XRES_{relay}$ to obtain XRES_relay in the MME-RN or HSS.
- K_{ASME_relay} = KDF(K_{relay}, K_ASME || IDy || … other parameters …) in the relay node and the MME-RN or HSS, IDy being the specific identifier for this KDF

The RES_{relay} should then be truncated in order to fill in the NAS message format already defined for transporting the standard RES value. This value would be compared to a truncated $XRES_{relay}$ in the MME-RN. KDF identifiers, IDx and IDy, the authentication challenge RAND and the USIM response RES, K_ASME and possible other parameters (such as AUTN) should be used in order to diversify further these key derivation functions.

By signing the network authentication challenge RAND and USIM response RES with its own secret symmetric key $K_{relay,}$the RN platform is authenticated by the network in the same time than the RN subscription. After a successful authentication, the K_{ASME_relay} can be taken into use by the MME-RN and the relay to generate the full EPS key hierarchy (with NAS and AS security contexts), as illustrated in the following figure where K_{relay} is handled by the MME-RN:

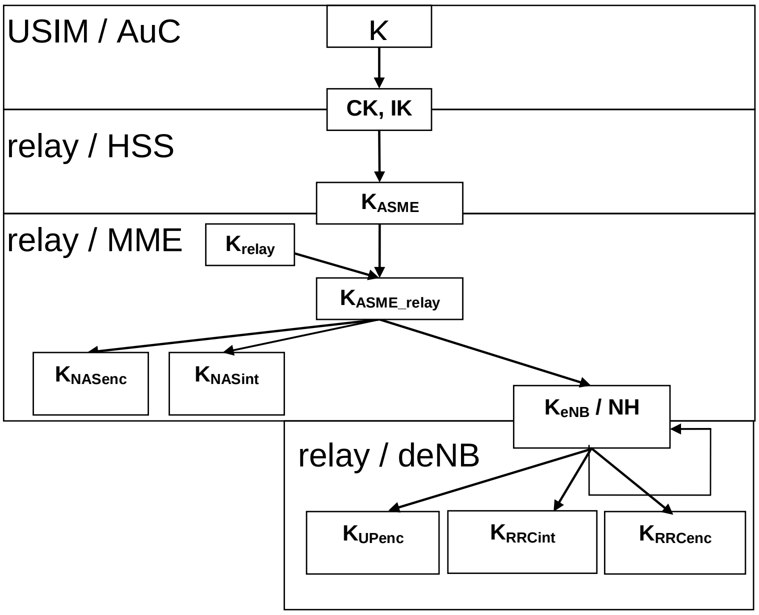


Figure 7.9.2.1-1: enhanced LTE key hierarchy using a relay device secret key

As an alternative, the K_{relay} can be handled in the HSS and the K_{ASME_relay} and XRES_relay can be generated in the HSS and the relay.

With this key hierarchy, NAS and AS security contexts benefit from the RN platform authentication in addition to the RN subscription (USIM) authentication and are not predictable from the keys provided by the USIM {CK, IK} on its interface with the relay node device. Furthermore, S1-AP, RRC and NAS messages will not need any changes as the carried information has exactly the same format than with a standard EPS-AKA procedure.

10.8.2.3 Improvement using enhanced authentication data

Editor's note: the *K_platform* in this section corresponds to the K_{relay} of previous section 10.8.2.2

In order to generate the enhanced authentication data, a RN platform related security key *K_platform* is assumed to be shared between RN platform and the HSS. And the enhanced the authentication data e.g. enhanced *RAND*, *AUTN* or K_{ASME} can be generated in HSS.

Further clarification for *K_platform*:

1, as one of the example, the *K_platform* can be pre-shared key between HSS and RN, and in HSS it can be indexed by the RN equipment identity e.g. IMEI.

2, as another example, assume HSS has the certificate of RN and the HSS holds the public key, the *K_platform* can be a nonce generated by HSS, HSS encrypt the *K_platform* and send it to RN, and the RN decrypts the *K_platform*.

Figure 10.8.2.3-1 illustrates the security procedure of the alternative enhancing AKA to include device authentication via symmetric key in RN and HSS/MME.

At the beginning of the EPS-AKA, the HSS conceals the EPS authentication data with *K_platform*, and generates the enhanced authentication data, i.e. *eRAND*, *eAUTN* and eK_{ASME}:

$eRAND = E_{K\_platform}(RAND)$ and

$eAUTN = E_{K\_platform}(AUTN)$

where $E_{K\_platform}(RAND)$ means *RAND* encrypted with key *K_platform*, and $E_{K\_platform}(AUTN)$ likewise.

Then, the enhanced authentication data, (i.e. $eRAND\|\ XRES\|K_{AMSE}\|eAUTN$), are sent to the RN instead of the original authentication data (i.e. $(RAND\|\ XRES\|K_{AMSE}\|AUTN)$). It is expected that only the real RN platform can unconcealed the initial authentication data.

In this way, the network completes the RN subscription authentication and RN platform authentication together.

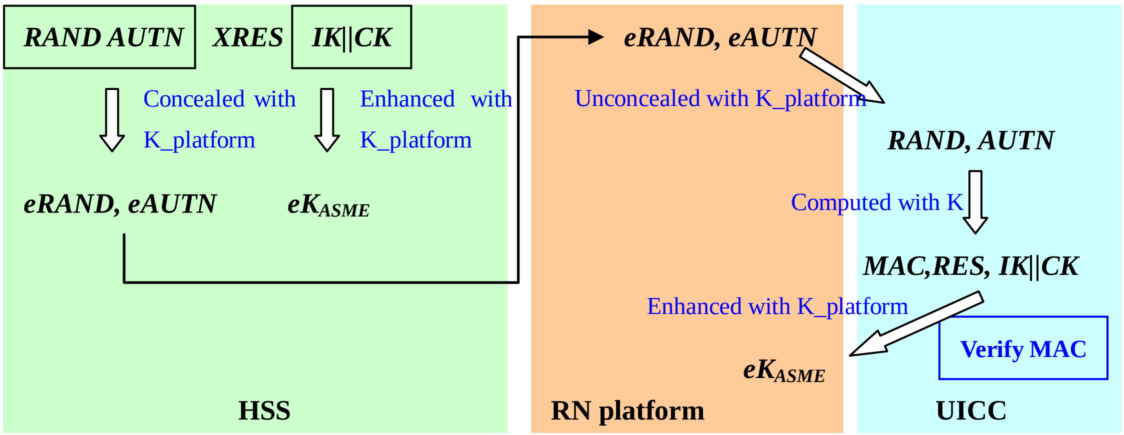


Figure 10.8.2.3-1. Authentication data enhancement

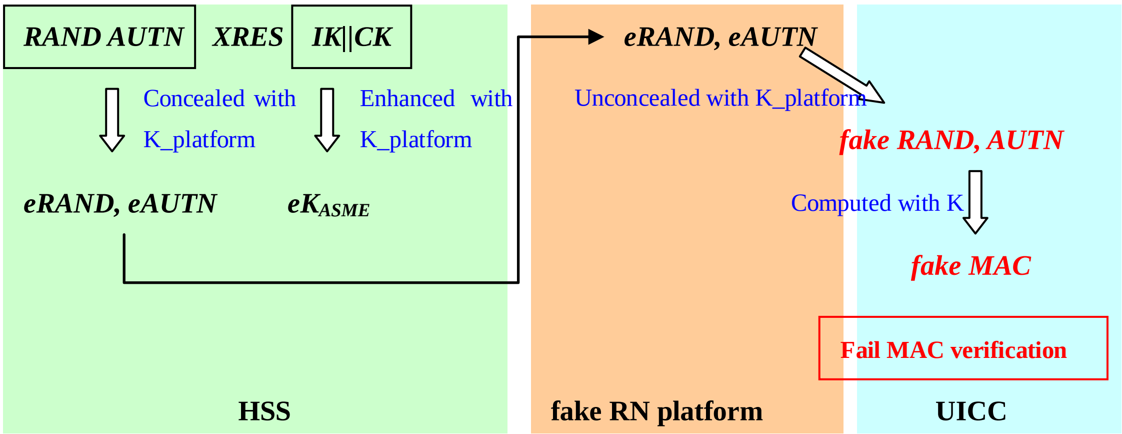


Figure 10.8.2.3-2. Authentication failure if UICC is inserted to a false RN

Moreover, the binding between EPS security key and the RN platform security key (e.g. *K_platform*) can also be done during this process. As an example, the enhanced intermediate key eK_{ASME} can be derived based on *IK*||*CK* and *K_platform*:

$$eK_{ASME} = \mathrm{KDF}(K\_platform,\ \mathrm{CK}\|\mathrm{IK} IK||CK,\ SN\ ID)$$

Just as shown in figure 10.8.2.3-3. Then, the eK_{ASME} can be used to derive the other AS or NAS keys just like a normal K_{ASME}. With this enhancement, the MitM threat can be eliminated, because the attacker can not predict the RN platform key.

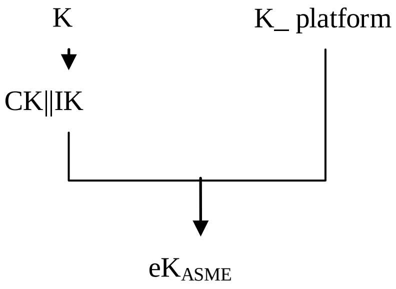


Figure 10.8.2.3-3. Key Binding

This solution has some advantages as following:

1. It is backward compatible, and no modification is needed for current EPS AKA procedure.
2. It can save the signalling overhead and latency, because that the RN platform authentication and key binding can be done in one procedure, and no other additional procedure is needed.

according to TS24.301 [10], the UICC will first verify MAC and then derive K_{ASME}. If before EPS-AKA the UICC is inserted to a false RN, the false RN which does not hold *K_platform* can not get *RAND* and thus the UICC will not send *IK*||*CK* to RN, it can prevent false RN from getting *IK*||*CK* and predicting further K_{ASME}.

10.8.3 UICC Aspects in RN scenarios

Editor's Note: A UICC in a UE provides security under quite different assumptions from a UICC in an RN. What would happen if a UICC was removed from a genuine RN and inserted into a false RN? Is binding of USIM and RN in some way required? This should be considered.

In the solution proposed in 10.8.2.1, the USIM is a standard one. Its use must be associated with the relay device secret key K_{relay} in order to authenticate the relay device toward the network. No specific binding is required for the UICC interface.

10.8.4 Enrolment procedures for RNs for backhaul link security

This is FFS as it is not yet known whether the same credentials can be used at the IKE and E-UTRAN layer.

10.8.5 Analysis of solution 8

10.8.5.1 How does solution 8 address the threats in clause 5.3?

Threat 1: Impersonation of a RN to attack user attached to RN

Response: threat 1 can be countered by device authentication. Solution 8 provides device authentication via enhanced AKA procedure. With this solution, only the real RN platform could send back the valid RES/RESrelay and complete the enhanced AKA procedure successfully. So this attack can be prevented.

Threat 2: MitM on the Un interface between RN and DeNB

Response: The solution 8 provides a key binding mechanism between the EPS key and a security key (e.g. Krelay /K_platform) which is related to RN platform. The RN platform related key is stored inside the RN secure environment, and the MitM node can not access it. So the solution 8 guarantees all security tunnels from the RN terminate in the real network instead of in a MitM node.

Threat 3: Attacking the traffic on the Un interface between RN and DeNB

Response: The solution use either IPsec exactly as for eNBs as described in clause 11 of TS 33.401 [2] or enhanced AS security to protect the S1-AP/X2-AP interface between the RN and DeNB.

Other user traffic over Un can also be protected by AS security or high level security, e.g. IPsec.

Threat 4: Impersonation of a RN to attack the network

Response: The RN platform is authenticated by the network as it attaches to the network. The impersonation will be shown up by the authentication when it try to access the network.

Threat 5: Attacks on the interface between the RN and the UICC

Response: since the RN platform authentication and the UICC authentication are performed together, the attacks on the interface will be detected during the authentication procedure. Hence the security of solution 8 does not rely on the security of any traffic passed across this interface.

Threat 6: Control of the RN platform

Response: This threat is prevented by autonomous validation and RN platform authentication.

Threat 7: DoS type attacks

The description of this threat has two parts:

a) "When the attacker removes the USIM, RN without USIM can't be authenticated by the network. So the legal RN can't connect to network and provide services."
Response: An attacker removing a USIM could just as easily physically destroy the RN so this type of DoS cannot be prevented.

b) "The attacker could also insert the USIM into another RN, then the topology of access network will be changed and cause interference problem to other eNB."
Response: If the other RN is a fake then the threat can be prevented just like the countermeasure to threat 1 and 3. If the other RN is real, solution 8 could bind a USIM with a RN in the MME and HSS as the MME and HSS authenticates both these entities. Furthermore, the threat can also be detected by the OAM when it try to access the configuration.

Threat 8: RN stays as UE after initial attach

Response: This solution can not solve the problem directly, but it can provide assistant authentication information when the network tries to differentiate the real RN and UE.

10.8.5.2 How does the solution 8 fulfil the requirements in clause 6.2?

We quote text from clause 6.2

"If end to end protection between the RN and the core network is needed, then the same solution as for backhaul protection should be considered."

Response: But e2e protection is not possible due to the chosen architecture alternative, as stated in the next paragraph, so this sentence should be removed.

"Integrity protection for the S1 control plane traffic over the Un shall be mandatory."

Response: Integrity protection is provided in this solution by the use of enhanced AS security or IPsec.

"The S1 control plane traffic between RN and MME-UE shall be integrity protected between the DeNB and the MME-UE with at least the same strength as in the current EPS architecture."

Response: This requirement seems compatible with all solutions described in clause 10. It is addressed as in clause 11 of TS 33.401 [2] today.

"Integrity protection for the X2 control plane traffic over the Un shall be mandatory. The X2 control plane traffic between RN and eNB/RN shall be integrity protected between the DeNB and the eNB/RN with at least the same strength as in the current EPS architecture."

Response: same as for S1 traffic.

"Mutual authentication between RN and network shall be supported."

Response: Mutual authentication between RN(which includes RN platform and UICC) and MME-RN is provided by the enhanced EPS AKA performed according to solution 8.

"Relay device authentication is mandatory."

Response: RN platform authentication is provided in this solution.

"The certificates used for the relay node device authentication shall be validated."

Response: there is no certificate involved in this solution.

"The DeNB shall not accept or send S1-AP and X2-AP message from/to the RN until a successful Relay device authentication has happened."

Response: RN platform authentication is provided as part of the RN attach procedure.

"Security of RN Management shall be guaranteed."

Response: this requirement seems compatible with all solutions described in clause 10. Either a separate TLS connection is set up to the OAM server, or, after the successful completion of the RN attach procedure, the management traffic is secured end to end.Besides, If a separate TLS connection is established, it can make use of the relay node platform secret key, as described in the TLS-PSK standard.

"The wireless resource: security shall be able to prevent misuse by identifying whether the attached terminal is a UE or a RN. The identification could be implicit."

Response: In this solution, the identification is implicit. If the terminal is a UE, it will fail in enhanced AKA procedure because it has not the valid RN platform related key e.g. Krelay/K_platform

"The connection between relay and network should be confidentiality protected. Confidential protection for the S1/X2 user plane traffic over the Un should provide protection as same as the user plane data transferred on Uu interface, i.e. provide optional confidentiality protection on Un interface."

Response: this is provided by AS security .

"Both user plane and control plane must be considered as they may not require the same level of protection."

Response: This solution satisfies the requirement by means of enhanced AS security or IPsec.

“The RN platform shall protect from reading and/or modification of security parameters and security functions by unauthorized parties (platform security). The integrity of the RN platform shall be validated as part of the RN start up procedure.”

Response: RN platform autonomous integrity validation is performed before the RN attach procedure and RN platform authentication is performed in the procedure as well.

“RN specific device security features, e.g. security storage of sensitive data, device integrity check, USIM aspects, shall be considered.”

Response: All of the features is considered as the precondition of this solution.

10.8.5.3 How does the solution 8 address the general Editor’s notes and the residual threats in clause 8.1.2.1.2?

This clause is only appropriate if the version of solution 8 using IPsec to integrity protect the S1 and X2 signaling is chosen. We quote from clause 8.1.2.1.1.

“Editor’s Note: It needs to be clarified whether all traffic over the Un user plane, or only S1 signalling traffic, is to be protected by NDS/IP, e.g. for performance reasons. If the latter applies then appropriate mapping of parameters identifying S1 signalling traffic to IPsec selectors (IP addresses, ports, transport protocol) would have to be performed. “

Response: The S1 and X2 signallling traffic could be protected by means of enhanced AS security or IPsec. It’s FFS that whether and how all user traffic over Un should be prevented from the threat 3 described in clause 5.3.

Editor’s Note: The enrolment process for credentials to set up backhaul link security between RN and MME-RN, and RN and S-/P-GW-RN (i.e. distribution of IPsec certificates and set up of IPsec tunnel) needs to be studied.

Response: There is no credential involved in solution 8.

We quote from clause 8.1.2.1.2:

“**Residual Threat:** threats of eavesdropping on and modification of traffic of DRBs is satisfactorily addressed by platform integrity and use of IPsec. As RRC traffic cannot be protected by IPsec it needs to be considered separately. The main threat to RRC seems to be that an attacker modifies bearers on Un. This seems to be possible when an attacker knows the RRC integrity key.
Editor’s Note: threats to AS security for RRC over Un need further study. In particular: how can an attacker obtain knowledge of the RRC integrity key? ”

Response: in solution 8 the attacker cannot obtain the RRC integrity key.

“**Residual Threat:** neither RRC nor UP-UE traffic are protected by IPsec. (UP-UE = user plane data sent by UE.) In addition to the remarks made on RRC in 8.1.2.1.2.1, the attacker could eavesdrop on UP-UE. An attacker could e.g. fraudulently establish an RN-DeNB radio connection via a MitM as described for threat 2 in clause 5.

Depending on the way in which the attacker obtains knowledge of the keys it may not be enough to ascertain that the IPsec SAs and AS security have the same endpoints, i.e. that all security tunnels from the RN terminate in the real network instead of in a MitM node may not be sufficient. It may neither be sufficient to bind the USIM to the RN, e.g. by using EAP-AKA inside IKEv2 in the way done for HeNBs.”
Editor’s Note: threats to AS security for RRC and UP-UE over Un need further study.”

Response: in solution 8 the attacker cannot obtain the UP-UE encryption key.

10.8.5.4 How does solution 8 address the general Editor's notes and the residual threats in clause 8.1.2.2?

This clause is only appropriate if the version of solution 8 using enhanced AS security to integrity protect the S1 and X2 signaling is chosen. We quote from clause 8.1.2.2.2.

"**Residual Threat:** as already noted in 8.1.1, integrity protection of S1-UE is required, but can be only guaranteed if the AS security mechanisms on Un are modified with respect to Uu as Uu does not provide integrity on DRBs. Furthermore, all threats that apply to RRC and UP-UE in case 8.1.2.2.2 now apply to all traffic over Un.

Editor's Note: threats to AS security for all traffic over Un need further study. Integrity protection for S1-UE traffic needs further study."

Response: in solution 8, the attacker cannot obtain the RRC integrity key or the UP-UE encryption key.

10.8.5.5 Analysis of solution 8 not related to threats

In solution 8, it enhanced the existing EPS AKA procedure to provide the authentication for UICC and RN platform. The existing authentication vectors (e.g. RAND, AUTN, or RES) are enhanced and reused to perform the RN platform. A symmetric security key (i.e. Krelay/K_platfrom) which is RN platform related is used to provide the enhancement of the AKA. The solution has little influence on the AS/NAS signaling and the key hierarchy.

10.9 Solution 9 – IPsec or PDCP security for control plane and with key binding for AS security

10.9.1 General

This solution has two different flavours: an IPsec based flavour and an AS security based flavour. The first one uses IPsec to protect the S1/X2 User-UE control plane between the RN and DeNB and AS level security mechanism to protect the user plane. The IPsec tunnel provides integrity and confidentiality protection for the S1/X2 User-UE control plane between the RN and the DeNB. Confidentiality protection for the User-UE user plane traffic is provided by AS confidentiality protection. The keys used for AS protection are bound to the IPSec SA (keys) that is set-up and its associated authentication of the RN as a genuine relay node, i.e., RN platform authentication. The setup is depicted in Figure 10.9.1-1.

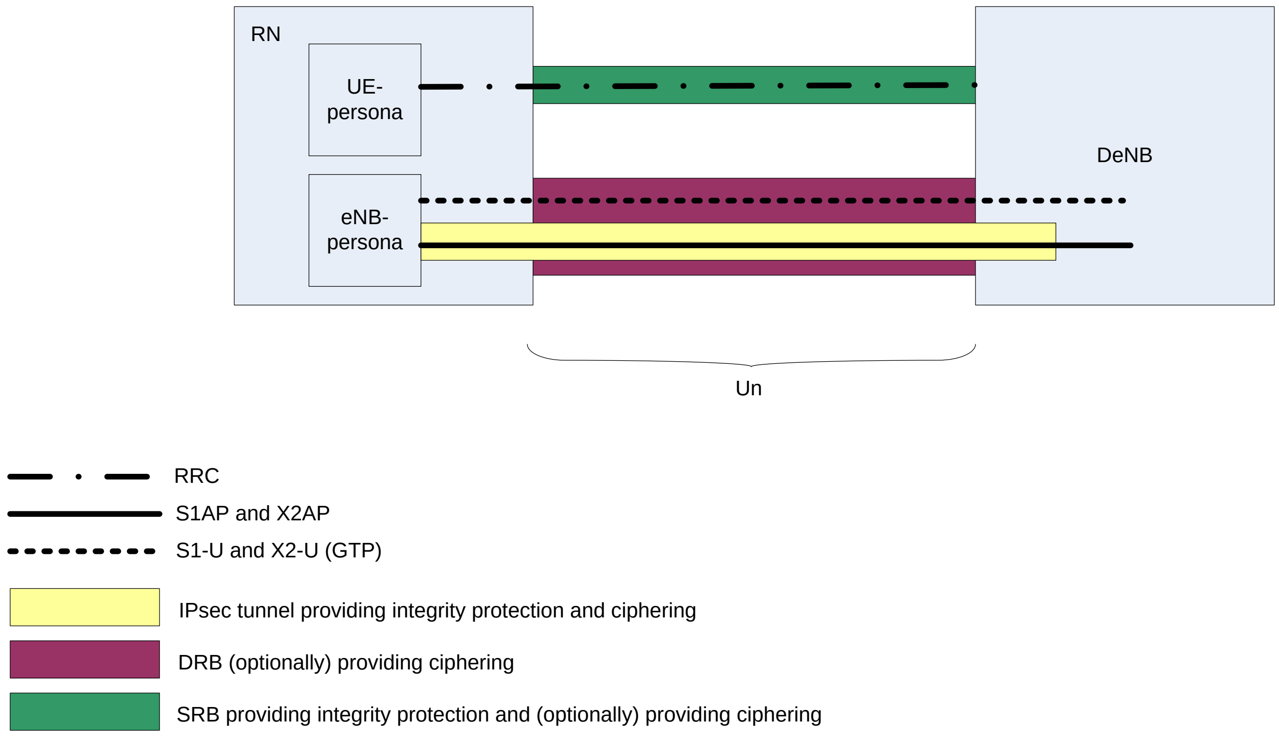

RN
UE-persona
eNB-persona
DeNB
Un
RRC
S1AP and X2AP
S1-U and X2-U (GTP)
IPsec tunnel providing integrity protection and ciphering
DRB (optionally) providing ciphering
SRB providing integrity protection and (optionally) providing ciphering

Figure 10.9.1-1 Set up of security protocols for Solution 9 when IPsec is used to protect S1AP/X2AP

The second flavour of Solution 9 is based on that integrity protection and ciphering of S1AP/X2AP is provided by AS. For this to be possible, it must be possible to configure also DRBs to use integrity protection. In this case there is no need to use IPsec. However, to allow for RN platform authentication and to bind the AS keys to the RN platform authentication, a TLS tunnel is setup between the eNB-persona of the RN and the DeNB. The AS keys are then bound to the RN platform authentication via the keys established for the TLS tunnel. This is depicted in Figure 10.9.1-2.

A first observation is that they both use X509v3 certificates. The profiling done in TS 33.310 [7] does not seem prohibit the use of the same certificate in both places. In fact, clause 6.1.3 (referenced from 6.1.3b for NEs) of TS 33.310 [7] states:

> SEG certificates shall be directly signed by the SEG CA in the operator domain that the SEG belongs to. **Any SEG shall use exactly one certificate to identify itself within the NDS/AF**.

However, clause 6.1.3a specifying the TLS entity certificate profile does not give any such requirement. This indicates that it would be allowed to have a TLS certificate in addition to the IPsec certificate used for the backhaul.

It is a question whether one would prefer a policy where one of the certificates has a shorter lifetime or uses a different policy. In that case it could make sense to use different certificates. Even if the certificates are not the same, there seems to be nothing preventing them to be part of the same PKI.

It can be left to operator policy to choose whether the TLS certificate and the IPsec certificate are the same or coming from the same PKI.

Editor's note: If there is a requirement for two certificates, then the details are FFS.

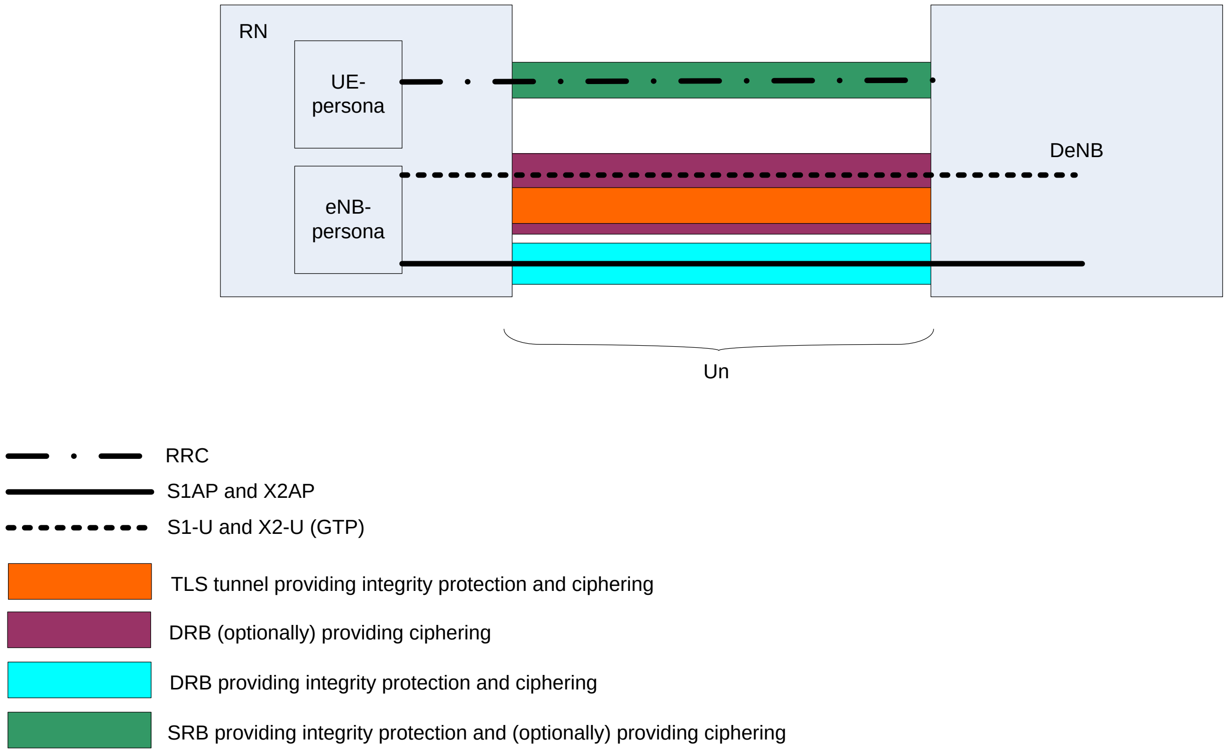

RN
UE-persona
eNB-persona
DeNB
Un
RRC
S1AP and X2AP
S1-U and X2-U (GTP)
TLS tunnel providing integrity protection and ciphering
DRB (optionally) providing ciphering
DRB providing integrity protection and ciphering
SRB providing integrity protection and (optionally) providing ciphering

Figure 10.9.1-2 Set up of security protocols for Solution 9 when AS is used to protect S1AP/X2AP

Note that the so called IPsec based flavour could of course also be implemented by using TLS as the secure channel for protection of S1AP and X2AP and establishment of K_O.

10.9.2 Security Procedures

10.9.2.1 Start up procedure phase II: Attach for RN operation

To counter bidding down-attack (modification of SMC) the set of allowed algorithms for AS and NAS it is assumed that the set of allowed algorithms in the RN and DeNB only contain strong algorithms. This can be achieved by administrative means in the configuration of DeNB and RN. Another countermeasure is to issue a new SMC after the platform authentication has been performed and the MME has been informed about a successful RN attach (see below).

To ensure that RN specific services are not allowed in Phase I of the start up procedure (see TS 36.300 [4]), the MME needs to be informed whether the attaching entity is an RN or not. This is by definition achieved via the platform authentication. In solution 9, the MME does not take part in the platform authentication and does hence not know when the procedure has successfully completed. The DeNB is the node performing the platform authentication. Therefore, the DeNB can inform the MME about whether platform authentication of the attaching entity has succeeded. After that point, the MME may allow the attaching entity to access services necessary to perform the RN function, e.g., access to certain APNs.

The way the DeNB informs the MME about the success of the platform authentication can probably be achieved in many ways. The simplest seems to be to simply pass an S1AP message from the DeNB to the MME. This could be a newly defined S1AP message, or it could be defined that a DeNB does not respond to the S1 UE INITIAL CONTEXT SETUP message until platform authentication has succeeded.

An RN engaging in Phase II of the start up procedure (see TS 36.300 [4]) to establish itself as a connected relay node providing service to UEs attaches to the network and authenticates itself the RN as a UE using the USIM in a regular EPS AKA NAS procedure. As a result of this attach and authentication, standard (Uu) security mechanisms are applied on the Un interface; this is shown as the DRB and SRB in the figure above. This step only provides connectivity between the RN and the DeNB.

The DeNB (which includes S-GW and PDN GW functionality) blocks all traffic but IKEv2, or TLS setup traffic respectively, on the single DRB at this point. The DeNB could also provide access to an enrolment server and/or other

O&M servers, but the RN's access shall be as restricted as possible. The reason for allowing the RN access to an enrolment server or O&M server is that one wish to allow the RN to have certificates enrolled also at this point in time). In particular, any attempt by the RN initiate traffic towards general network nodes (i.e., not the enrolment server or the O&M network) or the Internet is blocked by the DeNB. This implies that the RN cannot perform an attack to gain free internet service or attack any nodes which are not allowed to be accessed by the operator. It also implies that the RN cannot establish connections towards the network for UEs until the IPsec or TLS tunnel and AS security is enabled; there is therefore no need for protecting this (non-existent) traffic.

For the IPsec based flavour, the next step is to establish an IPsec tunnel between the RN and the DeNB using IKEv2 for SA establishment. An offset key is generated in the DeNB and sent to the RN. The offset key is denoted K_O. If the AS security based flavour, the next step is to establish a TLS tunnel. From the keys established at the TLS setup, the offset K_O is derived using RFC 5705 Keying Material Exporters for Transport Layer Security (TLS) [18].

After the DeNB has set up the IPsec or TLS tunnel and has activated the K_O-bound AS security context (see below), the DeNB considers the RN to be both RN subscriber authenticated and RN platform authenticated. Therefore, after these two activations, the DeNB allows the RN to establish bearers for other UEs (and to receive keys for these UEs' security protection).

The purpose of the K_O is to bind the PDCP keys to the platform authentication. Therefore, any AS context binding is already taken care of by the K_{eNB} and PDCP key constructions. The K_O binding is just an additional binding to a more restricted context. Even though the attacks mentioned in RFC 5705 regarding the RSA based cipher suites seems very difficult to mount in this setting, it seems reasonable to be cautious and require that a ephemeral Diffie-Hellman based cipher suit is used to avoid the possibility of attacks yet to be discovered.

NOTE: If RN and DeNB use TLS key exporter for any other purpose then a new label must be used and the label must be registered with IANA

10.9.2.2 Binding of RN platform authentication to the AS security context

10.9.2.2.1 Purpose of the binding

Since the K_O is protected by IPsec tunnel or is extracted from the TLS keying material which is bound to RN platform authentication, it is only accessible inside the RN secure environment and the DeNB secure environment. The CK/IK from the RN subscription authentication are transferred to the RN secure environment. To ensure that encryption and integrity protection can only terminate inside the secure environment of a legitimate RN, the CK/IK from the RN subscription authentication (or a key derived from there, e.g., K_{eNB}, see below for details) and the K_O are mixed. The result of the mixing is applied as integrity and encryption keys for the AS security context.

K_O is only known inside the secure environment and hence an attacker having access to CK/IK from the USIM will not be able to read user plane data from mobile connected to the RN. Neither will the attacker be able to read/inject/modify any of the S1AP/X2AP messages passed between the RN and the DeNB.

10.9.2.2.2 Binding K_O and the keys from RN subscription authentication

The binding of K_O and the keys from the RN subscription authentication is achieved by including the K_O as a parameter to the KDF input for the K_{RRCint}, K_{RRCenc}, and K_{UPenc} derivations. Remember that at the point of the binding there is already a complete existing EPS key hierarchy active. The K_{eNB} from this current EPS key hierarchy is used as the input key to the derivation as usual. Figure 10.9.2.2.2-1 shows the input to the KDF applications.

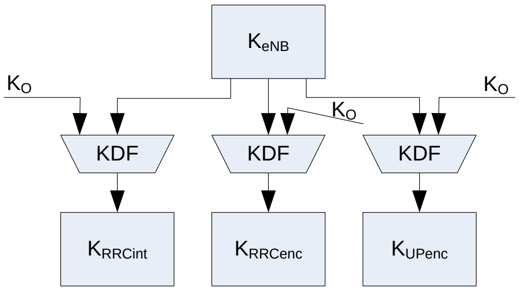


Figure 10.9.2.2.2-1 Derivation of the bound keys for RRC and UP protection. There are other inputs to the key derivations, but only the relevant ones are shown.

For the AS based flavour, a key for integrity protection of DRBs is also required. This key is derived using the same framework as in Figure 10.9.2.2.2-1. Following the same naming scheme as the other keys, the user plane integrity key should have the name K_{UPint}.

10.9.2.2.3 Switching to the K_O-bound AS security context

Changing to the newly created K_O-bound AS security context is very similar to a key change on the fly which already exists in LTE. The intra cell handover procedure consists of a RRC reconfiguration procedure which contains an mobility information element. Therefore, it seems appropriate to enable the new K_O-bound AS security context using a similar RRC reconfiguration procedure. It is however left up to the stage 3 groups to decide which is the best way for the DeNB to signal the start of K_O binding to the RN.

After the activation of a K_O-bound AS security context, the RN and the DeNB keeps using a K_O-bound AS security context even if the RN goes via RRC_IDLE state and comes back to RRC_CONNECTED. This avoids having to re-run the activation procedure after a CONNECTED-IDLE-CONNECTED cycle.

For a normal UE, if the UE goes to RRC_IDLE and comes back to RRC_CONNECTED, there is a new K_{eNB} used. For an RN the situation is the same. The RN and the DeNB creates a new K_O-bound AS security context using the new K_{eNB}. The same K_O is used in the creation.

10.9.2.2.4 Establishment of K_O

IPsec based flavour

After IKEv2 is run between the DeNB and the RN (see clause 10.9.2.1) the IPsec tunnel between the two is established. The endpoints for this tunnel are inside the secure environments of the DeNB and the RN respectively. The DeNB now simply generates a random key K_O, and transmits this to the secure environment of the RN. The transport can, e.g., be done in a new S1AP message or a UDP datagram destined for a certain port. The exact choice of protocol should be left to the stage 3 protocol groups to decide. The important security requirement is that the message is confidentiality protected and integrity protected. This implies that the IPsec tunnel shall provide both integrity and confidentiality protection. Due to the small amount of S1AP signalling and the fact that it is already integrity protected by IPsec, the addition of ciphering using IPsec does not significantly increase the load. Confirmation of K_O delivery (explicit or implicit) shall be assured.

AS based flavour

After the TLS handshake is run between the RN and the DeNB (see clause 10.9.2.1), they share master secret. From this master secret, the key K_O is extracted by the RN and the DeNB individually using RFC 5705 [18] Keying Material Exporters for Transport Layer Security (TLS) [6]. Compared to the IPsec based flavour, there is no need to transport K_O via the secure tunnel and hence there would be no need for a new message to transport K_O here.

10.9.2.2.5 K_{eNB} chaining, change of K_O and change of IPsec SAs

Change of K_{eNB}

In case there is an intra-eNB handover (or any type of handover for that matter), the K_{eNB} is chained via a horizontal key derivation of derived via a vertical key derivation. This implies that the keys used to protect the AS traffic, i.e., K_{UPenc}, K_{RRCenc} and K_{RRCint} needs to be re-derived. This is the normal behaviour at handover. If K_O-bound AS security context is activated, the RN and the DeNB re-derive the new AS protection keys using as normal, except that the current value of K_O that was used previously is input into the KDF as well. Hence, a handover with re-derivation of the K_{eNB} causes no issues for the K_O-bound AS security context.

Change of K_O

The DeNB may choose to establish a new K_O with the RN for the reason of achieving key refresh. If so, the RN and DeNB shall continue using the old K_O until it is signalled from the DeNB to the RN that a switch shall be made to the new K_O. It seems reasonable to use an intra-eNB handover to signal this change, but it is left to the stage 3 protocol groups to decide the exact measure to make the switch of keys. A key identifier to keep track of K_Os may be needed.

For the IPsec based solution, the DeNB sends down a new K_O through the IPsec tunnel to the RN in the same manner as the original K_O was established. For the AS based solution, the DeNB runs a new TLS handshake to establish a new TLS master secret, from which the RN and the DeNB extracts a new $K_{O.}$

Change of IPsec SAs

This is only applicable to the IPsec based solution.

The DeNB is in control of when to run IKEv2, when to change the SPI in the ESP packets and when to send a new K_O to the RN. Hence the DeNB can, and shall, ensure that there is not a simultaneous change of $K_{O,}$ IPsec SAs or K_{eNB}. When the DeNB ensures this, there is no risk of a race condition when it is unclear which keys are used.

NOTE: End-to-end NAS security relies on CK/IK. If these keys are eaves-dropped on the RN-UICC interface, the NAS security relies on the secure environment on DeNB, and on the AS security and S1 security.

Validation of security context after NAS Authentication procedure

After a successful NAS Authentication procedure towards the RN without generation of a fresh offset key it is necessary to validate that the DeNB has the same security context for AS protection as the RN will have; this to assure the RN that it is communicating with the same endpoint that it performed platform authentication with. No user data shall be sent over Un before the validation has taken place. To perform the validation it suffices to send a confirmation message inside the provided secure tunnel. Verification of the integrity of the sent message would give the required assurance. The described solution is very straightforward but other methods exist; the exact method is ffs and should be decided together with RAN to ensure that performance and security requirements are fulfilled.

10.9.2.3 Analysis of protection against identified threats

For the IPsec based flavour, IPsec will be used to protect the S1-AP/X2-AP interface between the RN and DeNB following the procedures for eNBs as described in clause 11 of TS 33.401 [2], i.e., both confidentiality and integrity protection is provided by ESP. For the AS based flavour, the S1AP/X2AP traffic is protected by ciphering and integrity protection by the PDCP protocol. The integrity protection prevents attacks 1 and 4b and the confidentiality protection prevents attack 3 completely for signalling traffic while user plane traffic only is confidentiality protected by the AS confidentiality protection provided by PDCP. However, this is according to accepted principles for user plane traffic protection over the Uu air interface. The overhead caused by the IPsec is negligible as there is little signalling compared to user plane traffic. If the integrity protection is provided by PDCP as in the AS based flavour, then the overhead is even less. AS level security efficiency is as for Uu protection mechanisms.

As the AS level security is bound to credentials directly on the RN, meaning that the RN is platform authenticated at the network access layer, all of the threats 2, 4c, 4d are mitigated.

For threat 5, first note that NAS signalling from the RN to the MME-UE will use keys derived from the K_{ASME} obtained by the LTE authentication (EPS AKA) procedure performed using the USIM. These keys may be exposed if the interface between the UICC and the RN is unprotected. However as NAS messages are tunnelled in the AS they will be protected by the modified AS security context (as soon as it has been established). Thus there is no possibility for an attack on Un to succeed in modifying the NAS signalling from the RN to the MME-UE and, as we have described above, the AS signalling is also protected. Thus threat 5 is countered by this solution.

With respect to Threat 7 it can be noted that if an attacker removes the USIM, the RN without USIM cannot be authenticated by the network, which means that the legal RN cannot connect to network and provide services. This would be equal to any other denial of service attack like disturbing or eliminating the radio connectivity. An attacker could also insert the USIM into another RN, but if the identities of the RN's used to track the topology of the access network are based on the RN identities carried in the RN certificates, no networking problems will occur.

One attack is to try to create a situation when AS keys are reused which would lead to a two time pad. In this attack it is assumed that the attacker is in control of the Un interface and is able to record and inject messages there and at the same time also have control of the RN to UICC interface and is able to record and inject messages there. The attacker replays a recorded NAS Authentication procedure which is unprotected and for which the attacker has recorded the used CK, IK, on the RN to UICC interface. The attacker injects the recorded CK, IK on the RN to UICC interface. This attack would then result in calculation of the same AS keys as in the recorded event as K_O is reused. The attack as such cannot be stopped but it can be detected and thus the tentative information leakage from the two time pad can be prevented by not sending any user data over Un before the RN has been reassured that the entity on the other end of the Un interface is the same as when the platform authentication was performed (the K_O was established). For countermeasures see clause 10.9.2.2.5.

In addition to the threat of modifying RN NAS signalling and AS traffic in Phase 1 (an attack common to all solutions) an attack on NAS signalling in phase II has also been discussed in relation to Solution 9. In this latter attack it is assumed that the attacker has been able to compromise the DeNB and will be able to access the offset key K_O which would allow the attacker to calculate the NAS keys and the modified AS keys. However, as the security solutions for relay node security are based on trust in the integrity of secure environments, attacks requiring compromise of a secure environment are not to be considered for development of specific countermeasures. The consequences of an attack on NAS signalling, assuming a compromised secure environment in a DeNB, would be the same as described for attacks on NAS signalling in Phase I of RN attach.

10.9.3 UICC Aspects in RN scenarios

The description in 10.9.2 shows that it is not necessary to have a protected interface between the UICC and the TRE in the RN. Furthermore, using RN identities for tracking the topology of the access network eliminates the need to verify RN UICC pairings. The final conclusion then is that removable UICCs can be used in RNs.

10.9.4 Enrolment procedures for RNs for backhaul link security

This solution allows the RN to enrol a device certificate as with macro eNBs.

10.10 Solution 10 – Secure channel between RN and USIM with a one-to-one mapping between RN and UICC

Editor's Note: Entities affected by security for relays (e.g. termination points of security protocols, entities with additional relay-related functionality) should be considered

10.10.1 General

This solution uses either IPsec or enhanced AS security to protect the control plane between the RN and DeNB and the AS level security mechanism to protect the user plane. It also uses a binding between the RN and UICC to protect the transfer of E-UTRAN keys over this interface. The binding also provides a one to one mapping between RN and UICC.

10.10.2 Security Procedures

Using IPsec exactly as for eNBs as described in clause 11 of TS 33.401 [2] or enhanced AS with the secure channel as discused in clause 7.5.3 to protect the S1-AP/X2-AP interface between the RN and DeNB will prevent attacks 1, 3 and 4b. The overhead caused by the IPsec would be negligble as there is little signalling compared to user plane traffic.

10.10.3 UICC Aspects in RN scenarios

Secure Channel, mechanism, as specified in ETSI TS 102 484 [12], shall be used between the UICC and the RN to prevent attacks 1, 2 and 5. This mechanism will prevent the removal of UICC from a genuine RN and its usage in a rouge RN, prevent also the usage of fake UICC in a real NB, and eliminate possibility to capture and manipulate information communicated between UICC and RN

10.10.4 Enrolment procedures for RNs for backhaul link security

This solution requires the RN to enroll a device certificate as with macro eNBs.

10.11 Solution 11 – Secure Channel between USIM and RN and AS integrity for S1 /X2; Variant with two USIMs

10.11.1 General

The main features of this solution are: (1) Autonomous validation of the RN platform; (2) Secure Channel between USIM-RN and RN; (3) certificate validation client on the UICC; (4) AS integrity for S1/X2; (5) Use of a second USIM, called USIM-INI, for initial IP connectivity purposes prior to RN attachment.

The solution is further characterized by the fact that the MME-RN delegates the platform authentication of the RN to the UICC and trusts that the USIM-RN on the UICC engages in an AKA run only after successful platform authentication of the RN, cf. clause 10.11.7.

Clauses 10.11.2 through 10.11.6 describe the solution with all its options.

Clauses 10.11.7.1 and 10.11.7.2 describe two profiles of solution 11, profiles 11A and 11B where the options are selected. It would be sufficient to standardize only one of these profiles.

10.11.2 Security Procedures

The start-up of an RN proceeds in the following steps. If one of the steps fails in any of the involved entities the procedure is aborted by that entity.

Phase I: Procedures prior to the RN attach procedure

E1. The RN performs an autonomous validation of the RN platform.

E2. The RN attaches as a UE using USIM-INI to be prepared for performing steps E5. and, optionally, E3.

E3. The RN optionally obtains an operator certificate through the enrolment procedures defined in TS 33.310 [7]. Details can be found in clause 10.11.4. The RN optionally establishes a secure connection to an OAM server. Details can be found in clause 10.11.5.

E4. Then the RN platform secure environment and the UICC establish a Secure Channel between RN and USIM-RN according to ETSI TS 102 484 [12] clause 7 "Secured APDU" with TLS handshake. This TLS handshake shall be initiated by the UICC and use certificates on both sides. The RN uses a pre-established certificate or the certificate enrolled in step E3. The UICC verifies that this certificate is limited to use with relay nodes. The UICC is pre-provisioned with an operator root certificate to verify the RN certificate. The UICC certificate needs to be pre-installed in the UICC by the operator. The RN is pre-provisioned with a root certificate to verify the UICC certificate.

NOTE 1: The root certificate, and potentially other data required e.g. according to profile 11B, that need to be stored in the UICC could be provisioned in the UICC during its personalization. The operator provides to smartcard manufacturer a list of data (e.g. IMSI, key K, etc) to be provisioned in the UICC during its personalization phase, before issuance of the UICC. The root certificate, and potentially other data, could be provided by the operator as part of the data to be personalized in the UICC by the smartcard manufacturer. In the field, the root certificate, and potentially other data, could also be updated by OTA means, if needed.

The private key corresponding to the RN certificate and the root certificate used to verify the UICC certificate are stored in the secure environment of the RN platform validated in step E1, and the TLS handshake terminates there. From the completion of this step onwards, all communication between the USIM-RN and the RN is protected by the Secure Channel. The USIM-RN shall not engage in any AKA-related communication prior to the establishment of the Secure Channel and a successful certificate validation check, cf. step E.5.

NOTE 2: Certificate use restriction may be made possible e.g. through a suitable name structure, or a particular intermediate CA in the verification path, or policy information terms, e.g. by a suitable object identifier (OID) in the certificate policies extension.

NOTE 3: The USIM-RN is activated after the completion of the secure channel set-up, cf. ETSI TS 102 484 [12].

E5. A certificate validation client on the UICC checks the validity of RN certificate used in the secure channel set-up with a certificate validation server. The check of revocation status and expiry time may be omitted when there is a one-to-one association between the USIM-RN and the RN (e.g. as represented by the subject name in the certificate), cf. profile 11B in clause 10.11.7.2, while the verification of the signatures in the certificate chain up to the root certificate shall be performed in any case. A certificate validation client on the RN checks the validity of UICC certificate used in the secure channel set-up with a certificate validation server. Details can be found in clause 10.11.6.

E6. The RN detaches from the network if it has attached for performing steps E2, E3, or E5.

NOTE 4: ETSI TS 102 484 [12] states in clause 6.2.2: "The UICC may present a self-signed certificate. The terminal or terminal application should temporarily accept such a certificate during the TLS handshake protocol, if it is able to establish by other means (e.g. successful network authentication) that the handshake protocol is conducted with an authentic UICC." And in the present solution for relay node security, the RN indeed verifies the authenticity of the USIM-RN by means of a successful RN attach procedure. However, the use of a self-signed UICC certificate, or no UICC certificate at all, would weaken network-to-RN authentication in cases where both the interfaces of the RN with the UICC and the network were under the control of an attacker. (Think of a stolen RN in a rogue environment.) Then the RN would happily use any key fed to it over the interface with a fake UICC and use this key in the communication with a fake network. The use of a UICC certificate prevents this threat as no rogue UICC can set up a secure channel with the RN. Similar considerations apply when the method in ETSI TS 102 484 [12] in clause 7 "Secured APDU" with TLS handshake is used.

NOTE 5: ETSI TS 102 484 [12] states in clause 6.2: "Both the terminal or the UICC shall be able to initiate a TLS secure channel." It is proposed here that the UICC assumes the role of TLS client for the following reason:
the certificate validation cf. step E.5, can be integrated with TLS according to RFC 4366 [13], otherwise the certificate validation would have to be a separate procedure following the TLS procedure. When the method in ETSI TS 102 484 [12] in clause 7 "Secured APDU" with TLS handshake is used this requires an addition to the TS.

NOTE 6: One may want to limit the lifetime of a secure channel between USIM-RN and RN for security reasons. Suitable counters providing such a limit include a record counter, cf. clause 6.4 of ETSI TS 102 484 [12], or a transaction counter, cf. clause 7 of ETSI TS 102 484 [12], or a counter on the AUTHENTICATE commands received over the secure channel. To disallow the resumption of TLS session, and to enforce a new TLS handshake on each RN attach, the USIM-RN may be configured accordingly, if necessary.

NOTE 7: Having two USIMs on one UICC is a standard feature available today (but only one USIM can be active at a time in current 3GPP specifications). The set-up of the secure channel between USIM-RN and RN causes the USIM-RN to be activated, but the connectivity and the security context established by means of USIM-INI may continue to be used. TS 33.401 [2], clause 6.4, requires the deletion of an EPS security context only when the UICC changes.

NOTE 8: The RN could distinguish a USIM-RN from a USIM-INI e.g. by the use of so-called "labels" for UICC applications; cf. TS 31.101 [15] for the definition and TS 33.220 [11] for an example where such labels are used in 3GPP security specifications.

Phase II: RN attach procedure

The RN performs the RN attach procedure for EPS as defined in TS 36.300 [4]. From a security point of view, this involves the following steps:

A1. If the USIM-RN is not already active the RN activates it and resumes or re-establishes the secure channel. The RN activates the USIM-RN and invalidates any EPS security context on the USIM-RN. The RN uses the IMSI (or a related GUTI) pertaining to the USIM-RN in the RN attach procedure.

NOTE 9: This IMSI differs from the one pertaining to the USIM-INI, therefore the network can distinguish the handling of the two USIMs.

A2. The MME-RN runs EPS AKA with the RN and the USIM-RN and establishes NAS security. The RN shall use only keys in an RN attach procedure that were received from the USIM-RN over the Secure Channel.

A3. The MME-RN checks from the RN-specific subscription data received from the HSS that the USIM-RN is dedicated to the use in RN attach procedures. The MME-RN communicates the fact that the attachment is for relay nodes to the DeNB in an extended S1 INITIAL CONTEXT SETUP message.

A4. Upon receipt of the extended S1 INITIAL CONTEXT SETUP message the DeNB sets up RN-specific AS security over Un, which differs from AS security over Uu in that integrity protection for PDCP frames carrying S1/X2 messages is provided. The DeNB rejects any attach request by relay nodes for which no confirmation has been received from the MME-RN that the attachment is for relay nodes.

The RN start-up is now complete from a security point of view, and UEs can start attaching to the RN.

10.11.3 USIM Binding Aspects in RN scenarios

The requirement of restricting the possible combinations of particular RNs and particular USIM-RNs is ffs, cf. clause 9.4. If such restrictions are required then authorization is required that could be enforced in at least one of the following ways:

(1) The RN enforces the allowed combinations.
The RN verifies the IMSI pertaining to the USIM-RN through the successful RN attach procedure. The RN can then learn about the allowed combinations of USIM-RN and RN as follows:

(1a) The RN knows the authorized USIM-RNs by configuration;

(1b) The OAM server with which a secure connection was established in step E.3 tells the RN the authorized identities;

NOTE: The check whether the binding between RN and USIM-RN is authorized can be entrusted to an RN with a validated platform. But only such RNs are able to establish a secure channel with a USIM-RN, which in turn is a pre-requisite for a successful RN attachment to the network, cf. clause 10.11.2. Hence the network can trust that the RN performs the check faithfully.

(2) The UICC enforces the allowed combinations.
The UICC verifies the RN identity through the TLS handshake in the secure channel set-up. The UICC knows the authorized RNs by configuration. The standard secure OTA mechanisms (TS 31.116 [9]) can be used to update the configuration of UICC and renew the stored identities if required.

(3) The MME enforces the allowed combinations.
The MME-RN may learn the RN device identity in a way similar to an MME learning the IMEI of a UE. The MME-RN then performs the check whether this combination of USIM and RN is authorized. The MME-RN may obtain the authorization information from the HSS.

Editor's Note: It is ffs whether the IMEI could serve as the RN device identity. If not a new NAS message or message field for sending the RN device identity may be required. In profiles 11A and 11B the sending of an RN device identity to the MME is not required.

10.11.4 Enrolment procedures for RNs

The RN may enroll a device certificate as with macro eNBs according to TS33.310 [7] prior to the RN attach procedure with the DeNB. This certificate may then be used for establishing the secure channel between RN and USIM.

The certificate enrolment procedure does not rely on the security at the AS level, but is secured at the application layer. It can be therefore executed before security on the Un interface has been established. However, the RN requires IP connectivity for the enrolment procedure to be able to reach the Registration Authority RA. The IP connectivity could be established in various ways:

(1) The RN uses offline means for enrolment purposes. No USIM is required.

(2) The RN attaches to an eNB like a normal UE using a USIM, called USIM-INI, different from the one used in the RN attach procedure to the DeNB, called USIM-RN. No secure channel between RN and USIM-INI is required.

In both cases, the network must ensure that the destinations the RN can reach are restricted, e.g. to only the PDN(s) where the RA, the OAM server and the certificate validation server are located. In case (2) this could be ensured e.g. by restricting IP traffic originating from the RN and sent over PDCP without integrity protection to only certain destinations (APNs). The restrictions are assumed to be part of the profile relating to the subscription associated with the USIM-INI.

10.11.5 Secure management procedures for RNs

The RN may establish a secure connection to an OAM server.

The OAM procedure does not rely on the security at the AS level. It can therefore be executed before security on the Un interface has been established. If no security on lower layers is available the communication between RN and OAM server would be typically secured using TLS. The RN requires IP connectivity for this procedure to be able to reach the OAM server. The IP connectivity established for enrolment purposes according to clause 10.11.4 could be re-used, or, if not available, it could be established in the same ways as described in clause 10.11.4.

Restrictions on the destinations the RN can reach must apply if the communication with the OAM server occurs prior to the RN attach procedure. They can be realized similar to what is described in clause 10.11.4.

10.11.6 Certificate validation

The solution in this clause requires the UICC and the RN to perform certificate validation of the RN certificate and the UICC certificate respectively used for the set up of the secure channel prior to the RN attach procedure with the DeNB unless additional restrictions, as for profile 11B, cf. 10.11.7.2, apply. The certificate validation protocol shall be self-secured and can therefore be executed over unsecured links. The client on the UICC needs to send and receive the certificate validation message via the RN if a certificate status check is required according to the selected profile of solution 11, cf. clause 10.11.2, step E5. The RN requires IP connectivity for the certificate validation messages to be able to reach the certificate validation server. The IP connectivity, and the restrictions on permitted destinations, can be established in the same ways as described in clause 10.11.4 case (2). The certificate validation in step E5. of clause 10.11.2, shall be integrated with the TLS handshake performed in step E4, according to RFC 4366 [13].

If certificate validation is required then OCSP, cf. RFC 2560 [17], shall be used for certificate validation in the following way: the UICC shall generate a nonce. This nonce is sent as part of the TLS client hello, as described in RFC 4366 [13]. The RN, acting as the OCSP client, shall form an OCSP request including this nonce in a requestExtension, as defined in RFC 2560 [17]. The signed response of the OCSP responder then also includes this nonce, according to RFC 2560 [17]. Furthermore, this signed response mandatorily includes a “producedAt” field, indicating the time at which the OCSP responder signed the response. The RN forwards the signed response of the OCSP responder as part of the TLS handshake to the UICC, as described in RFC 4366 [13]. The UICC then checks the CertStatus and that the expiry time of the RN certificate is later than the producedAt-time in the signed response of the OCSP responder.

NOTE: The above expiry time checking procedure ensures the UICC that the RN certificate was valid at the time the UICC started the TLS handshake. As the UICC has no clock the UICC cannot control the duration of the TLS handshake. In case this is a concern methods to enforce TLS handshakes, and hence OCSP checks, at defined events controlled by the network, e.g. AKA runs, may be used. An example is given in profile 11A, cf. clause 10.11.7.1.

10.11.7 Profiles of solution 11

This clause describes two profiles of solution 11, profile 11A in clause 10.11.7.1 and profile 11B in clause 10.11.7.2.

10.11.7.1 Solution profile 11A

10.11.7.1.1 General

The UICC inserted in the RN contains two USIMs: a USIM-RN which shall communicate with the RN only via a secure channel, and a USIM-INI communicating with the RN without secure channel and used for initial IP connectivity purposes prior to RN attachment.

USIM-INI and USIM-RN could be functionally identical to Rel-99 USIMs. But a restriction of the command set, compared to a Rel-99 USIM, may be appropriate. In addition there will be other requirement on the UICC to perform the TLS handshake (BIP-UICC server mode or UICC USB).

NOTE: The proposed solution with USIM-INI and USIM-RN does not imply new functionality on Rel-99 USIM. Only additional files may be needed, e.g. for RN profile. The secure channel features are at the UICC platform level and Rel-x UICC implementing the secure channel could contain Rel-99 USIM.

No particular binding of RN and USIM-RN is required. But the UICC shall check in the secure channel set-up that the RN certificate is dedicated to use with RNs.

10.11.7.1.2 Security Procedures

The start-up of an RN proceeds in the following steps. If one of the steps fails in any of the involved entities the procedure is aborted by that entity.

Phase I: Procedures prior to the RN attach procedure

E1. The RN performs an autonomous validation of the RN platform.

E2. The RN attaches as a UE using USIM-INI.

E3. The RN optionally obtains an operator certificate through the enrolment procedures defined in TS 33.310 [7]. Details can be found in clause 10.11.7.1.4. The RN optionally establishes a secure connection to an OAM server. Details can be found in clause 10.11.7.1.5. The RN shall retrieve a CRL from a suitable server.

E4. Then the RN platform secure environment and the UICC establish a Secure Channel between RN and USIM-RN according to ETSI TS 102 484 [12] clause 7 “Secured APDU” with TLS handshake. This TLS handshake shall be initiated by the UICC and use certificates on both sides. The RN uses a pre-established certificate or the certificate enrolled in step E3. The UICC verifies that this certificate is limited to use with relay nodes. The UICC is pre-provisioned with an operator root certificate to verify the RN certificate. The UICC certificate needs to be pre-installed in the UICC by the operator. The RN is provisioned with a root certificate to verify the UICC certificate.

The private key corresponding to the RN certificate and the root certificate used to verify the UICC certificate are stored in the secure environment of the RN platform validated in step E1, and the TLS handshake terminates there. From the completion of this step onwards, all communication between the USIM-RN and the RN is protected by the Secure Channel. The USIM-RN shall not engage in any AKA-related communication prior to the establishment of the Secure Channel and a successful certificate validation check, cf. step E.5.

The UICC shall re-establish the Secure Channel including a new certificate validation according to clause 10.11.6 after every AUTHENTICATE command exchanged between RN and USIM-RN.

NOTE: TS 33.310 [7] mandates the use of the same key for digitalSignature and keyEncipherment, e.g. clause 6.1.3 for SEG certificate profile.

E5. A certificate validation client on the UICC checks the validity of RN certificate used in the secure channel set-up with a certificate validation server. The verification of the signatures in the certificate chain up to the root certificate shall be performed. A certificate validation client on the RN checks the validity of UICC certificate used in the secure channel set-up with a certificate validation server. Details can be found in clause 10.11.7.1.6.

E6. The RN detaches from the network if it has attached for performing steps E2, E3, or E5.

Phase II: RN attach procedure

The RN performs the RN attach procedure for EPS as defined in TS 36.300 [4]. From a security point of view, this involves the following steps:

A1. If the USIM-RN is not already active the RN activates it and resumes or re-establishes the secure channel. The RN invalidates any EPS security context on the USIM-RN. The RN uses the IMSI (or a related GUTI) pertaining to the USIM-RN in the RN attach procedure. The RN shall request access only to the default APN. The default APN allows access to only the OCSP server.

NOTE 1: A Default APN is defined as the APN which is marked as default in the subscription data and used during the Attach procedure and the UE requested PDN connectivity procedure when no APN is provided by the UE, cf. 23.401 [16], clause 3.

A2. The MME-RN runs EPS AKA with the RN and the USIM-RN and establishes NAS security. The RN shall use only keys in an RN attach procedure that were received from the USIM-RN over the Secure Channel.

A3. The MME-RN checks from the RN-specific subscription data received from the HSS that the USIM-RN is dedicated to the use in RN attach procedures. If the RN requested access to an APN other than the default APN the MME shall reject the request. The MME-RN communicates the fact that the attachment is for relay nodes to the DeNB in an extended S1 INITIAL CONTEXT SETUP message.

A4. Upon receipt of the extended S1 INITIAL CONTEXT SETUP message the DeNB sets up RN-specific AS security over Un, which differs from AS security over Uu in that integrity protection for PDCP frames carrying S1/X2 messages is provided. The DeNB rejects any attach request by relay nodes for which no confirmation has been received from the MME-RN that the attachment is for relay nodes.

A5. According to step E4., a new TLS handshake including certificate validation according to E.5 is performed. The RN uses the IP connectivity of the RN to the default APN establishes in step A4 to communicate with the server providing certificate validation information.

A6. The RN sends a PDN connectivity request for the APNs required for performing its function as a relay node. The MME shall challenge this request by sending an Authentication request. After successful completion of the authentication procedure and a corresponding key-change-on-the-fly, the MME shall establish the requested PDN connectivity for the RN. The MME shall control the time elapsed between steps A2 and A6 by setting a suitable timer.

The RN start-up is now complete from a security point of view, and UEs can start attaching to the RN.

NOTE 2: The above procedure ensures that a certificate validation check is completed by the UICC during the RN attach procedure. This ensures in turn that the RN certificate has not expired, for details cf. 10.11.7.1.6.

10.11.7.1.3 USIM Binding Aspects in RN scenarios

For this profile, no particular binding between USIM and RN is required.

10.11.7.1.4 Enrolment procedures for RNs

No change from 10.11.4.

10.11.7.1.5 Secure management procedures for RNs

No change from 10.11.5.

10.11.7.1.6 Certificate validation

Profile 11A requires the UICC and the RN to perform certificate validation as described in clause 10.11.6.

10.11.7.2 Solution profile 11B

10.11.7.2.1 General

The basic idea of the solution for relay node security presented in this Annex is realizing a one-to-one binding of an RN and a USIM called USIM-RN. Such a one-to-one binding is realized in this solution either by using symmetric pre-shared keys (psk) or by certificates. In the psk case, the binding needs to be pre-established in the UICC and in the RN prior to deployment; in the certificate case, the binding needs to be pre-established only in the UICC prior to deployment. The use of certificates has the advantage that there is a standardized procedure for enrolling the private key corresponding to the certificate in the secure environment of the RN while the use of a psk requires manual operation for establishing the psk. A further advantage is that the name (identity) in the cert can be given at time of enrolment, and does not have to be pre-established. On the other hand, psk has the advantage that no PKI is required and the procedure after pre-establishment of the psk is simpler. When using certificates for this one-to-one binding, a part of the usual certificate handling is replaced by subscription handling, as explained in clause 10.11. 7.2.6.

When using certificates the UICC inserted in the RN contains two USIMs: a USIM-RN which shall perform any communication only via a secure channel, and a USIM-INI communicating with the RN without secure channel and used for initial IP connectivity purposes prior to RN attachment. The UICC shall establish a secure channel only with a particular relay node. The UCC verifies this relay node by means of data pre-established in the UICC.

When using psk only the USIM-RN is required. This USIM-RN shall perform any communication only via a secure channel.

USIM-INI (if required) and USIM-RN can be functionally identical to Rel-99 USIMs. But a restriction of the command set, compared to a Rel-99 USIM, may be appropriate. In addition, for the certificate-based case, there will be other requirements on the UICC to perform the TLS handshake (BIP-UICC server mode or UICC USB).

NOTE: The proposed solution with USIM-INI and USIM-RN does not imply new functionality on Rel-99 USIM. The secure channel features are at the UICC platform level and a UICC implementing the secure channel could contain Rel-99 USIM. Only additional files, for storing the RN identity and the use restriction (cf. step E.5 and NOTE there), and rules for certificate checking for the certificate-based case, are needed on the UICC.

10.11.7.2.2 Security Procedures

The start-up of an RN proceeds in the following steps. If one of the steps fails in any of the involved entities the procedure is aborted by that entity.

Phase I: Procedures prior to the RN attach procedure (certificate-based case)

E1. The RN performs an autonomous validation of the RN platform.

E2. The RN attaches as a UE using USIM-INI if step E3 needs to be performed.

E3. The RN obtains an operator certificate through the enrolment procedure defined in TS33.310 [7] unless an operator certificate is already available. Details can be found in clause 10.11.7.2.4. The RN optionally establishes a secure connection to an OAM server. Details can be found in clause 10.11.7.2.5. The RN shall retrieve a CRL from a suitable server, if no valid CRL is available locally in the RN.

E4. After completing step E3, the RN shall detach from the network and de-activate the USIM-INI if it attached in step E2.

E5. The RN platform secure environment and the UICC establish a Secure Channel between RN and USIM-RN according to ETSI TS 102 484 [12] clause 7 “Secured APDU” with TLS handshake. This TLS handshake shall be initiated by the RN and use certificates on both sides. The RN either uses a pre-established certificate or the certificate enrolled in step E3. The UICC verifies that this certificate is limited to use with relay nodes. The UICC is pre-provisioned with an operator root certificate to verify the RN certificate. The UICC certificate needs to be pre-installed in the UICC by the operator. The RN is provisioned with a root certificate to verify the UICC certificate.

E6. A certificate validation client on the UICC shall verify the signatures in the RN certificate chain up to the root certificate. The check of revocation status and expiry time is omitted. A certificate validation client on the RN shall check the verification of the signatures in the UICC certificate chain up to the root certificate as well as the revocation status and expiry time. Details can be found in clause 10.11.7.2.6. Furthermore, the requirements in clause X.2.3 on ‘USIM Binding Aspects’ shall apply.

NOTE 1: NOTE1 from clause 10.11.2 applies without changes.

The private key corresponding to the RN certificate and the root certificate used to verify the UICC certificate are stored in the secure environment of the RN platform validated in step E1, and the TLS connection terminates there. From the completion of this step onwards, all communication between the USIM-RN and the RN is protected by the Secure Channel. The USIM-RN shall not engage in any communication prior to the establishment of the Secure Channel.

NOTE 2: NOTE2 from clause 10.11.2 applies without changes.

NOTE 3: NOTE3 from clause 10.11.2 is not relevant for profile 11B. NOTE: NOTE4 from clause 10.11.2 applies with the added clarification “Hence the RN cannot attach as an RN to a network other than the one of the operator who provisioned the root certificate in the RN”.

NOTE 4: NOTE5 from clause 10.11.2 is modified to: “It is proposed here that the RN assumes the role of TLS client to be in line with ETSI TS 102 484 [12], clause 7, on “Secured APDU” with TLS handshake”. There is no need to reverse the roles of TLS client and server as there is no RN certificate validation in profile 11B.

NOTE 5: NOTE6 from clause 10.11.2 applies with the changes that, for the transaction counter, clause 5, instead of clause 7, of ETSI TS 102 484 [12], should be referenced, and that the text on counter on the AUTHENTICATE commands is deleted.

NOTE 6: NOTE7 from clause 10.11.2 is modified to: “Having two USIMs on one UICC is a standard feature available today (but only one USIM can be active at a time in current 3GPP specifications).” When the secure channel between USIM-RN and RN is being set up the connectivity provided by USIM-INI is not needed any more as there is no RN certificate validation in profile 11B.

NOTE 7: NOTE8 from clause 10.11.2 is modified to: “The RN could distinguish a USIM-RN from a USIM-INI e.g. by the use of so-called ‘Application Identifiers (AID)’ for UICC applications.”

Phase I: Procedures prior to the RN attach procedure (pre-shared key based case)

E1. The RN performs an autonomous validation of the RN platform.

E2. The RN platform secure environment and the UICC establish a Secure Channel between RN and USIM-RN according to ETSI TS 102 484 [12] clause 7 “Secured APDU” using a pre-shared key. Furthermore, the requirements in clause X.2.3 on ‘USIM Binding Aspects’ shall apply.

From the completion of this step onwards, all communication between the USIM-RN and the RN is protected by the Secure Channel. The USIM-RN shall not engage in any communication prior to the establishment of the Secure Channel.

E3. The RN optionally establishes a secure connection to an OAM server. Details can be found in clause 10.11.7.2.5.

E4. The RN may remain attached to the network if it attached for performing step E3.

E5. void

E6. void.

NOTE 1: The use of the pre-shared key variant requires that the RN is configured with this pre-shared key e.g. in the factory, or at the operator’s premises or in the field during RN installation. The corresponding procedures are out of scope of the present document. For the UICC, the regular personalization procedures are expected to apply.

NOTE 2: NOTEs from clause 10.11.2 do not apply to the pre-shared key case, except NOTE 6, which applies with the changes that, for the transaction counter, clause 5, instead of clause 7, of ETSI TS 102 484 [12] should be referenced, that the text on counter on the AUTHENTICATE commands is deleted, and that the text on TLS is irrelevant.

Phase II: RN attach procedure (pre-shared key case and certificate-based case)

It is required that a secure channel between RN and USIM-RN exists throughout the execution of phase II.

The RN performs the RN attach procedure for EPS as defined in TS36.300 [4], using the USIM-RN. From a security point of view, this involves the following steps:

A1. If the USIM-RN is not already active the RN activates it and resumes or re-establishes the secure channel. In the certificate-based case this resumption or re-establishment is done by a new TLS handshake. The RN invalidates any EPS security context on the USIM-RN. The RN uses the IMSI (or a related GUTI) pertaining to the USIM-RN in the RN attach procedure.

NOTE: NOTE9 from clause 10.11.2 applies without changes.

A2. The MME-RN runs EPS AKA with the RN and the USIM-RN and establishes NAS security. The RN shall use only keys in an RN attach procedure that were received from the USIM-RN over the Secure Channel.

A3. The MME-RN checks from the RN-specific subscription data received from the HSS that the USIM-RN is permitted for use in RN attach procedures. The MME-RN communicates the fact that the attachment is for relay nodes to the DeNB in an extended S1 INITIAL CONTEXT SETUP message.

A4. Upon receipt of the extended S1 INITIAL CONTEXT SETUP message the DeNB and the RN set up AS security over Un, which differs from AS security over Uu in that integrity protection for PDCP frames carrying S1/X2 messages is provided. Integrity protection for PDCP frames on Data Radio Bearers over Un carrying other types of data is optionally supported. The DeNB rejects to attach any node as a relay node for which no confirmation has been received from the MME-RN that the attachment is for relay nodes.

The RN start-up is now complete from a security point of view, and UEs can start attaching to the RN.

10.11.7.2.3 USIM Binding Aspects

There shall be a one-to-one association between the USIM-RN and the RN.

In the pre-shared key case, this one-to-one association is ensured by the fact that the key that is pre-shared between the USIM-RN and the RN shall not be available in any other entity.

In the certificate-based case, this one-to-one association is ensured by the following requirements:

- the UICC shall verify the RN identity, represented by the RN identity in the certificate, through the TLS handshake as part of the secure channel set-up;

- the identity in an RN certificate shall be unique;

a particular RN identity shall be available in only one UICC.The UICC may know the identity of the RN authorized to set up a secure channel with the USIM-RN by configuration. The standard secure OTA mechanisms (TS31.116 [9]) can be used to update the configuration of UICC and renew the stored identities if required.

NOTE: The RN identity may be contained in the subject name or the subjectAltName of the certificate. The uniqueness of the subject name in a certificate is required by RFC 5280 [19], 4.1.2.6: “Where it is non-empty, the subject field MUST contain an X.500 distinguished name (DN). The DN MUST be unique for each subject entity certified by the one CA as defined by the issuer field.”

Editor’s Note: It is ffs whether the subject or subjectAltName field is used for uniquely identifiying the RN in the scope of the present document.

Whenever the operator intends to prevent the RN from attaching to the network the operator shall bar the subscription relating to the USIM-RN in the HSS. In the certificate-based case, the barring of the subscription relating to the USIM-RN is performed also whenever instead of revoking the RN certificate has to be revoked.

10.11.7.2.4 Enrolment procedures for RNs

This subclause applies only to the certificate-based case.

The RN may enroll a device certificate as with macro eNBs according to TS33.310 [7] prior to the RN attach procedure with the DeNB. This certificate may then be used for establishing the secure channel between RN and USIM-RN.

The certificate enrolment procedure does not rely on the security at the AS level, but is secured at the application layer. It can be therefore executed before security on the Un interface has been established. However, the RN requires IP connectivity for the enrolment procedure to be able to reach the Registration Authority RA.

The IP connectivity required for enrolment may be established in the following ways:

(1) The RN may use offline means for enrolment purposes. No USIM is required.

(2) The RN may attach to an eNB like a normal UE using a USIM, called USIM-INI, different from the one used in the RN attach procedure to the DeNB, called USIM-RN. No secure channel between RN and USIM-INI is required.

In both cases, the network shall ensure that the destinations the RN can reach are restricted to only the PDN(s) where the RA (Registration Authority for the certificate enrolment) and the OAM server are located. In case (2) this shall be ensured by restricting IP traffic originating from the RN and sent over PDCP to only certain destinations (APNs) if connectivity established by means of USIM-INI is used. The restrictions are assumed to be part of the profile relating to the subscription associated with the USIM-INI.

10.11.7.2.5 Secure management procedures for RNs

The RN may establish a secure connection to an OAM server.

The OAM procedure does not rely on the security at the AS level. It can therefore be executed before security on the Un interface has been established. If no security on lower layers is available the communication between RN and OAM server would be typically secured using TLS. (This is up to the operator.) The RN requires IP connectivity for this procedure to be able to reach the OAM server.

For the pre-shared key case in Phase I, IP connectivity can be established after step E2 with the RN attaching to an eNB like a normal UE using the USIM-RN.

For the certificate-based case in Phase I, IP connectivity established for enrolment purposes according to clause 10.11.7.2.4 may be re-used, or, if not available, it may be established in the same ways as described in clause 10.11.7.2.4.

Restrictions on the destinations the RN can reach shall apply if the communication with the OAM server occurs prior to the RN attach procedure. They shall be realized in the same way as described in clause 10.11.7.2.4.

10.11.7.2.6 Certificate and subscription handling

This subclause applies only to the certificate-based case.

As described in clause 10.11.7.2.2, step E.6, the certificate validation client on the UICC verifies the signatures in the RN certificate chain up to the root certificate, but omits the check of revocation status and expiry time. The certificate is revoked by barring the associated USIM-RN subscription in the HSS. A certificate validation client on the RN shall check the verification of the signatures in the UICC certificate chain up to the root certificate as well as the revocation status and expiry time. The revocation status of the UICC certificate is checked by means of the CRL obtained by the RN in 10.11.7.2.2, step E.3. Consequently, no OCSP server is needed in profile 11B.

Further considerations on certificate and subscription handling for profile 11B:

By using the one-to-one binding of RN and USIM-RN, a part of the usual certificate handling is replaced by subscription handling, as explained below:

Binding in network: The one-to-one binding of RN and USIM-RN is technically expressed by a one-to-one mapping of the RN identity, in any certificate issued to the RN and the IMSI in the USIM-RN. The operator would maintain a table with this mapping (the “mapping table”) .

Binding in UICC: cf. subclause 10.11.7.2.3.

Lifetime: The mapping table would also contain a limit on the lifetime of the subscription. When the lifetime of the subscription is up the subscription is barred in the HSS. The lifetime does not have to coincide with the lifetime of the certificate. The latter is not checked in the UICC, cf. subclause 10.11.7.2.2 step E6 (certificate-based case).

RN Certificate revocation: Whenever an RN certificate needs to be revoked the operator does not use CRLs or OCSP, but retrieves the IMSI associated with the subject name in the certificate and bars the subscription corresponding to the IMSI in the HSS. This implies that no new certificate shall be issued for the same RN identityfrom that point onwards.

RN compromise: If the operator has reason to believe that an RN has been compromised the corresponding subscription shall be barred in the HSS.

RN Certificate renewal: This process works as normal as long as the RN identity in the RN certificate remains the same.

NOTE: Certificate renewal with private key change may be useful even if the UICC does not check the expiry time of the certificate as, in this way, the use of the private key can be limited if desired.

NOTE: RN Certificate expiry: As the UICC has no clock it cannot check the expiry time and, hence, the RN could also use an expired certificate in the secure channel set-up. As the certificate is only checked by the UICC for RN platform authentication in the secure channel set-up this is not a problem as long as the corresponding private key has not left the secure environment of the RN. More generally, if there is a risk that it has been compromised the operator will bar the corresponding subscription in the HSS. The use of the certificate is limited by the lifetime of the subscription bound to the RN. However, a UICC can be re-used with a different RN after having been re-configured with a different RN identity.

10.11.8 Analysis of Solution 11

10.11.8.1 How does solution 11 address the threats in clause 5?

Threat 1: Impersonation of a RN to attack user attached to RN

The text in clause 5.3 states that threat 1 can be countered by device authentication (i.e. platform authentication). By the definition in clause 3.1, platform authentication “is performed between a secure environment in the RN platform and a network entity". No such protocol between a secure environment in the RN platform and a network entity is run in solution 11, but nevertheless solution 11 implicitly provides the same assurances to the MME-RN as platform authentication would provide, as can be seen from the following reasoning, in which we repeatedly refer to the elements of the definition in clause 3.1 We can therefore say that the solution in clause 7.12 provides implicit platform authentication to the MME-RN.

Definition from clause 3.1: "…the network entity has verified that the secure environment in the RN is in possession of a secret key associated with the RN."

Solution in clause 10.11: In short, the MME-RN delegates the platform authentication of the RN to the UICC and trusts that the USIM-RN on the UICC engages in an AKA run only after successful platform authentication of the RN. In more detail: The MME-RN successfully runs EPS AKA with the RN and USIM-RN. This is only possible when the USIM-RN engages in AKA-related communication with the terminal (i.e. here: the RN) in which it is inserted. The MME-RN knows that the USIM-RN is dedicated to be used in RN attach procedures and that such USIMs communicate with terminals only over secure channels. Furthermore, they do so only after they checked the validity of the terminal (i.e. here: the RN) certificate by means of certificate validation and that the certificate is limited to use with relay nodes, cf. clause 10.11.2. Hence the MME-RN concludes that the UICC has successfully checked that the RN has a valid certificate and the corresponding private key. But an RN private key corresponding to a valid certificate limited to use with relay nodes resides in the secure environment of a relay node. The RN attach procedure hence tells the MME-RN that the attached entity indeed resides on an RN platform, but it does not provide the MME-RN yet with a verified identity of an individual device. If the latter is also desired the RN can send the IMEI or another suitable identity via the NAS protocol to the MME-RN, as explained in clause 10.11.3. This completes the argument. For profile 11B of solution 11 the argument slightly varies in that the RN attach procedure will fail in the MME when the certificate tied to the subscription has been revoked or expired as then the subscription is barred.

Definition from clause 3.1: "RN platform authentication is intended to additionally provide implicit proof of the integrity of the RN platform to the network entity. This is achieved by assuming that the secure environment in the RN engages in RN platform authentication only after a successful autonomous RN platform validation has been performed."

Solution in clause 10.11: A secure environment in a genuine RN engages in the set-up of a secure channel with the USIM-RN only after a successful autonomous RN platform validation has been performed, and the USIM-RN verifies that it has set up a secure channel with a genuine RN, cf. clause 10.11.2. As the MME-RN learnt in the previous step that such a secure channel was successfully established the MME-RN can also conclude that a successful autonomous RN platform validation has been performed.

Threat 2: MitM on the Un interface between RN and DeNB

The description of threat 2 in clause 5.3 requires inserting the real UICC into the MitM node. This is prevented by the fact that the USIM-RN on the UICC checks whether the secure channel with a real RN has been set up successfully before engaging in AKA-related communication. The necessary validity check of the RN certificate is performed differently in profiles 11A and 11B, cf. clause 10.11.7.

In profile 11A according to clause 10.11.7.1 the UICC performs a complete validity check of the RN certificate including check of expiry and revocation status.

In profile 11B according to clause 10.11.7.2 the UICC only performs a check of the signature chain up to the root certificate, thus validating that the certificate chain really extends to the preconfigured root certificate. Expiry and revocation check in the UICC is replaced by the one-to-one binding of RN and USIM-RN. In this case a USIM-RN would still establish a secure channel with a RN presenting an expired or revoked certificate, but the AKA authentication of USIM-RN performed later would not succeed, as the USIM-RN is barred if the certificate is expired or revoked. Thus also in this case the MitM-RN could not attach as RN to the DeNB.

In addition the description of threat 2 in clause 5.3 assumes that a fake UICC can be inserted in a real RN. This is prevented in both profiles of solution 11 by the fact that the RN checks whether the secure channel with the USIM has been set up successfully before performing the RN attach procedure.

Threat 3: Attacking the traffic on the Un interface between RN and DeNB

Integrity protection of S1-AP and X2-AP signalling across the Un interface is provided by enhanced AS security between RN and DeNB. Other traffic over Un is sufficiently protected by AS security.

Threat 4: Impersonation of a RN to attack the network

The RN attach procedure can be successfully performed only by genuine RNs as explained in the reply to threat 1 above and in clause 10.11.

Threat 5: Attacks on the interface between the RN and the UICC

The attacks are prevented by the secure channel between the USIM and the RN. More precisely: as stated in clause 10.11.2, it is ensured that no NAS security context exists in the RN or the USIM-RN immediately prior to the set-up of the secure channel between USIM-RN and RN as the secure channel is a precondition for running EPS AKA with the USIM-RN. The RN attach procedure happens only after the secure channel between USIM-RN and RN has been set up. In this way, the RN ensures that the keys sent from the USIM-RN to the RN from which the AS security context on Un is derived were received by the RN through the secure channel. The MME-RN knows that the integrity of the platform of the RN attempting to attach is guaranteed, cf. response to threat 1. Hence the MME-RN knows that this RN has checked that the secure channel was in place before the start of the RN attach procedure, so the MME-RN knows that the AS keys are not compromised by attacks on the interface between RN and UICC, and, consequently, the MME-RN can hand the relevant part of the AS security context down to the DeNB for RN-specific AS security set-up, cf. step A.3 in clause 10.11.2. Furthermore, the RN is protected from accepting keys from a rogue UICC by checking the UICC certificate in the set-up of the secure channel, cf. NOTE2 in clause 10.11.2.

Threat 6: Control of the RN platform

This threat is prevented by autonomous validation and implicit platform authentication, cf. response to threat 1.

Threat 7: DoS type attacks

The description of this threat has two parts:

a) From clause 5.3: "When the attacker removes the USIM, RN without USIM can't be authenticated by the network. So the legal RN can't connect to network and provide services."
Response: An attacker removing a USIM could just as easily physically destroy the RN so this type of DoS cannot be prevented.

b) From clause 5.3: "The attacker could also insert the USIM into another RN, then the topology of access network will be changed and cause interference problem to other eNB."
Response: If the other RN is a fake then the threat is the same as threat 1. If the other RN is genuine then there are several solutions on top of the solution in clause 10.11 for ensuring that the binding between USIM and RN is authorized. Possible solutions are listed in clause 10.11.3.

10.11.8.2 How does the solution 11 fulfill the requirements in clause 6?

We quote text from clause 6.

"If end to end protection between the RN and the core network is needed, then the same solution as for backhaul protection should be considered."

Response: But e2e protection is not possible due to the chosen architecture alternative, as stated in the next paragraph, so this sentence should be removed.

"Integrity protection for the S1 control plane traffic over the Un shall be mandatory."

Response: This is provided in this solution by the mandatory use of integrity protection in the enhanced AS security between RN and DeNB.

"The S1 control plane traffic between RN and MME-UE shall be integrity protected between the DeNB and the MME-UE with at least the same strength as in the current EPS architecture."

Response: This requirement seems compatible with all solutions described in clause 10. It is addressed as in clause 11 of TS 33.401 [2] today.

"Integrity protection for the X2 control plane traffic over the Un shall be mandatory. The X2 control plane traffic between RN and eNB/RN shall be integrity protected between the DeNB and the eNB/RN with at least the same strength as in the current EPS architecture."

Response: same as for S1 traffic.

"Mutual authentication between RN and network shall be supported."

Response: This is a bit vague as the authenticating network entity is not mentioned. Mutual authentication between RN and MME-RN is provided by EPS AKA performed according to TS 33.401 [2].

"Relay device authentication is mandatory."

Response: cf. response in clause 10.11.8.1 to threat 1 where it is explained that implicit platform authentication is provided.

"The DeNB shall not accept or send S1-AP and X2-AP message from/to the RN until a successful Relay device authentication has happened."

Response: cf. response in clause 10.11.8.1to threat 1 where it is explained that implicit platform authentication is provided as part of the RN attach procedure.

"Security of RN Management shall be guaranteed."

Response: this requirement seems compatible with all solutions described in clause 7. Either a separate TLS connection is set up to the OAM server, or, after the successful completion of the RN attach procedure, the management traffic is secured hop-by-hop.

"The wireless resource: security shall be able to prevent misuse by identifying whether the attached terminal is a UE or a RN. The identification could be implicit."

Response: this requirement is addressed by step A.3 in clause 10.11.2: the MME-RN "checks from the RN-specific subscription data received from the HSS that the USIM-RN is dedicated to the use in RN attach procedures.".

"The connection between relay and network should be confidentiality protected. Confidential protection for the S1/X2 user plane traffic over the Un should provide protection as same as the user plane data transferred on Uu interface, i.e. provide optional confidentiality protection on Un interface."

Response: this is provided by AS security.

"Both user plane and control plane must be considered as they may not require the same level of protection."

Response: this solution satisfies this requirement by using enhanced AS security.

"The RN platform shall protect from reading and/or modification of security parameters and security functions by unauthorized parties (platform security). The integrity of the RN platform shall be validated as part of the RN start up procedure."

Response: cf. response in clause 10.11.8.1 to threat 1 where it is explained that implicit platform authentication and platform integrity are provided as part of the RN attach procedure.

"RN specific device security features, e.g. security storage of sensitive data, device integrity check, USIM aspects, shall be considered."

Response: for secure storage and device integrity cf. the preceding response, for USIM aspects a secure channel is provided, and the binding aspects between particular USIMS and RNs are considered in clause 10.11.3.

10.11.8.3 How does the solution 11 address the general Editor's notes and the residual threats in clause 8.1.2.1?

The solution in clause 10.11 is a more detailed version of Option 2: "AS security over the Un interface" described in clause 8.1.2.2. We quote from clause 8.1.2.2.

"…Option 2 must be ruled out unless Un security is modified such that integrity protection is provided in the Un user plane at least for PDCP PDUs carrying S1 signalling."

Response: the solution is based on the assumption that AS security is suitably enhanced over Un.

"An issue with this alternative is that it may require strong assurance of a binding of USIM and RN. Current eNBs do not provide this binding feature..."

Response: The strong binding is provided by the secure channel between RN and USIM-RN.

"The donor eNB must know if a particular subscription is a RN subscription or a UE subscription so the donor eNB must know if it is authorised to pass S1-AP traffic to the RN. It requires further study whether this requirement can be supported using the current S1-AP protocol and/or core network procedures. Furthermore the donor eNB must know that it has to apply the Un security procedures which are by assumption different to the Uu procedures."

Response: The DeNB obtains this information from the MME-RN, cf. step A.3 in clause 10.11.2.

"**Residual Threat:** as already noted in 8.1.1, integrity protection of S1-UE is required, but can be only guaranteed if the AS security mechanisms on Un are modified with respect to Uu as Uu does not provide integrity on DRBs. Furthermore, all threats that apply to RRC and UP-UE in case 8.1.2.2.2 now apply to all traffic over Un.

Editor's Note: threats to AS security for all traffic over Un need further study. Integrity protection for S1 -UE traffic needs further study."

Response: The threats to AS security in general are those for Rel-8 LTE. It is indeed ffs how AS integrity protection can be provided for S1/X2. But this is the task of RAN2, not SA3.

10.12 Solution 12 – Secure Channel between USIM and RN and AS integrity for S1 /X2; Variant with modified KASME

Editor's note: The certificate validation mechanism needs to be detailed further.

Editor's note: The supporting infrastructure and operational procedures need further description.

Editor's note: This solution works only with an MME enhanced for relay nodes. It is ffs how an eNB can direct an RN to such an MME in the initial phase. This further study includes considerations on the impact on RAN specifications.

10.12.1 General

The main features of this solution are: (1) Autonomous validation of the RN platform; (2) Secure Channel between USIM-RN and RN; (3) certificate validation client on the UICC; (4) AS integrity for S1 /X2; (5) Computation of K_{ASME} on the UICC; (6) Key derivation function for K_{ASME} dependent on whether a secure channel is established.

The solution is further characterized by the fact that the MME-RN delegates the platform authentication of the RN to the UICC and trusts that the USIM-RN on the UICC engages in an AKA run usable in an RN attach procedure only after successful platform authentication of the RN, cf. clause 10.12.7.

The USIM-RN has the following additional properties compared to a Rel-8 USIM:

- K_{ASME} is computed on the UICC. This K_{ASME} is identical to the K_{ASME} that is computed in the HSS according to TS 33.401 [2], A.2, and transferred from the HSS to the MME-RN.

NOTE: TS 33.401 [2], clause 6.1, NOTE 5, already mentions the possibility of computing K_{ASME} on the UICC.

- When a secure channel exists between USIM-RN and RN then K_{ASME} is transferred from the USIM-RN to the RN.
- When no secure channel exists between USIM-RN and RN then only $K_{ASME}* = H (K_{ASME})$ is transferred from the USIM-RN to the RN where H is a one-way hash function.
- CK and IK do not leave the UICC. In particular, when the UICC supports storage of (parts of) the EPS security context then the RN can retrieve only K_{ASME} or $K_{ASME}*$, not CK and IK, from the UICC.

10.12.2 Security Procedures

The start-up of an RN proceeds in the following steps. If one of the steps fails in any of the involved entities the procedure is aborted by that entity.

Procedures prior to the RN attach procedure

E1. The RN performs an autonomous validation of the RN platform.

E2. The RN attaches as a UE using USIM-RN to be prepared for performing steps E5. and, optionally, E3. The attach request shall indicate “RN attaching as UE”. When the MME-RN receives an attach request with this indication the MME-RN computes $K_{ASME}* = H (K_{ASME})$ and uses it in further key derivations instead of K_{ASME}. The USIM-RN computes $K_{ASME}* = H (K_{ASME})$ and returns this key to the RN, as the AUTHENTICATE command was received by the USIM-RN over an unsecured channel.

E3. The RN optionally obtains an operator certificate through the enrolment procedures defined in TS33.310 [7]. Details can be found in clause 10.12.4. The RN optionally establishes a secure connection to an OAM server. Details can be found in clause 10.12.5.

E4. The RN and the UICC establish a Secure Channel between RN and USIM-RN according to ETSI TS 102 484 [12] by means of a TLS connection. This TLS connection shall be initiated by the UICC and use certificates on both sides. The RN uses a pre-established certificate or the certificate enrolled in step E3. The UICC verifies that this certificate is limited to use with relay nodes. The UICC is pre-provisioned with a root certificate to verify the RN certificate. The UICC certificate needs to be pre-installed in the UICC by the operator. The RN is pre-provisioned with a root certificate to verify the UICC certificate.

The private key corresponding to the RN certificate is stored in the secure environment of the RN platform validated in step E1, and the TLS connection terminates there. From the completion of this step onwards, all communication between the USIM-RN and the RN is protected by the Secure Channel.

NOTE 1: Certificate use restriction may be made possible e.g. through a suitable name structure, or a particular intermediate CA in the verification path, or policy information terms, e.g. by a suitable object identifier (OID) in the certificate policies extension.

E5. An certificate validation client on the UICC checks the validity of RN certificate used in the secure channel set-up with an certificate validation server. An certificate validation client on the RN checks the validity of UICC certificate used in the secure channel set-up with an certificate validation server. Details can be found in clause 10.12.6.

E6. The RN detaches from the network if it has attached for performing steps E2, E3, or E5.

NOTE 2: ETSI TS 102 484 [12] states in clause 6.2.2: “The UICC may present a self-signed certificate. The terminal or terminal application should temporarily accept such a certificate during the TLS handshake protocol, if it is able to establish by other means (e.g. successful network authentication) that the handshake protocol is conducted with an authentic UICC.” And in the present solution for relay node security, the RN indeed verifies the authenticity of the USIM-RN by means of a successful RN attach procedure. However, the use of a self-signed UICC certificate, or no UICC certificate at all, would weaken network-to-RN authentication in cases where both the interfaces of the RN with the UICC and the network were under the control of an attacker. (Think of a stolen RN in a rogue environment.) Then the RN would happily use any key fed to it over the interface with a fake UICC and use this key in the communication with a fake network. (It is ffs how serious this threat is.) The use of a UICC certificate prevents this threat as no rogue UICC can set up a secure channel with the RN.

NOTE 3: ETSI TS 102 484 [12] states in clause 6.2: “Both the terminal or the UICC shall be able to initiate a TLS secure channel.” It is proposed here that the UICC assumes the role of TLS client for the following reason:
the certificate validation in step E.5 can be integrated with TLS according to RFC 4366 [13], otherwise the certificate validation would have to be a separate procedure following the TLS procedure.

NOTE 4: One may want to limit the lifetime of a secure channel between USIM-RN and RN for security reasons. Suitable counters providing such a limit include a record counter, cf. clause 6.4 of ETSI TS 102 484 [12], or a counter on the AUTHENTICATE commands received over the secure channel. To disallow the the resumption of TLS session, and to enforce a new TLS handshake on each RN attach, the USIM-RN may be configured accordingly, if necessary.

RN attach procedure

The RN performs the RN attach procedure for EPS as defined in TS 36.300 [4]. From a security point of view, this involves the following steps:

A1. The RN invalidates any EPS security context on the USIM-RN. The attach request shall indicate “RN attaching as relay”.

A2. The MME-RN runs EPS AKA with the RN and the USIM-RN and establishes NAS security. The USIM-RN computes K_{ASME} and returns this key to the RN, as the AUTHENTICATE command was received by the USIM-RN over a secured channel. The RN shall use only keys in an RN attach procedure that were received from the USIM-RN over the Secure Channel.

A3. The MME-RN checks from the RN-specific subscription data received from the HSS that the USIM-RN is dedicated to the use in relay node procedures. When the MME-RN receives an attach request without the indication "RN attaching as UE" the MME-RN takes K_{ASME} as received from the HSS and uses it in further key derivations instead of K_{ASME} . The MME-RN communicates the fact that the attachment is for relay nodes to the DeNB in an extended S1 INITIAL CONTEXT SETUP message.
(It is ffs whether an explicit indication in the RN attach request is required. It is also ffs whether other S1 messages would have to be similarly extended.)

A4. Upon receipt of the extended S1 INITIAL CONTEXT SETUP message the DeNB sets up RN-specific AS security over Un, which differs from AS security over Uu in that integrity protection for PDCP frames carrying S1/X2 messages is provided. The DeNB rejects any RN attach request by relay nodes for which no confirmation has been received from the MME-RN that the attachment is for relay nodes.

The RN start-up is now complete from a security point of view, and UEs can start attaching to the RN.

10.12.3 USIM Binding Aspects in RN scenarios

The requirement of restricting the possible combinations of particular RNs and particular USIM-RNs is ffs, cf. clause 9.4. If such restrictions are required then authorization is required that could be enforced in at least one of the following ways:

(1) The RN enforces the allowed combinations.
The RN verifies the IMSI pertaining to the USIM-RN through a successful EPS AKA run involving the USIM-RN. The RN can then learn about the allowed combinations of USIM-RN and RN as follows:

(1a) The RN knows the authorized USIM-RNs by configuration;

(1b) The OAM server with which a secure connection was established in step E.3 tells the RN the authorized identities;

NOTE: The check whether the binding between RN and USIM-RN is authorized can be entrusted to an RN with a validated platform. But only such RNs are able to establish a secure channel with a USIM-RN, which in turn is a pre-requisite for a successful RN attachment to the network, cf. clause 7.13.2. Hence the network can trust that the RN performs the check faithfully.

(2) The UICC enforces the allowed combinations.
The UICC verifies the RN identity through the TLS secure channel set-up. The UICC knows the authorized RNs by configuration The standard secure OTA mechanisms (TS31.116 [9]) can be used to update the configuration of UICC and renew the stored identities if required.

(3) The MME enforces the allowed combinations.
The MME-RN may learn the RN device identity in a way similar to an MME learning the IMEI of a UE. As the RN platform is validated, it is ensured that the RN communicates the correct platform identity. The MME-RN then performs the check whether this combination of USIM and RN is authorized. The MME-RN may obtain the authorization information from the HSS.

Editor's Note: It is ffs whether the IMEI could serve as the RN device identity. If not a new NAS message or message field for sending the RN device identity may be required.

10.12.4 Enrolment procedures for RNs

The RN may enroll a device certificate as with macro eNBs according to TS33.310 [7] prior to the RN attach procedure with the DeNB. This certificate may then be used for establishing the secure channel between RN and USIM.

The certificate enrolment procedure does not rely on the security at the AS level, but is secured at the application layer. It can be therefore executed before security on the Un interface has been established. However, the RN requires IP connectivity for the enrolment procedure to be able to reach the Registration Authority RA. The IP connectivity could be established in various ways:

(1) The RN uses offline means for enrolment purposes. No USIM is required.

(2) The RN attaches to an eNB like a normal UE using the USIM-RN. No secure channel between RN and USIM-RN is required.

In both cases, the network must ensure that the destinations the RN can reach are restricted, e.g. to only the PDN(s) where the RA, the OAM server and the certificate validation server are located. In case (2) this could be ensured e.g. by restricting IP traffic originating from the RN and sent over PDCP without integrity protection to only certain destinations (APNs). The restrictions are assumed to be part of the profile relating to the subscription associated with the USIM-RN, but are to be applied by the MME only when the RN attaches as a UE (which is signalled in the Attach request, according to clause 10.12.2).

10.12.5 Secure management procedures for RNs

The RN may establish a secure connection to an OAM server.

The OAM procedure does not rely on the security at the AS level. It can therefore be executed before security on the Un interface has been established. If no security on lower layers is available the communication between RN and OAM server would be typically secured using TLS. The RN requires IP connectivity for this procedure to be able to reach the OAM server. The IP connectivity established for enrolment purposes according to clause 10.12.4 could be re-used, or, if not available, it could be established in the same ways as described in clause 10.12.4.

Restrictions on the destinations the RN can reach must apply if the communication with the OAM server occurs prior to the RN attach procedure. They can be realized similar to what is described in clause 11.12.4.

10.12.6 Certificate validation checks

The solution in this clause requires the UICC and the RN to perform certificate validation checks of the RN certificate and the UICC certificate respectively used for the set up of the secure channel prior to the RN attach procedure with the DeNB. The certificate validation protocol is self-secured and can therefore be executed before security on the Un interface has been established. The certificate validation client on the UICC needs to send the IP packets carrying the certificate validation message via the RN. The RN requires IP connectivity for the certificate validation checks to be able to reach the certificate validation server. The IP connectivity, and the restrictions on permitted destinations, can be established as described in clause 10.12.4 case (2). The certificate validation checks in step E5. of clause 10.12.2, can be integrated with the TLS handshake performed in step E4, according to RFC 4366 [13].

Editor's note: it is ffs whether OCSP can be used for certificate validation.

10.12.7 Analysis of Solution 12

10.12.7.1 How does solution 12 address the threats in clause 5?

Threat 1: Impersonation of a RN to attack user attached to RN

The text in clause 5.3 states that threat 1 can be countered by device authentication (i.e. platform authentication). By the definition in clause 3.1, platform authentication "is performed between a secure environment in the RN platform and a network entity". No such protocol between a secure environment in the RN platform and a network entity is run in solution 12, but nevertheless solution 12 implicitly provides the same assurances to the MME-RN as platform authentication would provide, as can be seen from the following reasoning, in which we repeatedly refer to the elements of the definition in clause 3.1. We can therefore say that the solution in clause 7.13 provides implicit platform authentication to the MME-RN.

Definition from clause 3.1: "…the network entity has verified that the secure environment in the RN is in possession of a secret key associated with the RN."

Solution in clause 10.12: In short, the MME-RN delegates the platform authentication of the RN to the UICC and trusts that the USIM-RN on the UICC engages in an AKA run usable in an RN attach procedure only after successful platform authentication of the RN. In more detail: The MME-RN successfully runs EPS AKA with the RN and USIM-RN using K_{ASME} as defined in TS 33.401 [2]. This is only possible when the USIM-RN engages in AKA-related communication with the terminal (i.e. here: the RN) in which it is inserted. The MME-RN knows that the USIM-RN is dedicated to the use in relay node procedures and that such USIMs transfer K_{ASME} to terminals only over secure channels, and never transfer CK, IK. Furthermore, they do so only after they checked the validity of the RN certificate by means of certificate validation and that the certificate is limited to use with relay nodes, cf. clause 10.12.2. Hence the MME-RN concludes that the UICC has successfully checked that the RN has a valid certificate and the corresponding private key. But an RN private key corresponding to a valid certificate limited to use in relay node procedures resides in the secure environment of a relay node. The RN attach procedure hence tells the MME-RN that the attached entity indeed resides on an RN platform with a secure environment, but it does not provide the MME-RN yet with a verified identity of an individual device. If the latter is also desired the RN can send the IMEI or another suitable identity via the NAS protocol to the MME-RN, as explained in clause 10.12.3. This completes the argument.

Definition from clause 3.1: "RN platform authentication is intended to additionally provide implicit proof of the integrity of the RN platform to the network entity. This is achieved by assuming that the secure environment in the RN engages in RN platform authentication only after a successful autonomous RN platform validation has been performed."

Solution in clause 10.12: A secure environment in a genuine RN engages in the set-up of a secure channel with the USIM-RN only after a successful autonomous RN platform validation has been performed, and the USIM-RN verifies that it has set up a secure channel with a genuine RN, cf. clause 10.12.2. As the MME-RN learnt in the previous step that such a secure channel was successfully established the MME-RN can also conclude that a successful autonomous RN platform validation has been performed.

Threat 2: MitM on the Un interface between RN and DeNB

The description of threat 2 in clause 5.3 requires inserting the real UICC into the MitM node. This is prevented by the fact that the UICC checks whether the secure channel with a real RN has been set up successfully before engaging in AKA-related communication.

Threat 3: Attacking the traffic on the Un interface between RN and DeNB

Integrity protection of S1-AP and X2-AP signalling across the Un interface is provided by enhanced AS security between RN and DeNB. Other traffic over Un is sufficiently protected by AS security.

Threat 4: Impersonation of a RN to attack the network

The RN attach procedure can be successfully performed only by genuine RNs as explained in the reply to threat 1 above and in clause 10.12.

Threat 5: Attacks on the interface between the RN and the UICC

The attacks are prevented by the secure channel between the USIM and the RN. More precisely: as stated in clause 10.12.2, it is ensured that no NAS security context exists in the RN or the USIM-RN immediately prior to the set-up of the secure channel between USIM-RN and RN as the secure channel is a precondition for K_{ASME} transferring to the RN. The RN attach procedure happens only after the secure channel between USIM-RN and RN has been set up. In this way, the RN ensures that the keys sent from the USIM-RN to the RN from which the AS security context on Un is derived in the RN attach procedure were received by the RN through the secure channel. The MME-RN knows that the integrity of the platform of the RN attempting to attach is guaranteed, cf. response to threat 1. Hence the MME-RN knows that this RN has checked that the secure channel was in place before the start of the RN attach procedure, so the MME-RN knows that the AS keys are not compromised by attacks on the interface between RN and UICC, and, consequently, the MME-RN can hand the relevant part of the AS security context down to the DeNB for RN-specific AS security set-up, cf. step A.3 in clause 10.12.2. Furthermore, the RN is protected from accepting keys from a rogue UICC by checking the UICC certificate in the set-up of the secure channel, cf. NOTE 2 in clause 10.12.2.

Threat 6: Control of the RN platform

This threat is prevented by autonomous validation and implicit platform authentication, cf. response to threat 1.

Threat 7: DoS type attacks

The description of this threat has two parts:

a) From clause 5.3: "When the attacker removes the USIM, RN without USIM can't be authenticated by the network. So the legal RN can't connect to network and provide services."
Response: An attacker removing a USIM could just as easily physically destroy the RN so this type of DoS cannot be prevented.

b) From clause 5.3: "The attacker could also insert the USIM into another RN, then the topology of access network will be changed and cause interference problem to other eNB."
Response: If the other RN is a fake then the threat is the same as threat 1. If the other RN is genuine then there are several solutions on top of the solution in clause 10.12 for ensuring that the binding between USIM and RN is authorized. Possible solutions are listed in clause 10.12.3.

10.12.7.2 How does the solution 12 fulfill the requirements in clause 6?

We quote text from clause 6.

"If end to end protection between the RN and the core network is needed, then the same solution as for backhaul protection should be considered."

Response: But e2e protection is not possible due to the chosen architecture alternative, as stated in the next paragraph, so this sentence should be removed.

"Integrity protection for the S1 control plane traffic over the Un shall be mandatory."

Response: This is provided in this solution by the mandatory use of integrity protection in the enhanced AS security between RN and DeNB.

"The S1 control plane traffic between RN and MME-UE shall be integrity protected between the DeNB and the MME-UE with at least the same strength as in the current EPS architecture."

Response: This requirement seems compatible with all solutions described in clause 7. It is addressed as in clause 11 of TS 33.401 [2] today.

"Integrity protection for the X2 control plane traffic over the Un shall be mandatory. The X2 control plane traffic between RN and eNB/RN shall be integrity protected between the DeNB and the eNB/RN with at least the same strength as in the current EPS architecture."

Response: same as for S1 traffic.

"Mutual authentication between RN and network shall be supported."

Response: This is a bit vague as the authenticating network entity is not mentioned. Mutual authentication between RN and MME-RN is provided by EPS AKA performed according to TS 33.401.

"Relay device authentication is mandatory."

Response: cf. response to threat 1 where it is explained that implicit platform authentication is provided.

"The DeNB shall not accept or send S1-AP and X2-AP message from/to the RN until a successful Relay device authentication has happened."

Response: cf. response to threat 1 where it is explained that implicit platform authentication is provided as part of the RN attach procedure.

"Security of RN Management shall be guaranteed."

Response: this requirement seems compatible with all solutions described in clause 10. Either a separate TLS connection is set up to the OAM server, or, after the successful completion of the RN attach procedure, the management traffic is secured hop-by-hop.

"The wireless resource: security shall be able to prevent misuse by identifying whether the attached terminal is a UE or a RN. The identification could be implicit."

Response: this requirement is addressed by step A.3 in clause 10.12.2: the MME-RN "checks from the RN-specific subscription data received from the HSS that the USIM-RN is dedicated to the use in relay node procedures." .

"The connection between relay and network should be confidentiality protected. Confidential protection for the S1/X2 user plane traffic over the Un should provide protection as same as the user plane data transferred on Uu interface, i.e. provide optional confidentiality protection on Un interface."

Response: this is provided by AS security.

"Both user plane and control plane must be considered as they may not require the same level of protection."

Response: this solution satifies this requirement by using enhanced AS security.

"The RN platform shall protect from reading and/or modification of security parameters and security functions by unauthorized parties (platform security). The integrity of the RN platform shall be validated as part of the RN start up procedure."

Response: cf. response to threat 1 where it is explained that implicit platform authentication and platform integrity are provided as part of the RN attach procedure.

"RN specific device security features, e.g. security storage of sensitive data, device integrity check, USIM aspects, shall be considered."

Response: for secure storage and device integrity cf. the preceding response, for USIM aspects a secure channel is provided, and the binding aspects between particular USIMS and RNs are considered in clause 10.12.3.

10.12.7.3 How does the solution 12 address the general Editor's notes and the residual threats in clause 8.1.2.1?

The solution in clause 10.12 is a more detailed version of Option 2: "AS security over the Un interface" described in clause 8.1.2.2. We quote from clause 8.1.2.2.

"…Option 2 must be ruled out unless Un security is modified such that integrity protection is provided in the Un user plane at least for PDCP PDUs carrying S1 signalling."

Response: the solution is based on the assumption that AS security is suitably enhanced over Un.

"An issue with this alternative is that it may require strong assurance of a binding of USIM and RN. Current eNBs do not provide this binding feature..."

Response: The strong binding is provided by the secure channel between RN and USIM-RN.

"The donor eNB must know if a particular subscription is a RN subscription or a UE subscription so the donor eNB must know if it is authorised to pass S1-AP traffic to the RN. It requires further study whether this requirement can be supported using the current S1-AP protocol and/or core network procedures. Furthermore the donor eNB must know that it has to apply the Un security procedures which are by assumption different to the Uu procedures."

Response: The DeNB obtains this information from the MME-RN, cf. step A.3 in clause 10.12.2.

"**Residual Threat:** as already noted in 8.1.1, integrity protection of S1-UE is required, but can be only guaranteed if the AS security mechanisms on Un are modified with respect to Uu as Uu does not provide integrity on DRBs. Furthermore, all threats that apply to RRC and UP-UE in case 8.1.2.2.2 now apply to all traffic over Un.

Editor's Note: threats to AS security for all traffic over Un need further study. Integrity protection for S1-UE traffic needs further study."

Response: The threats to AS security in general are those for Rel-8 LTE. It is indeed ffs by RAN2 and RAN3 how AS integrity protection can be provided for S1/X2.

11 Conclusions

It was agreed to select solution 11b.

Annex A: Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2010-12	SA#50	SP-100735	-	-	Submission to SA for Information	---	1.0.0
2011-02	SA#51	SP-110026	--	--	Submission to SA for Approval	1.0.0	2.0.0
2011-03	--	--	--	--	Publication	2.0.0	10.0.0