Advanced Security Framework for HRPD and eHRPD Systems
EDITOR

Zhibi Wang
Alcatel Lucent
Tel: (+1) 630-713-8381
Email: zhibi.wang@alcatel-lucent.com

REVISION HISTORY

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial Publication</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Advanced Security Framework for HRPD and eHRPD Systems ....................................................... i
2. Introduction ................................................................................................................................. 2
   2.1 Scope ..................................................................................................................................... 2
3. References ............................................................................................................................... 2
   3.1 Normative References ............................................................................................................ 2
   3.2 Informative References .......................................................................................................... 3
4. Definitions, Abbreviations and Acronyms ................................................................................. 3
   4.1 Definitions ............................................................................................................................. 3
   4.2 Abbreviations and Acronyms ............................................................................................... 3
   4.3 Terminology .......................................................................................................................... 4
5. Architecture .............................................................................................................................. 4
6. Security Requirements .............................................................................................................. 6
7. Access Authentication and Authorization .................................................................................. 7
   7.1 EAP Protocol Negotiation ..................................................................................................... 7
   7.2 UE Behavior .......................................................................................................................... 7
6.2.1 UE Identity Management for eHRPD .................................................................................. 7
   6.2.2 UE Identity Management for HRPD ................................................................................ 7
   6.2.3 UE Network Access Authentication for eHRPD .............................................................. 7
   6.2.4 UE Network Access Authentication for HRPD ............................................................... 8
   6.3 HSGW Behavior ................................................................................................................. 8
   6.4 PDSN Behavior ..................................................................................................................... 8
   6.5 AAA Server Behavior .......................................................................................................... 8
   6.5.1 3GPP AAA Server Behavior ........................................................................................... 8
   6.5.2 3GPP2 AAA Server Behavior .......................................................................................... 8
   6.6 HSS Behavior ....................................................................................................................... 8
7. Key Generation .......................................................................................................................... 8
   7.1 Pairwise Master Key (PMK) Generation ................................................................................ 9
   7.2 Access Network Key Generation ......................................................................................... 10
   7.3 Access Network Key Generation for AALS ........................................................................ 11
8. Key Distribution ......................................................................................................................... 12
   8.1 eHRPD Master Session Key and Inter-HSGW Handoff ....................................................... 12
   8.2 HSGW/PDSN – (e)AN Key Distribution ............................................................................. 12
   8.3 Multi-Key Key Exchange Protocol and Intra-HSGW/PDSN inter-eAN Handoff ............... 13
   8.3.1 Reconfiguration Procedures ......................................................................................... 13
<table>
<thead>
<tr>
<th>9</th>
<th>Session Key Usage for AALS</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>Derivation and Management of Crypto-sync</td>
<td>14</td>
</tr>
<tr>
<td>9.2</td>
<td>AALS EMFPA and AALS MLMFPA</td>
<td>14</td>
</tr>
<tr>
<td>9.3</td>
<td>Air Interface Application Signaling Encryption/Decryption functions</td>
<td>15</td>
</tr>
<tr>
<td>9.4</td>
<td>Air Interface Application Signaling Integrity Protection</td>
<td>15</td>
</tr>
</tbody>
</table>
1 Introduction

This document defines security framework for HRPD and eHRPD access networks.

This document describes only normal operation. Handling of error cases and unsuccessful scenarios resulting from protocol failures is described in other relevant standards.

1.1 Scope

This document defines updated security framework for HRPD and eHRPD access networks. It presents consolidation of advanced security features defined to support authentication, key distribution, efficient upper layer ciphering, and information integrity protection.

2 References

2.1 Normative References

<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1] 3GPP2: X.S0057-0</td>
<td>“E-UTRAN – eHRPD Connectivity and Interworking: Core Network Aspects”</td>
</tr>
<tr>
<td>[14] 3GPP: TS 24.302</td>
<td>“Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3; (Release 9)”</td>
</tr>
</tbody>
</table>
3GPP2: A.S0022-0: “E-UTRAN – eHRPD Connectivity and Interworking: Access Network Aspects (E-UTRAN – HRPD IOS)”.


3GPP2: C.S0039-0: Enhanced Subscriber Privacy for cdma2000 High Rate Packet Data.


NIST: [CMAC-NIST-SP800-38B], Special Publication 800-38B, ”Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication”, May 2005.

3GPP2: A.S0008-C: “Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces With Session Control in the Access Network”.

3GPP2: A.S0009-C: “Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces With Session Control in the Access Network”.


2.2 Informative References

This section provides references to other documents that may be useful for the reader of this document.

3 Definitions, Abbreviations and Acronyms

This section contains definitions, symbols and abbreviations that are used throughout the document.

3.1 Definitions

3.1.1 Abbreviations and Acronyms

The following list provides abbreviations and acronyms used throughout this document.

3GPP 3rd Generation Partnership Project
3GPP2 3rd Generation Partnership Project 2
AAA Authentication, Authorization, Accounting
AALS Air interface Application Layer Security
3.1.2 Terminology

In this document, the term UE has the same meaning as AT in HRPD system.

4 Architecture

Figure 1 below shows the eHRPD security reference model. An eHRPD UE connects to the Evolved Packet Core (EPC) through the HRPD Serving Gateway (HSGW). Before connection to the HSGW is allowed, the UE performs HRPD Access Authentication with the AN-AAA through the evolved Access Network (eAN) using the A12 interface. The HRPD Access Authentication procedures are specified in [20] and [21].

The eHRPD network access authentication of the UE is performed by the 3GPP AAA Server. The 3GPP AAA server retrieves the UE subscription data and the authentication vectors from the HSS through SWx interface. The 3GPP2 AAA Proxy plays the role of AAA proxy during authentication procedures. The details of authentication procedures are specified in [1].
Figure 1  eHRPD Security Reference Model

Figure 2 below illustrates the HRPD security reference model. An HPRD AT connects to the cdma2000 packet core network through the Packet Data Serving Node (PDSN). Before connection to the PDSN is allowed, the AT performs HRPD Access Authentication with the AN-AAA through the Access Network (AN) using the A12 interface. The HRPD Access Authentication procedures are specified in [20] and [21].

The PDSN authentication of an AT is performed by the 3GPP2 AAA. The 3GPP2 AAA server stores the AT subscription data and the authentication credential(s).
5 Security Requirements

The following security requirements shall be supported by the HRPD and eHRPD systems compliant to this document:

- Mutual authentication between the UE and the network shall be supported.
- It shall be possible to perform data encryption on a per link flow basis.
- Confidentiality and integrity protection of the (e)HRPD access network signalling messages shall be supported with the following exceptions:
  - Messages required to establish the security context between the UE and the network
  - Emergency calls for an unauthenticated UE.
  - Any messages that are explicitly identified as not being protected by the specifications.

NOTE: For best effort (e)HRPD signaling messages, confidentiality protection is not supported as it relies on HRPD Security Layer specified in [16].

- Confidentiality protection of user data shall be supported.
- Mechanisms to perform key exchange or update shall be supported.
• It should be possible to provide user identity confidentiality.

### 6 Access Authentication and Authorization

This section defines (e)HRPD authentication and authorization procedures. These authentication and authorization procedures are based on EAP.

Access authentication for eHRPD system shall be based on EAP-AKA’ specified in [11].

Access authentication for HRPD system shall use EAP-AKA as specified in [9].

#### 6.1 EAP Protocol Negotiation

EAP is used for network access authentication for (e)HRPD system. During the PPP session negotiation between the HSGW/PDSN and the UE, the HSGW/PDSN shall propose EAP as the authentication protocol in the LCP Configure-Request message by setting Authentication-Protocol option to C227 (see [6]).

Once the UE receives LCP Configure-Request message from the HSGW/PDSN that contains Authentication-Protocol option set to C227, the UE responds with LCP Configure-Ack, indicating to the HSGW/PDSN the acceptance of the EAP based authentication for PPP session establishment, as described in [6] and [4].

Once the HSGW/PDSN receives Configure-Ack from the UE indicating acceptance of the EAP based authentication, the HSGW/PDSN shall select EAP as the PPP authentication protocol and proceed to play the role of EAP authenticator.

#### 6.2 UE Behavior

The UE shall support the EAP-AKA’ protocol defined in [11] for eHRPD Network Access Authentication. Therefore, upon receiving the initial EAP Request indicating EAP-AKA’ as EAP method Type, the UE shall not respond with EAP Nak indicating that the authentication Type is unacceptable.

The UE shall support the EAP-AKA protocol defined in [9] for HRPD Network Access Authentication. Therefore, upon receiving the initial EAP Request indicating EAP-AKA as EAP method Type, the UE shall not respond with EAP Nak indicating that the authentication Type is unacceptable.

#### 6.2.1 UE Identity Management for eHRPD

The UE shall use IMSI of the UE as the permanent identity formatted as NAI for the Network Access authentication. The UE ID management for EAP-AKA’ shall be as specified in [1].

#### 6.2.2 UE Identity Management for HRPD

UE identity handling for EAP-AKA shall be as specified in [22].

#### 6.2.3 UE Network Access Authentication for eHRPD

The detailed procedure for the UE Access Authentication is specified in [1].
After successful access authentication, both the UE and HSGW derive identical values of MSK.

### 6.2.4 UE Network Access Authentication for HRPD

The detailed procedure for the UE Access Authentication is specified in [22].

After successful access authentication, both the UE and PDSN derive identical values of MSK.

### 6.3 HSGW Behavior

The HSGW behavior for EAP-AKA’ network access authentication shall comply with [1].

The HSGW shall play the role of authenticator.

### 6.4 PDSN Behavior

The PDSN behavior for EAP-AKA’ authentication shall comply with [1].

The HSGW shall play the role of authenticator.

### 6.5 AAA Server Behavior

For eHRPD, the 3GPP AAA Server acts as the EAP Authentication Server.

For HRPD, the 3GPP2 AAA Server acts as the EAP Authentication Server.

#### 6.5.1 3GPP AAA Server Behavior

The 3GPP AAA behavior for eHRPD shall comply with [1, 12].

#### 6.5.2 3GPP2 AAA Server Behavior

The 3GPP2 AAA behavior for HRPD shall comply with [22].

### 6.6 HSS Behavior

For eHRPD system, the 3GPP AAA server obtains the authentication vectors for network authentication from the HSS as defined in [12].

### 7 Key Generation

This section provides methods and procedures for generating the Pairwise Master Key (PMK) from MSK. The PMK in turn is used by the Key Exchange protocol to generate keys for over-the-air security protection.
A pictorial representation of PMK generation for eHRPD is provided in Figure 3, while detailed description is provided in following sub-sections.

**Figure 3  eHRPD Key Generation**

### 7.1 Pairwise Master Key (PMK) Generation

As a result of successful access authentication based on EAP-AKA' [11] both UE and HSGW obtain the MSK. The UE and HSGW separate the 512 bits of the MSK into four equal portions of 128 bits each, i.e., four Sub-MSKs. The UE and HSGW use each Sub-MSK to generate four PMKs as follows:

- \[ PMK1 = \text{HMAC-SHA-256}(\text{Sub-MSK}, \text{“pmk@hrpd.3gpp2”, 0x01}, [0:127] \]
- \[ PMK2 = \text{HMAC-SHA-256}(\text{Sub-MSK}, \text{“pmk@hrpd.3gpp2”, 0x01}) [128:255], \]
- \[ PMK3 = \text{HMAC-SHA-256}(\text{Sub-MSK}, \text{“pmk@hrpd.3gpp2”, 0x02}) [0:127], \]
- \[ PMK4 = \text{HMAC-SHA-256}(\text{Sub-MSK}, \text{“pmk@hrpd.3gpp2”, 0x02}) [128:255], \]

where the key label “pmk@hrpd.3gpp2” is set to ASCII strings without NULL termination.

The UE and HSGW can pre-compute the PairwiseMasterKeyID associated with each PMK (i.e., PMK1 to PMK4) as specified in [2] as follows:

\[ \text{PairwiseMasterKeyID} = 128 \text{ most significant bits of ehmacsha256(key=PairwiseMasterKey, key_length=length of PairwiseMasterKey in units of octets, message = “PairwiseMasterKeyID”, message_length = length of message in units of bits, message_offset=0, MAC_length=16)} \]

In addition, the UE and HSGW can also pre-compute the PMKs and PairwiseMasterKeyIDs associated with the other Sub-MSKs. This pre-computation of PMKs and
PairwiseMasterKeyIDs enables the UE to identify the PMK it needs to use upon receiving request from the access network to derive session keys for access security.

The PMKs can be delivered to eAN from HSGW using the mechanism specified in [15] to be used for Multi-Key Key Exchange Protocol (MKEP) procedure to derive session keys as described in Section 7.2.

For HRPD, since inter-PDSN handoff is not supported in [22], the MSK obtained as a result of successful EAP-AKA authentication is directly used to derive the PMK as follows:

\[
PMK = \text{HMAC-SHA-256}(\text{MSK}, \text{“pmk@hrpd.3gpp2”})
\]

where the key label “pmk@hrpd.3gpp2” is set to ASCII strings without NULL termination.

This PMK is used in section 7.2 to derive the access network key(s).

### 7.2 Access Network Key Generation

As a result of successful Multi-Key Key Exchange Protocol (MKEP) message exchange, both the UE and the (e)AN generate Session Key(s) (SKey(S)) as specified in [2] and is summarized here.

A pictorial representation of Session Key and over-the-air key generation is provided in Figure 4.

![Diagram](image)

**Figure 4** SKey(s) and over-the-air key generation

The (e)AN and the UE use PMK, ANNonce and ATNonce as an input to generate SKey(s) and MICKey. ANNonce and ATNonce are corresponding fields of Multi-Key Key Exchange
Protocol (MKEP) messages, KeyRequest and KeyReponse, respectively. Each SKey is then truncated into authorization key and encryption key.

The UE and the (e)AN derive SKey[i] as follows, where i is SessionKeyIndex field of the corresponding MKEP KeyRequest message:

- Set k and m to an 8-bit number with value zero.
- while k<(NumSessionKeys+1), where NumSessionKeys is field of the corresponding KeyRequest message
  - Set SKeyTemp[i+k] to $\text{N}_{\text{MKEPSessionKeyLen}}$ least significant bits of {
    - $\text{ehmacsha256}$(key=PairwiseMasterKey, key_length=length of PairwiseMasterKey in units of octets, message=ATNonce|ANNonce|m, message_length= length of message in units of bits, message_offset=0, MAC_length=16),
  - where the $\text{ehmacsha256}$ function is specified in [3],
  - ANNonce and ANNonce are corresponding fields of KeyRequest and KeyReponse messages respectively, and m is represented as an 8-bit field.
- Set m to m+1.
- Set k to k+1.

The UE and the (e)AN derive the MICKey[i] as follows, where i is the SessionKeyIndex field of the corresponding KeyRequest message:

- Set MICKey[i] to the 128 most significant bits of {
  - $\text{ehmacsha256}$(key=PairwiseMasterKey, key_length=length of PairwiseMasterKey in units of octets, message=ATNonce|ANNonce, message_length= length of message in units of bits, message_offset=0, MAC_length=16),
  - where the $\text{ehmacsha256}$ function is specified in [3].

The keys used for authentication and encryption are generated from the session key as follows. The keys derived from SKey[i] are referred to by the subscript i.

The (e)AN and the UE set FACAuthKey[i], FPCAuthKey[i], RACAuthKey[i], and RPCAuthKey[i] to SKey[i][127:0], where i is the session key index.

The (e)AN and the UE set FACEncKey[i], FPCEncKey[i], RACEncKey[i], and RPCEncKey[i] to SKey[i][255:128], where i is the session key index.

The UE and the (e)AN compute and store a MICKey, Authentication Key, and Encryption Key. The keys derived from SKey[i] are referred to by the subscript i. The (e)AN and the UE use the Authentication Key and Encryption Key derived from the SKey with index i, where i is the value of the InUseSessionKeyIndex attribute defined in [2].

### 7.3 Access Network Key Generation for AALS

Air-Interface Application Layer Security (AALS) function at the (e)HRPD Air Interface Application layer coexists with security layer functionality defined in [16]. The AALS is defined to be independent of the Authentication Protocol and the Encryption Protocol defined by the security layer in [16].
Session security keys for the AALS, such as integrity (AuthKey) and encryption (EncKey) keys, shall be derived from the keys provided by the Key Exchange Protocol [2, 16] or MKE as described in section 7.2 above.

The session derivation mechanism is specified in [24].

8 Key Distribution

This section describes key distribution mechanisms in (e)HRPD.

8.1 eHRPD Master Session Key and Inter-HSGW Handoff

The HSGW sets its MSK to either the value of the MSK received from the AAA or to the value of the MSK received from another HSGW in the MSK Info field during the inter-HSGW handoff.

The HSGW uses the 128 most significant bits of the MSK (Sub-MSK) as the Master Session Key for the derivation of PMKs. The HSGW declares the remaining portion of the received MSK as the unused MSK information. The HSGW sets the value of the MSK Lifetime to the remaining lifetime of the authorized EAP session.

During Inter-HSGW handoff, the Source-HSGW sends the unused portion of the MSK to the Target-HSGW in the MSK Info field, only if the unused portion of the MSK information is \( \geq 128 \) bits, the Target-HSGW is trusted, and the link between the HSGWs is secure (e.g. IPsec is used). The Target-HSGW sets its MSK to the value of the received MSK context and acts as described above.

If the lifetime of the received MSK is close to expiry, or, during the inter-HSGW handoff, if the length of the received MSK Info is equal to 128 bits, or if the MSK is not received, the Target-HSGW initiates the authentication as soon as possible to continue with the session. When the new MSK AVP is received from the AAA, the Target-HSGW deprecates the current MSK value and replaces it with the value received in the MSK AVP. The Target-HSGW derives the new PMK from the new MSK as described in section 7.1.

8.2 HSGW/PDSN – (e)AN Key Distribution

If the HSGW/PDSN receives an indication in A11/A11’ -Registration Request message from the (e)AN that the PMK is needed for this session, the HSGW/PDSN returns the PMK to the (e)AN.

In the case of eHRPD, if the HSGW determines that it has no unused PMKs, the HSGW sets Sub-MSK as the 128-bit portion (Sub-MSK) occupying the highest order bit positions of the unused MSK information. The HSGW uses the Sub-MSK for the computation of PMKs using the procedures described in section 7.1.

In the case of HRPD, the MSK is used as is to derive the PMK as described in section 7.1.

Once the HSGW/PDSN generates the PMK or determines that the new PMK needs to be sent to the (e)AN/(e)PCF, the HSGW/PDSN sends a PMK and its lifetime in seconds to the (e)AN.
using A11/A11’-Registration Response or A11/A11’-Session Update message [15]. The lifetime of the PMK is set to not more than the remaining value of the MSK lifetime.

PMK(s) are delivered to (e)AN using mechanisms specified in [15] for eHRPD and [20], [21] for HRPD.

8.3 Multi-Key Key Exchange Protocol and Intra-HSGW/PDSN inter-(e)AN Handoff

If the MKEP is negotiated for a session, an (e)AN includes PMK Information IE in a A11/A11’-Registration Request message sent to HSGW/PDSN, indicating to the HSGW/PDSN that the PMK is needed for this session.

Once the (e)AN receives PMK(s) from the HSGW/PDSN, the (e)AN triggers MKEP. When the MKEP is triggered, the (e)AN indicates to the UE which PMK to use by including the PMK_ID in the KeyRequest Message. The UE selects appropriate PMK that corresponds to the indicated PMK_ID, either by computing the PMK and PMK_ID values in a real time, or from a buffer of precomputed values. The KeyRequest message also indicates to the UE in the NumSessionKeys parameter how many Session Key sets needs to be computed in one execution of the MKEP.

Upon successful MKEP message exchange, the (e)AN indicates to the UE which Authentication key and Encryption key to use by including the InUseSessionKeyIndex attribute in an AttributeUpdateRequest message sent on the Control Channel. The (e)AN and the UE use the Authentication Key and Encryption Key derived from the SKey with index i, where i is the value of the InUseSessionKeyIndex attribute received in AttributeUpdateRequest message.

If the (e)AN wants to use Authentication Key and Encryption Key derived from another SKey (different from one in use) to preserve the cryptographic separation, the (e)AN sends the AttributeUpdateRequest with another InUseSessionKeyIndex. Upon completion of this exchange, the (e)AN and the UE use the Authentication Key and Encryption Key derived from this new SKey.

If the (e)AN determines that new set of SKeys needs to be obtained, the (e)AN can trigger a new MKEP message exchange.

During, inter-(e)AN handoff (A13 or A16 session transfer) the Source-(e)AN sends unused SKeys included in SKey Parameter of Session State Information Record (SSIR) and existing PMKs in the PMK Parameter of SSIR to the Target-(e)AN.

8.3.1 Reconfiguration Procedures

If multiple session keys are derived through the Multi-Key Key Exchange Protocol specified in [2], the access terminal and the access network use the Generic Attribute Update Protocol (GAUP) to update values of the session key index to change the session keys. Regardless of when the key change reconfiguration takes place, the new session key takes effect upon transition from idle to active mode. In other words, the GAUP updates the session key index for the next active mode session, and the session key remains unchanged for the duration of the current active mode session.
9 Session Key Usage for AALS

AALS Function at the Air Interface Application layer consists of the following functionalities [24]:

- Derivation and management of the cryptographic synchronization value (crypto-sync) for crypto-processing of transmitted and received Air Interface Application layer data.
- Air Interface Application Encryption and Integrity Protection.

The AALS function operates using the session security keys generated in 7.3.

The AALS function utilizes the crypto-sync for all crypto-processing to provide the replay protection for processed data. Derivation and maintenance of crypto-sync assures that each and every byte of processed data is crypto-processed using unique and non-repeating cryptographic constants applicable exclusively for this byte. The crypto-sync is independently derived at the communicating peers, and is not transmitted over the air interface.

9.1 Derivation and Management of Crypto-sync

The procedure and parameter used to derive the crypto-sync for the signaling packet protection is specified in the section 3.1.2 of [24]. The procedures and parameters used to derive the crypto-sync for the AALS Enhanced Multi-Flow Packet Application (EMFPA) and the AALS Multi-Link Multi-Flow Packet Application Flow (MLMFPA) are specified in the section 4.5.4.1.2 and 5.5.4.1.2 of reference [24] respectively.

9.2 AALS EMFPA and AALS MLMFPA

The AALS Enhanced Multi-Flow Packet Application (EMFPA) Data Encryption uses the AES (a.k.a. Rijndael) procedures defined in [15] in order to encrypt and decrypt the EMFPA packets. The AALS Multi-Link Multi-Flow Packet Application (MLMFPA) Data Encryption also uses the AES (a.k.a. Rijndael) procedures defined in [15] in order to encrypt and decrypt the MLMFPA packets.

This encryption can be applied selectively to individual link flows. That is, depending on session configuration, some link flows may be encrypted, while others are not. Encryption mode is individually configured for each data flow during the configuration phase of the session. The policy on which link flows are encrypted is determined by the (e)AN (e.g., either based on local policy at the (e)AN or by other means). Each RLP block is encrypted by the transmitter using the AES algorithm in a counter mode. Because all required cryptographic configuration parameters are either provided by other protocols (session encryption keys) or internally derived (crypto-sync), no additional headers are required for crypto-processing the data.

AES encryption is applied to data before it is presented for fragmentation and transmission. Similarly, received data is presented for AES decryption after it is re-assembled by lower layers.
9.3 Air Interface Application Signaling Encryption/Decryption functions

The Air Interface Application Signaling Encryption/Decryption Functions use the AES (a.k.a. Rijndael) procedures defined in [15] in order to encrypt and decrypt the Air Interface Application Layer signaling packets.

The SLP-D message is security protected based on negotiated session configuration. The signaling packet is encrypted by the transmitter using the AES algorithm in a counter mode [15]. Because all required cryptographic configuration parameters are either provided by other protocols (session encryption keys) or internally derived by the AALS function (cryptosync), no additional headers are required for crypto-processing the signaling packet. For signaling integrity protection, a 32 bits authentication tag is attached to the SLP-D packet as described in the next subsection.

9.4 Air Interface Application Signaling Integrity Protection

Air Interface Application Signaling Integrity Function employs the explicit Message Authentication Code to provide a method for integrity protection of signaling messages by applying the AES CMAC function (see [1], [15], and [16]).

The transmitting function appends the Authentication Tag to the signaling message in SLP-D and forwards it to the next procedure for processing.

When the receiving function receives packet for processing, it calculates the message Authentication Tag and compares the computed value with the one received. If they match, the Authentication Tag will be removed and the remaining packet is delivered to SNP for processing.