

3GPP2 S.S0145-0

Version 1.0

Version Date: 26 May 2011



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

Advanced Security Framework for HRPD and eHRPD Systems

© 3GPP2 2011

COPYRIGHT NOTICE

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

EDITOR

1 Zhibi Wang
2 Alcatel Lucent
3 Tel: (+1) 630-713-8381
4 Email: zhibi.wang@alcatel-lucent.com
5

6 **REVISION HISTORY**

7

REVISION HISTORY		
1.0	<i>Initial Publication</i>	<i>26 May 2011</i>

8

Table of Contents

1			
2		Advanced Security Framework for HRPD and eHRPD Systems	i
3	1	Introduction.....	2
4		1.1 Scope	2
5	2	References.....	2
6		2.1 Normative References	2
7		2.2 Informative References.....	3
8	3	Definitions, Abbreviations and Acronyms.....	3
9		3.1 Definitions	3
10		3.1.1 Abbreviations and Acronyms.....	3
11		3.1.2 Terminology.....	4
12	4	Architecture	4
13	5	Security Requirements	6
14	6	Access Authentication and Authorization.....	7
15		6.1 EAP Protocol Negotiation	7
16		6.2 UE Behavior	7
17		6.2.1 UE Identity Management for eHRPD	7
18		6.2.2 UE Identity Management for HRPD	7
19		6.2.3 UE Network Access Authentication for eHRPD.....	7
20		6.2.4 UE Network Access Authentication for HRPD	8
21		6.3 HSGW Behavior.....	8
22		6.4 PDSN Behavior	8
23		6.5 AAA Server Behavior	8
24		6.5.1 3GPP AAA Server Behavior.....	8
25		6.5.2 3GPP2 AAA Server Behavior.....	8
26		6.6 HSS Behavior.....	8
27	7	Key Generation.....	8
28		7.1 Pairwise Master Key (PMK) Generation.....	9
29		7.2 Access Network Key Generation.....	10
30		7.3 Access Network Key Generation for AALS.....	11
31	8	Key Distribution	12
32		8.1 eHRPD Master Session Key and Inter-HSGW Handoff	12
33		8.2 HSGW/PDSN – (e)AN Key Distribution.....	12
34		8.3 Multi-Key Key Exchange Protocol and Intra-HSGW/PDSN inter-eAN Handoff.....	13
35		8.3.1 Reconfiguration Procedures	13

1	9	Session Key Usage for AALS.....	14
2	9.1	Derivation and Management of Crypto-sync.....	14
3	9.2	AALS EMFPA and AALS MLMFPA.....	14
4	9.3	Air Interface Application Signaling Encryption/Decryption functions	15
5	9.4	Air Interface Application Signaling Integrity Protection.....	15
6			
7			

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

- [1] **3GPP2:** X.S0057-0: “E-UTRAN – eHRPD Connectivity and Interworking: Core Network Aspects”.
- [2] **3GPP2:** C.S0067-A: “Key Exchange Protocols for cdma2000 High Rate Packet Data Air Interface”.
- [3] **3GPP2:** S.S0078-B: “Common Security Algorithms”.
- [4] **IETF:** RFC1661: “The Point-to-Point Protocol (PPP)”, July 1994.
- [5] **IETF:** RFC3588: “Diameter Base Protocol”, September 2003.
- [6] **IETF:** RFC3748: “Extensible Authentication Protocol (EAP)”, June 2004.
- [7] **IETF:** RFC4005: “Diameter Network Access Server Application”, August 2005.
- [8] **IETF:** RFC4072: “Diameter Extensible Authentication Protocol (EAP) Application”, August 2005.
- [9] **IETF:** RFC4187: “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”, January 2006.
- [10] **IETF:** RFC4282: “The Network Access Identifier”, December 2005.
- [11] **IETF:** RFC5448: “Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”, May 2009.
- [12] **3GPP:** TS 33.402: “Security aspects of non-3GPP accesses (Release 9)”.
- [13] **3GPP:** TS 23.003: “Numbering, addressing and identification (Release 9)”.
- [14] **3GPP:** TS 24.302: “Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3; (Release 9)”.

- 1 [15] **3GPP2:** A.S0022-0: “E-UTRAN – eHRPD Connectivity and Interworking:
2 Access Network Aspects (E-UTRAN – HRPD IOS)”.
- 3 [16] **3GPP2:** C.S0024-B: cdma2000 High Rate Packet Data Air Interface
4 Specification.
- 5 [17] **3GPP2:** C.S0039-0: Enhanced Subscriber Privacy for cdma2000 High Rate
6 Packet Data.
- 7 [18] **IETF:** RFC 4493: "The AES-CMAC Algorithm", June 2006.
- 8 [19] **NIST:** [CMAC-NIST-SP800-38B], Special Publication 800-38B,
9 "Recommendation for Block Cipher Modes of Operation: The CMAC Mode
10 for Authentication", May 2005.
- 11 [20] **3GPP2:** A.S0008-C: “Interoperability Specification (IOS) for High Rate
12 Packet Data (HRPD) Radio Access Network Interfaces With Session Control
13 in the Access Network”.
- 14 [21] **3GPP2:** A.S0009-C: “Interoperability Specification (IOS) for High Rate
15 Packet Data (HRPD) Radio Access Network Interfaces With Session Control
16 in the Access Network”.
- 17 [22] **3GPP2:** X.S0011-E: “cdma2000 Wireless IP Network Standard”.
- 18 [23] **IETF:** RFC2865: "Remote Authentication Dial In User Service (RADIUS)",
19 June 2000.
- 20 [24] **3GPP2:** C.S0102-0: “HRPD Air Interface Application Layer Security
21 (AALS): Air Interface Aspects”.

22 **2.2 Informative References**

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

25

26 **3 Definitions, Abbreviations and Acronyms**

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

29 **3.1 Definitions**

30

31 **3.1.1 Abbreviations and Acronyms**

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

33	3GPP	3rd Generation Partnership Project
34	3GPP2	3rd Generation Partnership Project 2
35	AAA	Authentication, Authorization, Accounting
36	AALS	Air interface Application Layer Security

1	AKA	Authentication and Key Agreement
2	AN-AAA	Access Network AAA
3	AT	Access Terminal
4	eAN	Evolved Access Network
5	EAP	Extensible Authentication Protocol
6	EPC	Evolved Packet Core
7	ePCF	Evolved Packet Control Function
8	EPS	Evolved Packet System
9	E-UTRAN	Evolved Universal Terrestrial Radio Access Network
10	HRPD	High Rate Packet Data
11	HSGW	HRPD Serving Gateway
12	HSS	Home Subscriber Service
13	IMSI	International Mobile Subscriber Identity
14	IP	Internet Protocol
15	IP-CAN	IP Connectivity Access Network
16	MSK	Master Session Key
17	NAI	Network Access Identifier
18	P-GW	Packet Data Network Gateway (specified by 3GPP)
19	PDN	Packet Data Network
20	PDSN	Packet Data Serving Node
21	RLP	Radio Link Protocol
22	SNP	Signaling Network Protocol
23	RAN	Radio Access Network
24	UE	User Equipment

25 3.1.2 Terminology

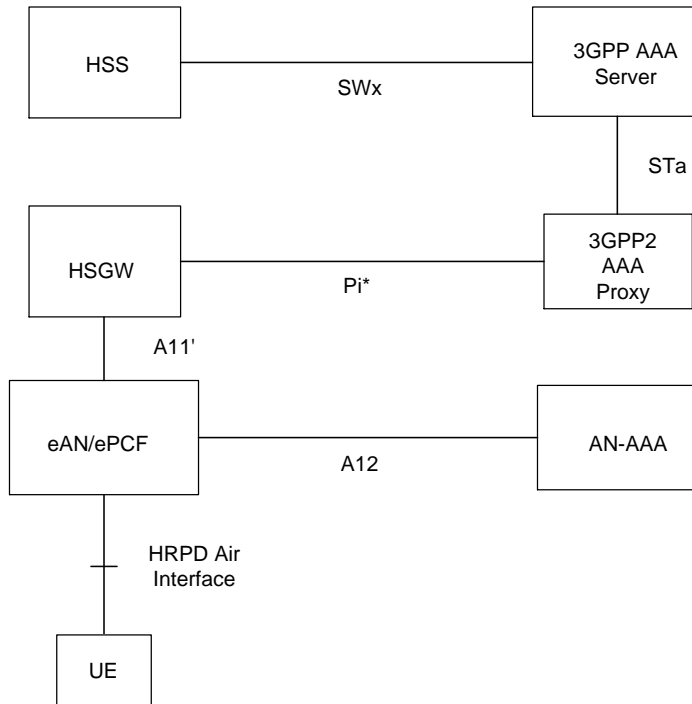
26 In this document, the term UE has the same meaning as AT in HRPD system.

27 4 Architecture

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

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

37



1
2

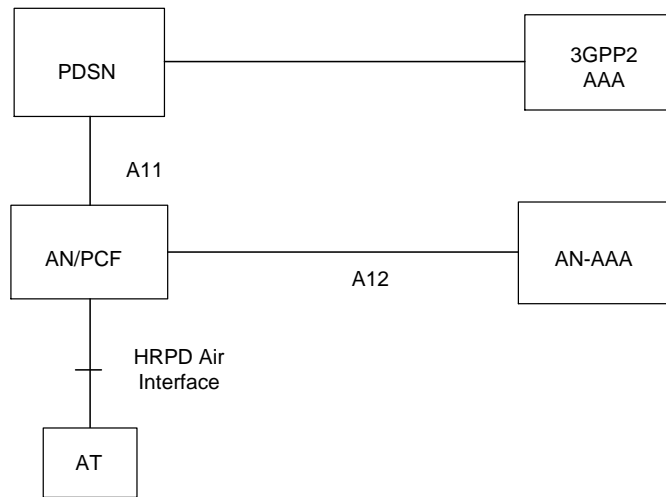
Figure 1 eHRPD Security Reference Model

3
4
5
6
7
8

Figure 2 below illustrates the HRPD security reference model. An HRPD 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].

9
10

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).



1
2 **Figure 2 HRPD Security Reference Model**

3 **5 Security Requirements**

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

- 6
- Mutual authentication between the UE and the network shall be supported.
 - 7
 - It shall be possible to perform data encryption on a per link flow basis.
 - 8
 - Confidentiality and integrity protection of the (e)HRPD access network signalling
9 messages shall be supported with the following exceptions:
 - 10 - Messages required to establish the security context between the UE and the network
 - 11 - Emergency calls for an unauthenticated UE.
 - 12 - Any messages that are explicitly identified as not being protected by the
13 specifications.

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

- 16
- Confidentiality protection of user data shall be supported.
 - 17
 - 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].

1 After successful access authentication, both the UE and HSGW derive identical values of
2 MSK.

3 **6.2.4 UE Network Access Authentication for HRPD**

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

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

7 **6.3 HSGW Behavior**

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

9 The HSGW shall play the role of authenticator.

10 **6.4 PDSN Behavior**

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

12 The HSGW shall play the role of authenticator.

13 **6.5 AAA Server Behavior**

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

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

16 **6.5.1 3GPP AAA Server Behavior**

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

18 **6.5.2 3GPP2 AAA Server Behavior**

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

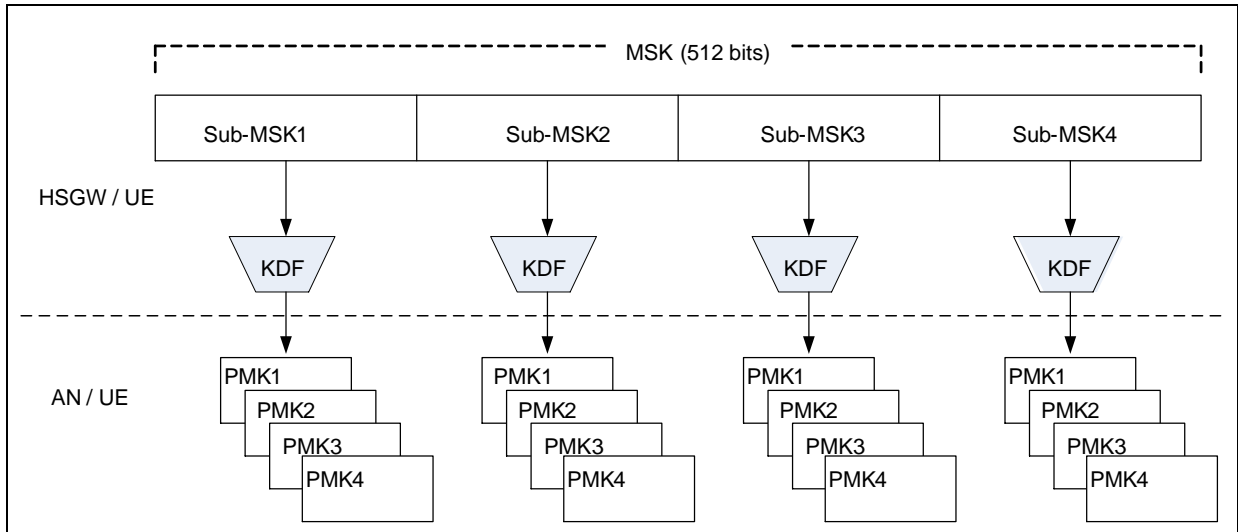
20 **6.6 HSS Behavior**

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

23 **7 Key Generation**

24 This section provides methods and procedures for generating the Pairwise Master Key (PMK)
25 from MSK. The PMK in turn is used by the Key Exchange protocol to generate keys for over-
26 the-air security protection.

1 A pictorial representation of PMK generation for eHRPD is provided in Figure 3 , while
 2 detailed description is provided in following sub-sections.



3
 4 **Figure 3 eHRPD Key Generation**

5

6 **7.1 Pairwise Master Key (PMK) Generation**

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

11
$$\text{PMK1} = \text{HMAC-SHA-256}(\text{Sub-MSK}, \text{"pmk@hrpd.3gpp2"}, 0x01), [0:127]$$

12
$$\text{PMK2} = \text{HMAC-SHA-256}(\text{Sub-MSK}, \text{"pmk@hrpd.3gpp2"}, 0x01) [128:255],$$

13
$$\text{PMK3} = \text{HMAC-SHA-256}(\text{Sub-MSK}, \text{"pmk@hrpd.3gpp2"}, 0x02) [0:127],$$

14
$$\text{PMK4} = \text{HMAC-SHA-256}(\text{Sub-MSK}, \text{"pmk@hrpd.3gpp2"}, 0x02) [128:255],$$

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

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

18
$$\text{PairwiseMasterKeyID} = 128 \text{ most significant bits of } \text{ehmacsha256}(\text{key}=\text{PairwiseMasterKey},$$

 19
$$\text{key_length}=\text{length of PairwiseMasterKey in units of octets, message} =$$

 20
$$\text{"PairwiseMasterKeyID"}, \text{message_length} = \text{length of message in units of bits,}$$

 21
$$\text{message_offset}=0, \text{MAC_length}=16)$$

22 In addition, the UE and HSGW can also pre-compute the PMKs and PairwiseMasterKeyIDs
 23 associated with the other Sub-MSKs. This pre-computation of PMKs and

1 PairwiseMasterKeyIDs enables the UE to identify the PMK it needs to use upon receiving
2 request from the access network to derive session keys for access security.

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

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

$$8 \quad \text{PMK} = \text{HMAC-SHA-256}(\text{MSK}, \text{"pmk@hrpd.3gpp2"})$$

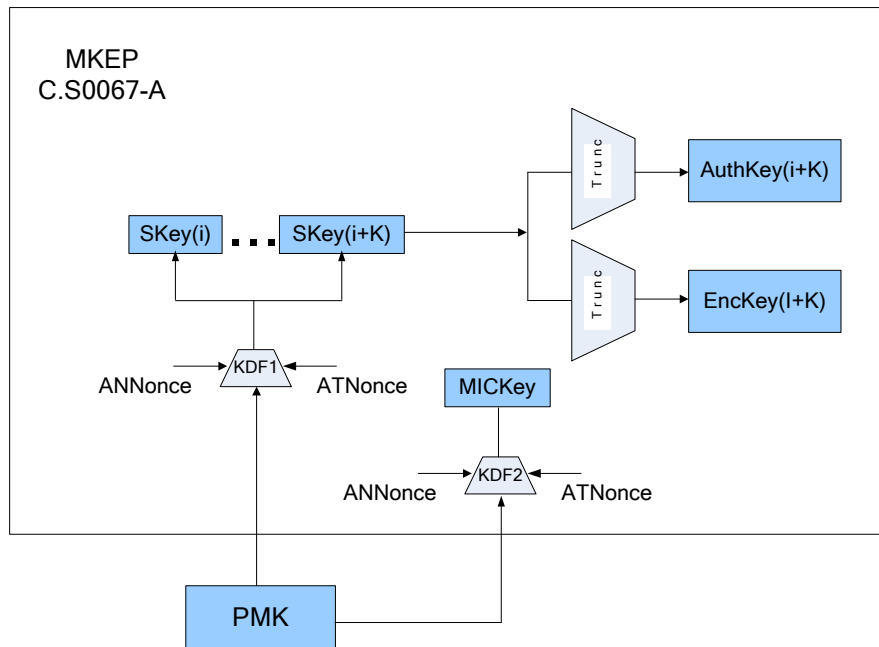
9 where the key label "pmk@hrpd.3gpp2" is set to ASCII strings without NULL termination.

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

11 7.2 Access Network Key Generation

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

15 A pictorial representation of Session Key and over-the-air key generation is provided in Figure
16 4.



17

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

19 The (e)AN and the UE use PMK, ANNonce and ATNonce as an input to generate SKey(s) and
20 MICKey. ANNonce and ATNonce are corresponding fields of Multi-Key Key Exchange

1 Protocol (MKEP) messages, KeyRequest and KeyReponse, respectively. Each SKey is then
2 truncated into authorization key and encryption key.

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

- 5 ▪ Set k and m to an 8-bit number with value zero.
- 6 ▪ while $k < (\text{NumSessionKeys} + 1)$, where NumSessionKeys is field of the corresponding
7 KeyRequest message
 - 8 Set SKeyTemp[i+k] to $N_{\text{MKEPSessionKeyLen}}$ least significant bits of {
 - 9 SKeyTemp[i+k] | 128 most significant bits of
 - 10 ehmacsha256(key=PairwiseMasterKey, key_length=length of
 - 11 PairwiseMasterKey in units of octets, message=ATNonce|ANNonce|m,
 - 12 message_length= length of message in units of bits, message_offset=0,
 - 13 MAC_length=16) }, where the ehmacsha256 function is specified in [3],
 - 14 ANNonce and ANNonce are corresponding fields of KeyRequest and
 - 15 KeyReponse messages respectively, and m is represented as an 8-bit field.
- 16 ▪ Set m to m+1.
- 17 ▪ Set k to k+1.

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

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

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

27 The (e)AN and the UE set FACAAuthKey[i], FPCAAuthKey[i], RACAAuthKey[i], and
28 RPCAAuthKey[i] to SKey[i][127:0], where i is the session key index.

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

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

35 7.3 Access Network Key Generation for AALS

36 Air-Interface Application Layer Security (AALS) function at the (e)HRPD Air Interface
37 Application layer coexists with security layer functionality defined in [16]. The AALS is
38 defined to be independent of the Authentication Protocol and the Encryption Protocol defined
39 by the security layer in [16].

1 Session security keys for the AALS, such as integrity (AuthKey) and encryption (EncKey)
 2 keys, shall be derived from the keys provided by the Key Exchange Protocol [2, 16] or MKE
 3 as described in section 7.2 above.

4 The session derivation mechanism is specified in [24].

5 **8 Key Distribution**

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

7 **8.1 eHRPD Master Session Key and Inter-HSGW Handoff**

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

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

15 During Inter-HSGW handoff, the Source-HSGW sends the unused portion of the MSK to the
 16 Target-HSGW in the MSK Info field, only if the unused portion of the MSK information is \geq
 17 128 bits, the Target-HSGW is trusted, and the link between the HSGWs is secure (e.g. IPsec is
 18 used). The Target-HSGW sets its MSK to the value of the received MSK context and acts as
 19 described above.

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

26 **8.2 HSGW/PDSN – (e)AN Key Distribution**

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

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

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

35 Once the HSGW/PDSN generates the PMK or determines that the new PMK needs to be sent
 36 to the (e)AN/(e)PCF, the HSGW/PDSN sends a PMK and its lifetime in seconds to the (e)AN

1 using A11/A11'-Registration Response or A11/A11'-Session Update message [15]. The
2 lifetime of the PMK is set to not more than the remaining value of the MSK lifetime.

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

5 **8.3 Multi-Key Key Exchange Protocol and Intra-HSGW/PDSN inter-** 6 **eAN Handoff**

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

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

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

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

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

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

33 **8.3.1 Reconfiguration Procedures**

34 If multiple session keys are derived through the Multi-Key Key Exchange Protocol specified in
35 [2], the access terminal and the access network use the Generic Attribute Update Protocol
36 (GAUP) to update values of the session key index to change the session keys. Regardless of
37 when the key change reconfiguration takes place, the new session key takes effect upon
38 transition from idle to active mode. In other words, the GAUP updates the session key index
39 for the next active mode session, and the session key remains unchanged for the duration of the
40 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 (cryptosync), 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.