

3GPP2 C.S0084-005-0

Version 3.0

Date: August 2008



**3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"**

Security Functions for Ultra Mobile Broadband (UMB) Air Interface Specification

COPYRIGHT

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 <mailto:secretariat@3gpp2.org>. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See <http://www.3gpp2.org/> for more information.

No text.

CONTENTS

1	FOREWORD	ix
2	NOTES	xi
3	REFERENCES	xi
4	1 Introduction	1-1
5	2 AES CIPHERING PROTOCOL	2-1
6	2.1 Primitives and Public Data	2-1
7	2.1.1 Commands	2-1
8	2.1.2 Return Indications	2-1
9	2.1.3 Procedure Calls	2-1
10	2.1.4 Local Common Data	2-2
11	2.1.5 Public Data	2-2
12	2.2 Protocol Data Unit	2-2
13	2.3 Procedures and Messages for the InConfiguration Instance of the Protocol	2-2
14	2.3.1 Protocol Initialization for the InConfiguration Protocol Instance	2-2
15	2.3.2 Procedures	2-3
16	2.3.3 Message Formats	2-3
17	2.4 Procedures and Messages for the InUse Instance of the Protocol	2-3
18	2.4.1 Procedures	2-3
19	2.4.1.1 Protocol Initialization for the InUse Protocol Instance	2-3
20	2.4.1.2 Hard Commit Procedures	2-3
21	2.4.1.3 Soft Commit Procedures	2-3
22	2.4.1.4 Constructing the Ciphering Key	2-3
23	2.4.1.5 Constructing the Cryptosync	2-4
24	2.4.1.6 Encrypt Procedures	2-5
25	2.4.1.7 Decryption Procedures	2-7
26	2.4.2 Message Formats	2-9
27	2.4.3 Interface to Other Protocols	2-9
28	2.4.3.1 Commands	2-9
29	2.4.3.2 Indications	2-9
30	2.5 Configuration Attributes	2-9
31	2.5.1 Simple Attributes	2-9

CONTENTS

1	2.5.2 Complex Attributes	2-10
2	2.5.2.1 FTCReducedStrengthCipherringKey Attribute	2-10
3	2.5.2.2 RTCReducedStrengthCipherringKey Attribute	2-10
4	2.6 Non-Attribute Data	2-11
5	2.7 Protocol Numeric Constants	2-11
6	2.8 Session State Information	2-11
7	3 Basic Message Integrity Protocol	3-1
8	3.1 3.1 Overview	3-1
9	3.2 Primitives and Public Data	3-1
10	3.2.1 Commands	3-1
11	3.2.2 Return Indications	3-1
12	3.2.3 Procedure Calls	3-1
13	3.2.4 Local Common Data	3-2
14	3.2.5 Public Data	3-2
15	3.3 Protocol Data Unit.....	3-2
16	3.4 Procedures and Messages for the InConfiguration Instance of the Protocol.....	3-3
17	3.4.1 Protocol Initialization for the InConfiguration Protocol Instance.....	3-3
18	3.4.2 Procedures	3-3
19	3.4.3 Message Formats	3-3
20	3.5 Procedures and Messages for the InUse Instance of the Protocol	3-3
21	3.5.1 Procedures	3-3
22	3.5.1.1 Protocol Initialization for the InUse Protocol Instance	3-3
23	3.5.1.2 Hard Commit Procedures	3-3
24	3.5.1.3 Soft Commit Procedures	3-3
25	3.5.1.4 Constructing the Message Integrity Key	3-3
26	3.5.1.5 Constructing the Cryptosync	3-4
27	3.5.1.6 Authentication Header.....	3-5
28	3.5.1.7 AUTHENTICATE_ADD_TAG procedures	3-6
29	3.5.1.8 AUTHENTICATE_CHECK_TAG procedures	3-7
30	3.5.1.9 CREATE_ID_TAG procedures.....	3-9
31	3.5.2 Message Formats	3-10
32	3.6 Interface to Other Protocols.....	3-10

CONTENTS

1	3.6.1 Commands	3-10
2	3.6.2 Indications	3-10
3	3.7 Configuration Attributes	3-10
4	3.8 Non-Attribute Data	3-10
5	3.9 Protocol Numeric Constants	3-10
6	3.10 Session State Information	3-10
7	4 Basic Key Exchange Protocol	4-1
8	4.1 Overview	4-1
9	4.2 Primitives and Public Data	4-1
10	4.2.1 Commands	4-1
11	4.2.2 Return Indications	4-1
12	4.2.3 Local Common Data	4-1
13	4.2.4 Public Data	4-1
14	4.2.5 Interface to Other Protocols	4-2
15	4.2.5.1 Commands	4-2
16	4.2.5.2 Indications	4-2
17	4.3 Protocol Data Unit	4-2
18	4.4 Procedures and Messages for the InConfiguration Instance of the Protocol	4-2
19	4.4.1 Protocol Initialization for the InConfiguration Protocol Instance	4-2
20	4.4.2 Procedures	4-2
21	4.4.3 Message Formats	4-3
22	4.5 Procedures and Messages for the InUse Instance of the Protocol	4-3
23	4.5.1 Procedures	4-3
24	4.5.1.1 Protocol Initialization for the InUse Protocol Instance	4-3
25	4.5.1.2 Hard Commit Procedures	4-3
26	4.5.1.3 Soft Commit Procedures	4-3
27	4.5.1.4 Access Terminal Requirements	4-3
28	4.5.1.4.1 Initiating the key exchange	4-4
29	4.5.1.4.2 Processing a KeyResponse message	4-4
30	4.5.1.4.3 Processing a KeyReject message	4-5
31	4.5.1.4.4 Processing an ATSupportedSecuritySubtypesRequest message	4-5
32	4.5.1.5 Access Network Requirements	4-6

CONTENTS

1	4.5.1.5.1 Initiating the key exchange	4-6
2	4.5.1.5.2 Processing a KeyRequest message	4-6
3	4.5.1.5.3 Processing a KeyComplete message	4-6
4	4.5.1.6 MICKey Derivation.....	4-6
5	4.5.1.7 Message Integrity Key and Ciphering Key Generation	4-6
6	4.5.1.7.1 Temporary Security Key Derivation.....	4-7
7	4.5.1.7.2 Message Integrity Key and Ciphering Keys Generation from TSKey	4-7
8	4.5.1.8 EHMAC-SHA256(key, message, MAC_length).....	4-7
9	4.5.2 Message Formats	4-8
10	4.5.2.1 KeyRequest.....	4-8
11	4.5.2.2 KeyResponse	4-8
12	4.5.2.3 KeyComplete	4-11
13	4.5.2.4 KeyReject.....	4-12
14	4.5.2.5 InitiateKeyRequest.....	4-13
15	4.5.2.6 ATSupportedSecuritySubtypesRequest.....	4-13
16	4.5.2.7 ATSupportedSecuritySubtypesResponse.....	4-13
17	4.5.3 Interface to Other Protocols	4-15
18	4.5.3.1 Commands	4-15
19	4.5.3.2 Indications	4-15
20	4.6 Configuration Attributes	4-15
21	4.6.1 Simple Attributes	4-15
22	4.6.2 Complex Attributes	4-15
23	4.6.2.1 ATSupportedSecuritySubtypes Attribute	4-15
24	4.7 Non-Attribute Data	4-16
25	4.8 Protocol Numeric Constants.....	4-16
26	4.9 Session State Information	4-16
27	4.9.1 DerivedMSK Parameter	4-16
28		

FIGURES

1 Figure 3-1. AUTHENTICATE_ADD_TAG procedure call payloads3-6
2 Figure 3-2. AUTHENTICATE_CHECK_TAG procedure call payloads.....3-8
3

FIGURES

- 1 No text.

TABLES

1	Table 2-1. Subfield of the Cryptosync	2-5
2	Table 2-2. Configurable Values.....	2-9
3	Table 3-1. Subfield of the Cryptosync	3-4
4	Table 3-2. Authentication Headers	3-5
5	Table 3-3. AuthKeyIndex encoding	3-5
6	Table 3-4. Protocol Numeric Constants	3-10
7	Table 4-1. KeyRequest Message.....	4-8
8	Table 4-2. Definition of Result field	4-12
9	Table 4-3. Protocol Numeric Constants	4-16
10	Table 4-4. The Format of the Parameter Record for the DerivedMSK Parameter.....	4-17
11		

TABLES

- 1 No text.

FOREWORD

1 **(This foreword is not part of this Standard)**

2 This standard was prepared by Technical Specification Group C of the Third Generation
3 Partnership Project 2 (3GPP2). This Standard is the Security Functions part of the Ultra
4 Mobile Broadband™ (UMB™)¹ air interface. Other parts of this Standard are:

- 5 • Overview for Ultra Mobile Broadband (UMB) Air Interface Specification
- 6 • Physical Layer for Ultra Mobile Broadband (UMB) Air Interface Specification
- 7 • MAC Layer for Ultra Mobile Broadband (UMB) Air Interface Specification
- 8 • Radio Link Layer for Ultra Mobile Broadband (UMB) Air Interface Specification
- 9 • Application Layer for Ultra Mobile Broadband (UMB) Air Interface Specification
- 10 • Connection Control Plane for Ultra Mobile Broadband (UMB) Air Interface Specification
- 11 • Session Control Plane for Ultra Mobile Broadband (UMB) Air Interface Specification
- 12 • Route Control Plane for Ultra Mobile Broadband (UMB) Air Interface Specification
- 13 • Broadcast-Multicast Upper Layers for Ultra Mobile Broadband (UMB) Air Interface
14 Specification

15 Other Standards may be required to implement this system and are listed in the References
16 section of each part.

17 This standard provides a specification for land mobile wireless systems based upon cellular
18 principles. This Standard is one part of the IMT-2000 CDMA Multi-Carrier, IMT-2000
19 CDMA MC, also known as cdma2000®².

¹ Ultra Mobile Broadband™ and (UMB™) are trade and service marks owned by the CDMA Development Group (CDG).

² cdma2000® is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.

FOREWORD

- 1 No text.

REFERENCES

1 The following documents contain provisions, which, through reference in this text,
2 constitute provisions of this document. References are either specific (identified by date of
3 publication, edition number, version number, etc.) or non-specific. For a specific reference,
4 subsequent revisions do not apply. For a non-specific reference, the latest version applies.
5 In the case of a reference to a 3GPP2 document, a non-specific reference implicitly refers to
6 the latest version of that document in the same Release as the present document.

- 7
- 8 [1] C.S0084-000-0, Overview for Ultra Mobile Broadband (UMB) Air Interface
9 Specification.
- 10 [2] C.S0084-001-0, Physical Layer for Ultra Mobile Broadband (UMB) Air Interface
11 Specification.
- 12 [3] C.S0084-002-0, MAC Layer for Ultra Mobile Broadband (UMB) Air Interface
13 Specification.
- 14 [4] C.S0084-003-0, Radio Link Layer for Ultra Mobile Broadband (UMB) Air Interface
15 Specification.
- 16 [5] C.S0084-004-0, Application Layer for Ultra Mobile Broadband (UMB) Air Interface
17 Specification.
- 18 [6] Reserved.
- 19 [7] C.S0084-006-0, Connection Control Plane for Ultra Mobile Broadband (UMB) Air
20 Interface Specification.
- 21 [8] C.S0084-007-0, Session Control Plane for Ultra Mobile Broadband (UMB) Air
22 Interface Specification.
- 23 [9] C.S0084-008-0, Route Control Plane for Ultra Mobile Broadband (UMB) Air
24 Interface Specification.
- 25 [10] C.S0084-009-0, Broadcast-Multicast Upper Layer for Ultra Mobile Broadband
26 (UMB) Air Interface Specification.
- 27 [11] C.R1001, Administration of Parameter Value Assignments for cdma2000 Spread
28 Spectrum Standards. (Informative)
- 29 [12] S.S0055, Enhanced Cryptographic Algorithms.
- 30 [13] S.S0078, Common Security Algorithms.
- 31 [14] NIST, Special Publication 800-38B Draft, "Recommendation for Block Cipher
32 Modes of Operation: The CMAC Method for Authentication", March 9, 2005."
- 33 [15] Song, JH., Poovendran, R., Lee, J., and T. Iwata, "The AES-CMAC Algorithm", RFC
34 4493, June 2006."
- 35 [16] [CMAC-NIST-SP800-38B] NIST, Special Publication 800-38B, "Recommendation for
36 Block Cipher Modes of Operation: The CMAC Mode for Authentication", May 2005.
- 37 [17] IETF RFC 4493, The AES-CMAC Algorithm. (Informative)

REFERENCES

- 1 | [\[18\] IETF RFC 1305, Network Time Protocol \(Version 3\) Specification, Implementation](#)
2 | [and Analysis.](#)

- 1 **1 INTRODUCTION**
- 2 Security Function consists of following protocols:
- 3 • AES Ciphering Protocol
- 4 • Basic Message Integrity Protocol
- 5 • Basic Key Exchange Protocol

- 1 No text.

1 **2 AES CIPHERING PROTOCOL**

2 The AES Ciphering Protocol uses the AES (a.k.a. Rijndael) procedures defined in [12] in
3 order to encrypt and decrypt the Radio Link Protocol packets.

4 **2.1 Primitives and Public Data**

5 2.1.1 Commands

6 This protocol does not define any commands.

7 2.1.2 Return Indications

8 This protocol does not return any indications.

9 2.1.3 Procedure Calls

10 • ENCRYPT

- 11 – Inputs: *Direction*, *DataUnit*, *StreamID*, *RouteCounter*, *SARResetCounter*,
12 *SARSequenceNumber*, *SARSequenceRolloverCounter*, *PayloadSize*, *Payload*
- 13 – Outputs: *Payload* (Encrypted), *CipheringKeyIndex*
- 14 – Possible values of each input and output are as follows:
 - 15 + *Direction* – ‘0’ (ForwardLink) or ‘1’ (ReverseLink)
 - 16 + *DataUnit* – ‘00’ (Octets), ‘01’ (RLP Packet Payload)
 - 17 + *StreamID* – 16-bit hexadecimal number
 - 18 + *RouteCounter* – 15-bit hexadecimal number
 - 19 + *SARResetCounter* – 8-bit hexadecimal number
 - 20 + *SARSequenceNumber* – Hexadecimal number of n bits, where n is less than or
21 equal to 48.
 - 22 + *SARSequenceRolloverCounter* – Hexadecimal number of (48 – length of
23 *SARSequenceNumber*) bits.
 - 24 + *PayloadSize* – Payload size in octets
 - 25 + *Payload* – Payload to be encrypted
 - 26 + *Payload* (Encrypted) – Encrypted payload of same size as input Payload and is
27 available at same memory space as the input Payload.
 - 28 + *CipheringKeyIndex* – ‘00’ (not encrypted); ‘01’, ‘10’, ‘11’ (encrypted with key
29 corresponding to index ‘01’, ‘10’ or ‘11’ respectively)

30 • DECRYPT

- 31 – Inputs: *Direction*, *DataUnit*, *StreamID*, *RouteCounter*, *SARResetCounter*,
32 *SARSequenceNumber*, *SARSequenceRolloverCounter*, *PayloadSize*, *Payload*,
33 *CipheringKeyIndex*

- 1 – Outputs: *Payload* (Decrypted)
- 2 – Possible values of each input and output are as follows:
 - 3 + *Direction* – ‘0’ (ForwardLink) or ‘1’ (ReverseLink)
 - 4 + *DataUnit* – ‘00’ (Octets), ‘01’ (RLP Packet Payload)
 - 5 + *StreamID* – 16-bit hexadecimal number
 - 6 + *RouteCounter* – 15-bit hexadecimal number
 - 7 + *SARResetCounter* – 8-bit hexadecimal number
 - 8 + *SARSequenceNumber* – Hexadecimal number of n bits, where n is less than or
 - 9 equal to 48.
 - 10 + *SARSequenceRolloverCounter* – Hexadecimal number of (48 – length of
 - 11 *SARSequenceNumber*) bits.
 - 12 + *PayloadSize* – Payload size in octets
 - 13 + *Payload* – Payload to be decrypted
 - 14 + *CipheringKeyIndex* – ‘00’ (not encrypted); ‘01’, ‘10’, ‘11’ (encrypted with key
 - 15 corresponding to index ‘01’, ‘10’ or ‘11’ respectively)
 - 16 + *Payload* (Decrypted) – Decrypted payload of same size as input Payload and is
 - 17 available at same memory space as the input Payload.

18 2.1.4 Local Common Data

19 This protocol does not define any Local Common Data.

20 2.1.5 Public Data

21 This protocol shall make the following data public:

- 22 • Subtype for this protocol
- 23 • [RTCCiphering](#)
- 24 • All data defined as Static Attribute, Static Non-Attribute Data, and Local Common Data

25 **2.2 Protocol Data Unit**

26 This protocol does not transmit or receive data. This protocol provides encryption and
27 decryption services to Radio Link Protocol.

28 **2.3 Procedures and Messages for the InConfiguration Instance of the Protocol**

29 2.3.1 Protocol Initialization for the InConfiguration Protocol Instance

30 Upon creation, the InConfiguration instance of this protocol in the access terminal and the
31 access network shall perform the procedures specified in [1].

1 2.3.2 Procedures

2 This protocol uses the services of the Session Control Protocol to perform negotiation of
3 attribute values.

4 2.3.3 Message Formats

5 This protocol does not define any messages.

6 **2.4 Procedures and Messages for the InUse Instance of the Protocol**

7 2.4.1 Procedures

8 2.4.1.1 Protocol Initialization for the InUse Protocol Instance

9 Upon creation, the InUse instance of this protocol in the access terminal and access
10 network shall perform the procedures specified in [1].

11 2.4.1.2 Hard Commit Procedures

12 The access terminal and the access network shall perform the procedures specified in
13 [1]when directed by the InUse instance of the Session Control Protocol to execute the Hard
14 Commit procedures.

15 2.4.1.3 Soft Commit Procedures

16 The access terminal and the access network shall perform the procedures specified in [1]
17 when directed by the InUse instance of the Session Control Protocol to execute the Soft
18 Commit procedures.

19 2.4.1.4 Constructing the Ciphering Key

20 The AES Ciphering Protocol shall construct the Ciphering keys as follows:

- 21 • If the value of the FTCCiphering attribute is equal to 0x01, then the protocol shall
22 construct the Ciphering key for the Forward Traffic Channel, FTCCipheringKey, as
23 follows:
 - 24 – If the FACCipheringKey[KeyIndex] public data of the Key Exchange Protocol is set to
25 NULL, the protocol shall set FTCCipheringKey to NULL.
 - 26 – Otherwise, the protocol shall perform the following:
 - 27 + If the length of FACCipheringKey[KeyIndex] is equal to 128, then
28 FTCCipheringKey shall be set to FACCipheringKey[KeyIndex].
 - 29 + Otherwise, if the length of FACCipheringKey[KeyIndex] is greater than 128, then
30 FTCCipheringKey shall be the 128 most significant bits of
31 FACCipheringKey[KeyIndex].
 - 32 + Otherwise, if the length of FACCipheringKey[KeyIndex] is less than 128, then
33 FTCCipheringKey shall be the concatenation of zeros at the end (LSB) of
34 FACCipheringKey[KeyIndex], such that the length of the result is 128.
 - 35 – The protocol shall perform the following:

- 1 + Call the KeyStrengthRedAlg procedure specified in [13] with its inputs set as
2 follows:
- 3 ▪ Set the *KeyLength* to 16.
- 4 ▪ Set the *OriginalKey* to the value of the FTCCipheringKey.
- 5 ▪ Set the *SaltLength* to the value of the FTCSaltLength parameter.
- 6 ▪ Set the *Salt* to the value of the FTCSalt parameter.
- 7 ▪ Set the *KeyEntropy* to the value of the FTCKeyEntropy parameter.
- 8 + When the KeyStrengthRedAlg procedure returns, set the FTCCipheringKey to
9 *RedStrengthKey* which is the output of the KeyStrengthRedAlg procedure.
- 10 • If the value of the RTCCiphering attribute is equal to 0x01, then the protocol shall
11 construct the Ciphering key for the Reverse Traffic Channel, RTCCipheringKey, as
12 follows:
- 13 – If the RACCipheringKey[KeyIndex] public data of the Key Exchange Protocol is set to
14 NULL, the protocol shall set RTCCipheringKey to NULL.
- 15 – Otherwise, the protocol shall perform the following:
- 16 + If the length of RACCipheringKey[KeyIndex] is equal to 128, then
17 RTCCipheringKey shall be set to RACCipheringKey[KeyIndex].
- 18 + Otherwise, if the length of RACCipheringKey[KeyIndex] is greater than 128, then
19 RTCCipheringKey shall be the 128 most significant bits of
20 RACCipheringKey[KeyIndex].
- 21 + Otherwise, if the length of RACCipheringKey[KeyIndex] is less than 128, then
22 RTCCipheringKey shall be the concatenation of zeros at the end (LSB) of
23 RACCipheringKey[KeyIndex], such that the length of the result is 128.
- 24 – The protocol shall perform the following:
- 25 + Call the KeyStrengthRedAlg procedure specified in [13] with its inputs set as
26 follows:
- 27 ▪ Set the *KeyLength* to 16.
- 28 ▪ Set the *OriginalKey* to the value of the RTCCipheringKey.
- 29 ▪ Set the *SaltLength* to the value of the RTCSaltLength parameter.
- 30 ▪ Set the *Salt* to the value of the RTCSalt parameter.
- 31 ▪ Set the *KeyEntropy* to the value of the RTCKeyEntropy parameter.
- 32 + When the KeyStrengthRedAlg procedure returns, set the RTCCipheringKey to
33 *RedStrengthKey* which is the output of the KeyStrengthRedAlg procedure.

34 2.4.1.5 Constructing the Cryptosync

35 The protocol shall construct the Cryptosync as shown in Table 2-1.

1

Table 2-1. Subfield of the Cryptosync

Subfield	Length (bits)
FunctionCode	2
Reserved	6
Direction	1
RouteCounter	15
StreamID	16
SARResetCounter	8
VirtualSARSequenceNumber	48

2 FunctionCode

This field shall be set to '00' to indicate Ciphering function.

3 Reserved

All the bits in this field shall be set to '0'.

4 Direction

If the payload being encrypted or decrypted is for Forward Link then this field shall be set to '0'. Otherwise, this field shall be set to '1'. Direction is received as *Direction* input to ENCRYPT and DECRYPT procedure calls.

8 RouteCounter

This field shall be set to the RouteCounter corresponding to the payload being encrypted or decrypted. RouteCounter is received as *RouteCounter* input to ENCRYPT and DECRYPT procedure calls.

12 StreamID

This field shall be set to the StreamID corresponding to the payload being encrypted or decrypted. StreamID is received as *StreamID* input to ENCRYPT and DECRYPT procedure calls.

15 SARResetCounter

This field shall be set to SARResetCounter corresponding to the payload being encrypted or decrypted. SARResetCounter is received as *SARResetCounter* input to ENCRYPT and DECRYPT procedure calls.

19 VirtualSARSequenceNumber This field shall be set to VirtualSARSequenceNumber corresponding to the payload being encrypted or decrypted. VirtualSARSequenceNumber value is set as specified in sections 2.4.1.6 and 2.4.1.7.

23 2.4.1.6 Encrypt Procedures

24 The protocol shall provide encryption services through ENCRYPT procedure call.

25 If any of the following conditions is true:

- 26 • The Ciphering attribute for the channel under consideration (e.g., FTCCiphering) is
27 equal to 0x00.

- 1 • The KeyIndex public data of the Key Exchange Protocol is set to NULL.
- 2 • The CipherringKey for the channel under consideration (e.g., FTCCipherringKey),
- 3 constructed as specified in 2.4.1.4 where KeyIndex is set to KeyIndex public data of the
- 4 Key Exchange Protocol, is NULL.
- 5 Then, the ENCRYPT procedure shall set the outputs of the ENCRYPT procedure as follows:
- 6 • Set *Payload* to the input *Payload*.
- 7 • Set *CipherringKeyIndex* to '00'.
- 8 Otherwise, the ENCRYPT procedure shall perform the following:
- 9 • If *DataUnit* is set to '01' then the ENCRYPT procedure shall perform the following:
- 10 – The ENCRYPT procedure shall call the ESP_AES procedure specified in [12] with its
- 11 inputs set as follows:
- 12 + Set the *key* to the CipherringKey for the channel under consideration (e.g.,
- 13 FTCCipherringKey) constructed as specified in 2.4.1.4 where KeyIndex is set to
- 14 KeyIndex public data of the Key Exchange Protocol.
- 15 + Set *fresh* to the value of the Cryptosync constructed as specified in 2.4.1.5,
- 16 where VirtualSARSequenceNumber is set to (*SARSequenceRolloverCounter* |
- 17 *SARSequenceNumber*).
- 18 + Set the *freshsize* to the length of the Cryptosync in octets.
- 19 + Set the *buf* to the address of the beginning of the memory space that contains
- 20 the *Payload*.
- 21 + Set the *bit_offset* to zero.
- 22 + Set the *bit_count* to 8 times *PayloadSize*.
- 23 – After the ESP_AES procedure is returned, the ENCRYPT procedure shall set the
- 24 outputs of the ENCRYPT procedure as follows:
- 25 + Set *Payload* to the output of the ESP_AES procedure which starts at the memory
- 26 space specified by *buf* and is of the same size as the input *Payload*.
- 27 + Set *CipherringKeyIndex* to KeyIndex public data of the Key Exchange Protocol.
- 28 • If *DataUnit* is set to '00' then the ENCRYPT procedure shall perform the following:
- 29 – Set VirtualSARSequenceNumberInUse to (*SARSequenceRolloverCounter* |
- 30 *SARSequenceNumber*)
- 31 – Set *n* to 1.
- 32 – The ENCRYPT procedure shall perform following steps *PayloadSize* times³:

³ Even though steps here are performed on each octet of payload, in implementation the steps can be performed on data blocks of 16 octets of payload except first and last data blocks which could have fewer octets.

- 1 + Call the ESP_AES procedure specified in [12] with its inputs set as follows:
- 2 ▪ Set the *key* to the CipherringKey for the channel under consideration (e.g.,
- 3 FTCCipherringKey) constructed as specified in 2.4.1.4 where KeyIndex is set
- 4 to KeyIndex public data of the Key Exchange Protocol.
- 5 ▪ Set *fresh* to the value of the Cryptosync constructed as specified in 2.4.1.5,
- 6 where VirtualSARSequenceNumber is set to $16 \times \lfloor$
- 7 VirtualSARSequenceNumberInUse / 16 \rfloor .
- 8 ▪ Set the *freshsize* to the length of the Cryptosync in octets.
- 9 ▪ Create a *temp_buf* and initialize it to (VirtualSARSequenceNumberInUse mod
- 10 16) octets of 0x00 followed by the nth octet of *Payload*. Set the *buf* to the
- 11 address of the beginning of the memory space that contains the *temp_buf*.
- 12 ▪ Set the *bit_offset* to zero.
- 13 ▪ Set the *bit_count* to $\lfloor (\text{VirtualSARSequenceNumberInUse mod } 16) + 1 \rfloor \times 8$.
- 14 + After the ESP_AES procedure is returned, the ENCRYPT procedure shall skip
- 15 first (VirtualSARSequenceNumberInUse mod 16) octets of the output of the
- 16 ESP_AES procedure which starts at the memory space specified by *temp_buf*,
- 17 and overwrite nth octet of the *Payload* with the value of the next octet of the
- 18 ESP_AES procedure output.
- 19 + Increment value of n
- 20 + Increment value of VirtualSARSequenceNumberInUse modulo 2^{48} .
- 21 – The ENCRYPT procedure shall set the outputs of the ENCRYPT procedure as
- 22 follows:
- 23 + Set *CipherringKeyIndex* to KeyIndex public data of the Key Exchange Protocol.

24 2.4.1.7 Decryption Procedures

25 The protocol shall provide decryption services through DECRYPT procedure call.

26 If the Cipherring attribute for the channel under consideration (e.g., FTCCipherring) is equal

27 to 0x01 and *CipherringKeyIndex* is not set to '00', the DECRYPT procedure shall perform the

28 following:

- 29 • If *DataUnit* is set to '01' then the DECRYPT procedure shall perform the following:
- 30 – The DECRYPT procedure shall call the ESP_AES procedure specified in [12] with its
- 31 inputs set as follows:
- 32 + Set the *key* to the CipherringKey for the channel under consideration (e.g.,
- 33 FTCCipherringKey) constructed as specified in 2.4.1.4 where KeyIndex is set to
- 34 *CipherringKeyIndex*.
- 35 + Set *fresh* to the value of the Cryptosync constructed as specified in 2.4.1.5,
- 36 where VirtualSARSequenceNumber is set to $(\text{SARSequenceRolloverCounter} \mid$
- 37 *SARSequenceNumber* $)$.
- 38 + Set the *freshsize* to the length of the Cryptosync in octets.

- 1 + Set the *buf* to the address of the beginning of the memory space that contains
2 the *Payload*.
- 3 + Set the *bit_offset* to zero.
- 4 + Set the *bit_count* to 8 times *PayloadSize*.
- 5 – After the ESP_AES procedure is returned, the DECRYPT procedure shall set the
6 outputs of the DECRYPT procedure as follows:
- 7 + Set *Payload* to the output of the ESP_AES procedure which starts at the memory
8 space specified by *buf* and is of the same size as the input *Payload*.
- 9 • If *DataUnit* is set to '00' then the DECRYPT procedure shall perform the following:
- 10 – Set *VirtualSARSequenceNumberInUse* to (*SARSequenceRolloverCounter* |
11 *SARSequenceNumber*).
- 12 – Set *n* to 1.
- 13 – The DECRYPT procedure shall perform following steps *PayloadSize* times⁴:
- 14 + Call the ESP_AES procedure specified in [12] with its inputs set as follows:
- 15 ▪ Set the *key* to the *CipheringKey* for the channel under consideration (e.g.,
16 *FTCCipheringKey*) constructed as specified in 2.4.1.4 where *KeyIndex* is set
17 to *CipheringKeyIndex*.
- 18 ▪ Set *fresh* to the value of the *Cryptosync* constructed as specified in 2.4.1.5,
19 where *VirtualSARSequenceNumber* is set to $16 \times \lfloor$
20 *VirtualSARSequenceNumberInUse* / 16 \rfloor .
- 21 ▪ Set the *freshsize* to the length of the *Cryptosync* in octets.
- 22 ▪ Create a *temp_buf* and initialize it to (*VirtualSARSequenceNumberInUse* mod
23 16) octets of 0x00 followed by the *n*th octet of *Payload*. Set the *buf* to the
24 address of the beginning of the memory space that contains the *temp_buf*.
- 25 ▪ Set the *bit_offset* to zero.
- 26 ▪ Set the *bit_count* to $\lfloor (\text{VirtualSARSequenceNumberInUse mod } 16) + 1 \rfloor \times 8$.
- 27 + After the ESP_AES procedure is returned, the DECRYPT procedure shall skip
28 first (*VirtualSARSequenceNumberInUse* mod 16) octets of the output of the
29 ESP_AES procedure which starts at the memory space specified by *temp_buf*,
30 and overwrite *n*th octet of the *Payload* with the value of the next octet of the
31 ESP_AES procedure output.
- 32 + Increment value of *n*.
- 33 + Increment value of *VirtualSARSequenceNumberInUse* modulo 2^{48} .

⁴ Even though steps here are performed on each octet of payload, in implementation the steps can be performed on data blocks of 16 octets of payload except first and last data blocks which could have fewer octets.

1 Otherwise, the DECRYPT procedure shall set the outputs of the DECRYPT procedure as
 2 follows:

- 3 • Set *Payload* to the input *Payload*

4 2.4.2 Message Formats

5 No messages are defined for the InUse instance of this protocol.

6 2.4.3 Interface to Other Protocols

7 2.4.3.1 Commands

8 This protocol does not issue any commands.

9 2.4.3.2 Indications

10 This protocol does not register to receive any indications.

11 **2.5 Configuration Attributes**

12 The following attributes and default values are defined (see [1] for attribute record
 13 definition).

14 2.5.1 Simple Attributes

15 The configurable simple attributes for this protocol are listed in the Table 2-2.

16 The default value for each attribute is typed in ***bold italics***.

17

Table 2-2. Configurable Values

Attribute ID	Attribute	Commit/Scope	Values	Meaning
0x0000	FTCCiphering	Soft/Dynamic	0x00	RLP packets destined for the FTC shall not be encrypted by the sender and shall not be decrypted by the receiver.
			<i>0x01</i>	RLP packets destined for the FTC shall be encrypted by the sender and shall be decrypted by the receiver.
			0x02-0xff	Reserved
0x0001	RTCCiphering	Soft/Dynamic	0x00	RLP packets destined for the RTC shall not be encrypted by the sender and shall not be decrypted by the receiver.
			<i>0x01</i>	RLP packets destined for the RTC shall be encrypted by the sender and shall be decrypted by the receiver.
			0x02-0xff	Reserved

1 2.5.2 Complex Attributes

2 The following complex attributes are defined for reduction of the Ciphering key strength for
3 each channel.

4 2.5.2.1 FTCSaltLengthCIPHERINGKey Attribute

5 The sender shall set AttributeID field to 0x8000.
6

Field	Length (bits)	Default Value
FTCSaltLength	8	0
FTCSalt	FTCSaltLength × 8	N/A
FTCKeyEntropy	8	16

7 FTCSaltLength The sender shall set this field to the length of the FTCSalt
8 field in octets.

9 FTCSalt The sender shall set this field to the value of the *Salt* input
10 parameter that is to be used in the KeyStrengthRedAlg
11 procedure specified in [13] for the FTC Ciphering key.

12 FTCKeyEntropy The sender shall set this field to the value of the *KeyEntropy*
13 input parameter that is to be used in the KeyStrengthRedAlg
14 procedure specified in [13] for the FTC Ciphering key. The
15 valid values for this field are 0 through 16, inclusive.
16

Commit	Hard	Scope	Dynamic
---------------	------	--------------	---------

17 2.5.2.2 RTCReducedStrengthCIPHERINGKey Attribute

18 The sender shall set AttributeID field to 0x8001.
19

Field	Length (bits)	Default Value
RTCSaltLength	8	0
RTCSalt	RTCSaltLength × 8	N/A
RTCKeyEntropy	8	16

20 RTCSaltLength The sender shall set this field to the length of the RTCSalt
21 field in octets.

22 RTCSalt The sender shall set this field to the value of the *Salt* input
23 parameter that is to be used in the KeyStrengthRedAlg
24 procedure specified in [13] for the RTC Ciphering key.

25 RTCKeyEntropy The sender shall set this field to the value of the *KeyEntropy*
26 input parameter that is to be used in the KeyStrengthRedAlg

1 procedure specified in [13] for the RTC Ciphering key. The
 2 valid values for this field are 0 through 16, inclusive.
 3

Commit	Hard	Scope	Dynamic
---------------	------	--------------	---------

4 **2.6 Non-Attribute Data**

5 This protocol does not define any non-attribute data.

6 **2.7 Protocol Numeric Constants**

7

Constant	Meaning	Value
N _{CPT} ype	Type field for this protocol	[1]
N _{CP} AES	Subtype field for this protocol	0x00

8 **2.8 Session State Information**

9 The Session State Information record (see [1]) consists of parameter records.

10 All configuration attributes and Non-attribute data are Session State Information records.

11 This protocol does not define additional parameter records.

- 1 No text.

1 **3 BASIC MESSAGE INTEGRITY PROTOCOL**

2 **3.1 3.1 Overview**

3 The Basic Message Integrity Protocol provides a method for integrity protection of signaling
4 messages by applying the AES CMAC function (see [14] and [15]).

5 **3.2 Primitives and Public Data**

6 3.2.1 Commands

7 This protocol does not define any commands.

8 3.2.2 Return Indications

9 This protocol does not define any indications.

10 3.2.3 Procedure Calls

- 11 • **AUTHENTICATE_ADD_TAG**
 - 12 – Inputs: *Direction*, *StreamID*, *RouteCounter*, *SARResetCounter*,
13 *SARSequenceNumber*, *SARSequenceRolloverCounter*, *InputPayloadSize*,
14 *InputPayload*
 - 15 – Outputs: *OutputPayloadSize*, *OutputPayload*
 - 16 – Possible values of each input and output are as follows:
 - 17 + *Direction* – ‘0’ (*ForwardLink*) or ‘1’ (*ReverseLink*)
 - 18 + *StreamID* – 16-bit hexadecimal number
 - 19 + *RouteCounter* – 15-bit hexadecimal number
 - 20 + *SARResetCounter* – 8-bit hexadecimal number
 - 21 + *SARSequenceNumber* – Hexadecimal number of n bits, where n is less than or
22 equal to 48
 - 23 + *SARSequenceRolloverCounter* – Hexadecimal number of (48 – length of
24 *SARSequenceNumber*) bits
 - 25 + *InputPayloadSize* – Input payload size in octets
 - 26 + *InputPayload* – Input payload
 - 27 + *OutputPayloadSize* – Output payload size in octets
 - 28 + *OutputPayload* – Output payload
- 29 • **AUTHENTICATE_CHECK_TAG**
 - 30 – Inputs: *Direction*, *StreamID*, *RouteCounter*, *SARResetCounter*, *SARSequenceNumber*,
31 *SARSequenceRolloverCounter*, *InputPayloadSize*, *InputPayload*
 - 32 – Outputs: *TagMatched*, *OutputPayloadSize*, *OutputPayload*

- 1 – Possible values of each input and output are as follows:
- 2 + *Direction* – ‘0’ (ForwardLink) or ‘1’ (ReverseLink)
- 3 + *StreamID* – 16-bit hexadecimal number
- 4 + *RouteCounter* – 15-bit hexadecimal number
- 5 + *SARResetCounter* – 8-bit hexadecimal number
- 6 + *SARSequenceNumber* – Hexadecimal number of n bits, where n is less than or
- 7 equal to 48.
- 8 + *SARSequenceRolloverCounter* – Hexadecimal number of (48 – length of
- 9 *SARSequenceNumber*) bits.
- 10 + *InputPayloadSize* – Input payload size in octets
- 11 + *InputPayload* – Input payload
- 12 + *TagMatched* – ‘1’ (TRUE), ‘0’ (FALSE)
- 13 + *OutputPayloadSize* – Output payload size in octets
- 14 + *OutputPayload* – Output payload
- 15 • CREATE_ID_TAG
- 16 – Inputs: SequenceNumber
- 17 – Outputs: IDTagSize, IDTag
- 18 – Possible values of each input and output are as follows:
- 19 + *SequenceNumber* – 32-bit hexadecimal number
- 20 + *IDTagSize* – ID Tag size in octets
- 21 + *IDTag* – ID Tag

22 3.2.4 Local Common Data

23 This protocol does not define any Local Common Data.

24 3.2.5 Public Data

25 This protocol shall make the following data public:

- 26 • Subtype for this protocol
- 27 • All data defined as Static Attribute, Static Non-Attribute Data, and Local Common Data

28 3.3 Protocol Data Unit

29 This protocol does not transmit or receive data. This protocol provides integrity protection
30 services to Radio Link Protocol.

1 **3.4 Procedures and Messages for the InConfiguration Instance of the Protocol**

2 3.4.1 Protocol Initialization for the InConfiguration Protocol Instance

3 Upon creation, the InConfiguration instance of this protocol in the access terminal and the
4 access network shall perform the procedures specified in [1].

5 3.4.2 Procedures

6 This protocol uses the services of the Session Control Protocol to perform negotiation of
7 attribute values.

8 3.4.3 Message Formats

9 This protocol does not define any messages.

10 **3.5 Procedures and Messages for the InUse Instance of the Protocol**

11 3.5.1 Procedures

12 3.5.1.1 Protocol Initialization for the InUse Protocol Instance

13 Upon creation, the InUse instance of this protocol in the access terminal and access
14 network shall perform the procedures specified in [1].

15 3.5.1.2 Hard Commit Procedures

16 The access terminal and the access network shall perform the procedures specified in [1]
17 when directed by the InUse instance of the Session Control Protocol to execute the Hard
18 Commit procedures.

19 3.5.1.3 Soft Commit Procedures

20 The access terminal and the access network shall perform the procedures specified in [1]
21 when directed by the InUse instance of the Session Control Protocol to execute the Soft
22 Commit procedures.

23 3.5.1.4 Constructing the Message Integrity Key

24 Basic Message Integrity Protocol shall construct the Message Integrity keys as follows:

- 25 • The protocol shall construct the Message Integrity key for the Forward Traffic Channel,
26 FTCKMIKey as follows:
 - 27 – If the FACMKIKey[KeyIndex] public data of the Key Exchange Protocol is set to NULL,
28 the protocol shall set FTCKMIKey to NULL.
 - 29 – Otherwise, the protocol shall perform the following:
 - 30 + If the length of FACMKIKey[KeyIndex] is equal to 128 bits, then FTCKMIKey shall
31 be set to FACMKIKey[KeyIndex].
 - 32 + Otherwise, if the length of FACMKIKey[KeyIndex] is greater than 128 bits, then
33 FTCKMIKey shall be the 128 most significant bits of FACMKIKey[KeyIndex].

- 1 + Otherwise, if the length of FACMIKey[KeyIndex] is less than 128 bits, then
 2 FTCTMIKey shall be the concatenation of zeros at the end (LSB) of
 3 FACMIKey[KeyIndex], such that the length of the result is 128 bits.
- 4 • The protocol shall construct the Message Integrity key for the Reverse Traffic Channel,
 5 RTCTMIKey as follows:
 - 6 – If the RACMIKey[KeyIndex] public data of the Key Exchange Protocol is set to NULL,
 7 the protocol shall set RTCTMIKey to NULL.
 - 8 – Otherwise, the protocol shall perform the following:
 - 9 + If the length of RACMIKey[KeyIndex] is equal to 128 bits, then RTCTMIKey shall
 10 be set to RACMIKey[KeyIndex].
 - 11 + Otherwise, if the length of RACMIKey[KeyIndex] is greater than 128 bits, then
 12 RTCTMIKey shall be the 128 most significant bits of RACMIKey[KeyIndex].
 - 13 + Otherwise, if the length of RACMIKey[KeyIndex] is less than 128 bits, then
 14 RTCTMIKey shall be the concatenation of zeros at the end (LSB) of
 15 RACMIKey[KeyIndex], such that the length of the result is 128 bits.

16 3.5.1.5 Constructing the Cryptosync

17 The protocol shall construct the Cryptosync as shown in Table 3-1.

18 **Table 3-1. Subfield of the Cryptosync**

Subfield	Length (bits)
Direction	1
RouteCounter	15
StreamID	16
SARResetCounter	8
VirtualSARSequenceNumber	48

- 19 Reserved All the bits in this field shall be set to '0'.
- 20 Direction If the payload is for Forward Link then this field shall be set
 21 to '0'. Otherwise, this field shall be set to '1'. Direction is
 22 received as Direction input to AUTHENTICATE_ADD_TAG and
 23 AUTHENTICATE_CHECK_TAG procedure calls.
- 24 RouteCounter This field shall be set to the RouteCounter corresponding to
 25 the payload. RouteCounter is received as RouteCounter input
 26 to AUTHENTICATE_ADD_TAG and
 27 AUTHENTICATE_CHECK_TAG procedure calls.
- 28 StreamID This field shall be set to the StreamID corresponding to the
 29 payload. StreamID is received as StreamID input to

1 AUTHENTICATE_ADD_TAG and
2 AUTHENTICATE_CHECK_TAG procedure calls.

3 SARResetCounter This field shall be set to SARResetCounter corresponding to
4 the payload. SARResetCounter is received as
5 SARResetCounter input to AUTHENTICATE_ADD_TAG and
6 AUTHENTICATE_CHECK_TAG procedure calls.

7 VirtualSARSequenceNumber This field shall be set to VirtualSARSequenceNumber
8 corresponding to the payload. VirtualSARSequenceNumber
9 value is set as specified in sections 3.5.1.7 and 3.5.1.8.

10 3.5.1.6 Authentication Header

11 The Authentication Header, which precedes the payload, has the following format, as
12 shown in Table 3-2.

13 **Table 3-2. Authentication Headers**

Field	Length (bits)
AuthKeyIndex	2
Reserved	6
AuthTag	0 or 64

14 AuthKeyIndex The protocol shall set this field to indicate index of the key
15 used for authentication of the payload as specified in Table
16 3-3.

17 **Table 3-3. AuthKeyIndex encoding**

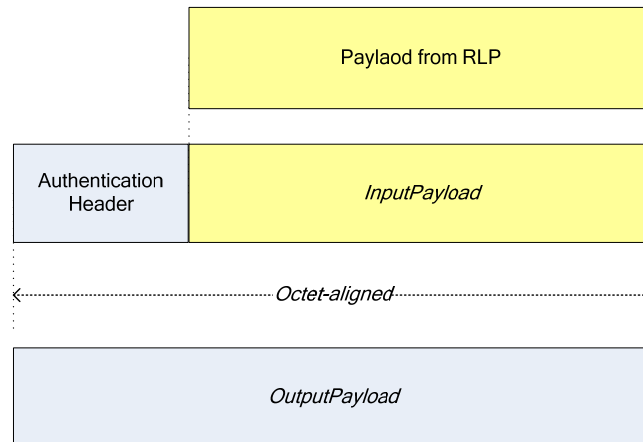
AuthKeyIndex	Meaning
'00'	AuthTag not included
'01'	AuthTag computed with key corresponding to index '01'
'10'	AuthTag computed with key corresponding to index '10'
'11'	AuthTag computed with key corresponding to index '11'

18 Reserved The protocol shall set all the bits in this field to '0'.

19 AuthTag The protocol shall omit this field if the AuthKeyIndex field is
20 set to '00'; otherwise, the protocol shall include this field and
21 set it to authentication tag.

1 3.5.1.7 AUTHENTICATE_ADD_TAG procedures

2 The protocol shall provide service of adding authentication tag through
 3 AUTHENTICATE_ADD_TAG procedure call. Figure 3-1 illustrates the relationship between
 4 an InputPayload and an OutputPayload of AUTHENTICATE_ADD_TAG procedure call.



5

6

Figure 3-1. AUTHENTICATE_ADD_TAG procedure call payloads

7 If any of the following conditions is true:

- 8 • The KeyIndex public data of the Key Exchange Protocol is set to NULL.
- 9 • The MIKey for the channel under consideration (e.g., FTCTMIKey), constructed as
 10 specified in 3.5.1.4 where KeyIndex is set to KeyIndex public data of the Key Exchange
 11 Protocol, is NULL.
- 12 • Payload contains a message for which authentication tag is not required (See [1] and
 13 each protocol text) and if protocol decides not to include the authentication tag.

14 then, the AUTHENTICATE_ADD_TAG procedure shall set the outputs of the
 15 AUTHENTICATE_ADD_TAG procedure as follows:

- 16 • Construct Authentication Header with the AuthKeyIndex field set to '00'.
- 17 • Set *OutputPayload* to (Authentication Header | *InputPayload*).
- 18 • Set *OutputPayloadSize* to (*InputPayloadSize* + size of the Authentication Header in
 19 octets).

20 Otherwise, the AUTHENTICATE_ADD_TAG procedure shall perform the following:

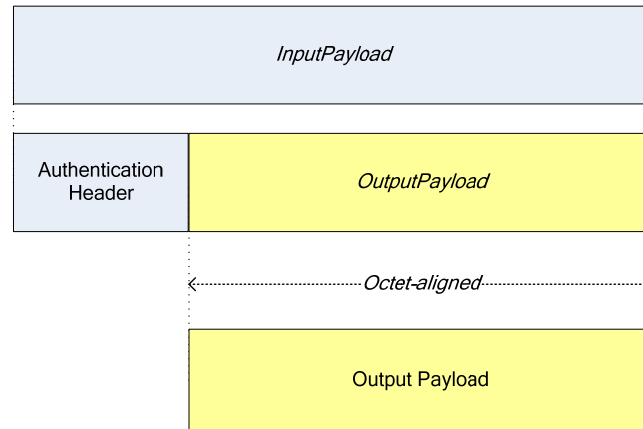
- 21 • The AUTHENTICATE_ADD_TAG procedure shall call the CMAC(K, M, Mlen, Tlen)
 22 procedure specified in Section 6.2 of [16] with its inputs set as follows:
- 23 – Set the *K* to the MIKey for the channel under consideration (e.g., FTCTMIKey)
 24 constructed as specified in 3.5.1.4 where KeyIndex is set to KeyIndex public data of
 25 the Key Exchange Protocol.

- 1 – Set the M to $BOHeader | B0 | InputPayload$, where $BOHeader$ and $B0$ are set as
2 follows:
- 3 + Set $BOHeader$ to ‘10011100’⁵.
- 4 + Set $B0$ to $(fresh | L)$, where $fresh$ is set to the value of the Cryptosync
5 constructed as specified in 3.5.1.5 with $VirtualSARSequenceNumber$ set to
6 $(SARSequenceRolloverCounter | SARSequenceNumber)$, and L is set to size of the
7 $InputPayload$ in octets expressed as 32-bit hexadecimal number.
- 8 – Set the $Mlen$ to 8 times size of M in octets.
- 9 – Set the $Tlen$ to 64.
- 10 • After the CMAC procedure is returned, the AUTHENTICATE_ADD_TAG procedure shall
11 set the outputs of the AUTHENTICATE_ADD_TAG procedure as follows:
- 12 – Construct Authentication Header with fields set as follows:
- 13 + Set the AuthTag field to the output of the CMAC procedure.
- 14 + Set the AuthKeyIndex field to KeyIndex public data of the Key Exchange
15 Protocol.
- 16 – Set $OutputPayload$ to $(Authentication\ Header | InputPayload)$
- 17 – Set $OutputPayloadSize$ to $(InputPayloadSize + \text{size of the Authentication Header in}$
18 octets)

19 3.5.1.8 AUTHENTICATE_CHECK_TAG procedures

20 The protocol shall provide service of checking authentication tag through
21 AUTHENTICATE_CHECK_TAG procedure call. Figure 3-2 illustrates the relationship
22 between an $InputPayload$ and an $OutputPayload$ of AUTHENTICATE_CHECK_TAG
23 procedure call.

⁵ Bits 5,4,3 of $BOHeader$ are encoded as $(M-2)/2$; where MSB of $BOHeader$ is bit 7, and M is $Tlen/8$ and can take the values 4, 6, 8, 10, 12, 14 and 16. Presently $Tlen$ is always 64, and hence bits 5, 4, 3 or $BOHeader$ are always set to 011.



1

2

Figure 3-2. AUTHENTICATE_CHECK_TAG procedure call payloads

3 The AUTHENTICATE_CHECK_TAG procedure shall perform the following:

- 4 • The *InputPayload* consists of (Authentication Header | *OutputPayload*).
- 5 • The AUTHENTICATE_CHECK_TAG procedure shall remove Authentication Header from
- 6 *InputPayload* to produce *OutputPayload*.
- 7 • If the AuthKeyIndex field of the Authentication Header is set to '00', then
- 8 AUTHENTICATE_CHECK_TAG procedure shall set the outputs of the
- 9 AUTHENTICATE_CHECK_TAG procedure as follows:
- 10 – Set *TagMatched* to TRUE.
- 11 – Set *OutputPayloadSize* to size of *OutputPayload* in octets.
- 12 • Otherwise, the AUTHENTICATE_CHECK_TAG procedure shall call the CMAC(K, M,
- 13 Mlen, Tlen) procedure specified in Section 6.2 of [16] with its inputs set as follows:
- 14 – Set the *K* to the MIKey for the channel under consideration (e.g., FTCMIKey)
- 15 constructed as specified in 3.5.1.4 where KeyIndex is set to AuthKeyIndex field of
- 16 the Authentication Header.
- 17 – Set the *M* to B0Header | B0 | *OutputPayload*, where B0Header and B0 are set as
- 18 follows:
- 19 + Set B0Header to '10011100'⁶.
- 20 + Set B0 to (fresh | L), where fresh is set to the value of the Cryptosync
- 21 constructed as specified in 3.5.1.5 with VirtualSARSequenceNumber set to
- 22 (SARSequenceRolloverCounter | SARSequenceNumber), and L is set to size of the
- 23 *OutputPayload* in octets expressed as 32-bit hexadecimal number.

⁶ Bits 5,4,3 of B0Header are encoded as $(M-2)/2$; where MSB of B0Header is bit 7, and M is Tlen/8 and can take the values 4, 6, 8, 10, 12, 14 and 16. Presently Tlen is always 64, and hence bits 5, 4, 3 or B0Header are always set to 011.

- 1 – Set the *Mlen* to 8 times size of *M* in octets.
- 2 – Set the *Tlen* to 64.
- 3 • After the CMAC procedure is returned, the AUTHENTICATE_CHECK_TAG procedure
- 4 shall set the outputs of the AUTHENTICATE_CHECK_TAG procedure as follows:
- 5 – If output of the CMAC procedure matches the AuthTag field of the Authentication
- 6 Header, then set *TagMatched* to TRUE. Otherwise, set *TagMatched* to FALSE.
- 7 – Set *OutputPayloadSize* to size of *OutputPayload* in octets.

8 3.5.1.9 CREATE_ID_TAG procedures

9 The protocol shall provide service of creating IDTag CREATE_ID_TAG procedure call.

10 The CREATE_ID_TAG procedure shall perform the following:

- 11 • If ~~SessionAnchorKeyIndex~~KeyIndex or
- 12 ~~SessionAnchorRACMIKeyInUseRACMIKey[KeyIndex]~~ public ~~local~~ common data of the
- 13 Key Exchange Protocol is set to NULL, then perform the following:
- 14 – Set Reserved1 to '000000'.
- 15 – Set MIKeyIndex to '00'.
- 16 – Set Reserved2 to '0'.
- 17 – Set SessionAnchorRouteID to 7-bit RouteID of the SessionAnchor Route.
- 18 – sSet the outputs of the CREATE_ID_TAG procedure as follows:
 - 19 ~~+~~ + Set *IDTagSize* to 20
 - 20 ~~+~~ + Set *IDTag* to (Reserved1 | MIKeyIndex | Reserved2 | SessionAnchorRouteID)
 - 21 ~~+~~ + ~~NULL~~
- 22 • Otherwise, perform the following:
 - 23 – Set Reserved1 to '000000'.
 - 24 – Set MIKeyIndex to 2-bit SessionAnchorKeyIndex local common data of the Key
 - 25 Exchange Protocol.
 - 26 – Set Reserved2 to '0'.
 - 27 – Set SessionAnchorRouteID to 7-bit RouteID of the SessionAnchor Route.
 - 28 – ~~Set MIKeyID to EHMACHASH256(key=RACMIKey[KeyIndex], message= "MIKeyID",~~
 - 29 ~~MAC_length=4), where RACMIKey[KeyIndex] and KeyIndex are public data of the~~
 - 30 ~~Key Exchange Protocol and EHMACHASH256 function is specified in 4.5.1.8.~~
 - 31 – Set Tag to EHMACHASH256-
 - 32 SHA256(key=~~SessionAnchorRACMIKeyInUseRACMIKey[KeyIndex]~~, message=
 - 33 ~~SequenceNumber, MAC_length=8), where~~
 - 34 ~~SessionAnchorRACMIKeyInUseRACMIKey[KeyIndex] and KeyIndex are public is~~
 - 35 ~~local common~~ data of the Key Exchange Protocol, EHMACHASH256 function is
 - 36 specified in 4.5.1.8.

- 1 – Set the outputs of the CREATE_ID_TAG procedure as follows:
- 2 + Set *IDTagSize* to 102
- 3 + Set *IDTag* to (~~MIKeyID-Reserved1~~ | MIKeyIndex | Reserved2 |
- 4 SessionAnchorRouteID | Tag)

5 3.5.2 Message Formats

6 No messages are defined for the InUse instance of this protocol.

7 **3.6 Interface to Other Protocols**

8 3.6.1 Commands

9 This protocol does not issue any commands.

10 3.6.2 Indications

11 This protocol does not register to receive any indications.

12 **3.7 Configuration Attributes**

13 This protocol does not define any attributes.

14 **3.8 Non-Attribute Data**

15 This protocol does not define any non-attribute data.

16 **3.9 Protocol Numeric Constants**

17 **Table 3-4. Protocol Numeric Constants**

Constant	Meaning	Value
$N_{MIPType}$	Type field for this protocol	[1]
N_{BMIP}	Subtype field for this protocol	0x00

18 **3.10 Session State Information**

19 The Session State Information record (see [1]) consists of parameter records.

20 All configuration attributes and Non-attribute data are Session State Information records.

21 This protocol does not define additional parameter records.

1 **4 BASIC KEY EXCHANGE PROTOCOL**

2 **4.1 Overview**

3 The Basic Key Exchange Protocol provides a method for generating security keys at the
4 access terminal and the access network based on a Pairwise Master Key. The Pairwise
5 Master Key is established by higher layer protocols.

6 The Basic Key Exchange Protocol performs the following functions:

- 7 • Proves that both access terminal and access network have the same Pairwise Master
8 Key.
- 9 • Derives security keys from the Pairwise Master Key.
- 10 • Protects against a man-in-the-middle attack where a rogue entity causes the access
11 terminal and the access network to agree upon a weaker security protocol.

12 **4.2 Primitives and Public Data**

13 4.2.1 Commands

14 This protocol does not define any commands.

15 4.2.2 Return Indications

16 This protocol ~~does not~~ returns any following indications:-

- 17 • KeyExchange.KeyExchangeCompleted(Result) (AT only)

18 4.2.3 Local Common Data

19 This protocol defines the following Local Common Data (i.e., AT only):

- 20 • PMKList[]
21 A list of all Pairwise Master Keys.
- 22 • SessionAnchorKeyIndex
23 KeyIndex of the SessionAnchor Route. The access terminal shall set this data to
24 KeyIndex of the SessionAnchorRoute.
- 25 • SessionAnchorRACMIKeyInUse
26 Message Integrity Key used on Reverse Assigned Channels of the SessionAnchor Route.
27 The access terminal shall set this data to RACMIKey[KeyIndex] of the
28 SessionAnchorRoute.

29 4.2.4 Public Data

30 This protocol shall make the following data public:

- 31 • Subtype for this protocol
- 32 • ~~LatestPMK (access terminal only)~~
33 ~~Latest PMK established or used on this route.~~

1 •~~LatestPMKCreationTime (access terminal only)~~

2 ~~Creation time of the LatestPMK~~

3 • KeyIndex

4 The key index in use. Valid values are '01', '10', and '11'.

5 • FACMIKey[i] and its length for values of i '01' through '11'

6 The Message Integrity key for use on Forward Assigned Channels (e.g., the Forward
7 Traffic Channel).

8 • RACMIKey[i] and its length for values of i '01' through '11'

9 The Message Integrity key for use on Reverse Assigned Channels (e.g., the Reverse
10 Traffic Channel).

11 • FACCipheringKey[i] and its length for values of i '01' through '11'

12 The Ciphering key for use on Forward Assigned Channels (e.g., the Forward Traffic
13 Channel).

14 • RACCipheringKey[i] and its length for values of i '01' through '11'

15 The Ciphering key for use on Reverse Assigned Channels (e.g., the Reverse Traffic
16 Channel).

17 • All data defined as Static Attribute, Static Non-Attribute Data, and Local Common Data

18 4.2.5 Interface to Other Protocols

19 4.2.5.1 Commands

20 This protocol does not define any commands.

21 4.2.5.2 Indications

22 This protocol does not register to receive any indications.

23 **4.3 Protocol Data Unit**

24 The transmission unit of this protocol is a message. This is a control protocol and,
25 therefore, it does not carry payload on behalf of other layers or protocols.

26 This protocol uses the Signaling Protocol to transmit and receive messages.

27 **4.4 Procedures and Messages for the InConfiguration Instance of the Protocol**

28 4.4.1 Protocol Initialization for the InConfiguration Protocol Instance

29 Upon creation, the InConfiguration instance of this protocol in the access terminal and the
30 access network shall perform the procedures specified in [1].

31 4.4.2 Procedures

32 This protocol uses the services of the Session Control Protocol to perform negotiation of
33 attribute values.

1 The access network shall not initiate negotiation of the ATSupportedSecuritySubtypes
2 attribute.

3 If the ATSupportedSecuritySubtypes attribute is set to its default value, then the access
4 terminal shall initiate negotiation of the ATSupportedSecuritySubtypes attribute at the
5 earliest opportunity (i.e. when Session Control Protocol is in AT Initiated State).

6 4.4.3 Message Formats

7 This protocol does not define any messages.

8 **4.5 Procedures and Messages for the InUse Instance of the Protocol**

9 4.5.1 Procedures

10 The Basic Key Exchange Protocol derives security keys and exchanges security capabilities
11 as well as security protocols in use. The key exchange procedure uses the KeyRequest,
12 KeyResponse, KeyComplete, KeyReject, and InitiateKeyRequest messages.

13 4.5.1.1 Protocol Initialization for the InUse Protocol Instance

14 Upon creation, the InUse instance of this protocol in the access terminal and the access
15 network shall perform the following in the order specified:

- 16 • Perform the procedures specified in [1].
- 17 ~~• Access terminal shall Set LatestPMK to NULL.~~
- 18 ~~• Access terminal shall set LatestPMKCreationTime to NULL.~~
- 19 • Set KeyIndex to NULL.
- 20 • Set FACMIKey[i] to NULL, for values of i '01' through '11'.
- 21 • Set RACMIKey[i] to NULL, for values of i '01' through '11'.
- 22 • Set FACCipheringKey[i] to NULL, for values of i '01' through '11'.
- 23 • Set RACCipheringKey[i] to NULL, for values of i '01' through '11'.

24 4.5.1.2 Hard Commit Procedures

25 The access terminal and the access network shall perform the procedures specified in [1]
26 when directed by the InUse instance of the Session Control Protocol to execute the Hard
27 Commit procedures.

28 4.5.1.3 Soft Commit Procedures

29 The access terminal and the access network shall perform the procedures specified in [1]
30 when directed by the InUse instance of the Session Control Protocol to execute the Soft
31 Commit procedures.

32 4.5.1.4 Access Terminal Requirements

33 ~~When a Pairwise Master Key is established by higher layer protocols, the access terminal~~
34 ~~shall perform the following:~~

1 ~~•Add the established PMK to the PMKList along with creation time of the key.~~

2 ~~•Set LatestPMK to the established PMK~~

3 ~~•Set LatestPMKCreationTime to creation time of the established PMK.~~

4 4.5.1.4.1 Initiating the key exchange

5 Access terminal may initiate the key exchange procedure by sending a KeyRequest
6 message. If a Pairwise Master Key is available, then the aAccess terminal ~~should~~ shall send
7 a KeyRequest message when a new route open procedure is initiated.

8 Upon receiving the InitiateKeyRequest message, the access terminal shall send a
9 KeyRequest message unless access terminal has already sent a KeyRequest message and is
10 awaiting the response.

11 4.5.1.4.2 Processing a KeyResponse message

12 Upon receiving the KeyResponse message with a TransactionID field that matches the
13 TransactionID field of the associated KeyRequest message, the access terminal shall
14 perform the following in the order in which the requirements are specified:

- 15 • The access terminal shall identify the PairwiseMasterKey ~~from PMKList of any route~~
16 that satisfies PairwiseMasterKeyID = EHMAC-SHA256(key=PairwiseMasterKey,
17 message= "PairwiseMasterKeyID", MAC_length=8), where PairwiseMasterKeyID is a field
18 of the received KeyResponse message, "PairwiseMasterKeyID" is the ASCII encoded
19 value of the string, and the EHMAC-SHA256 function is specified in 4.5.1.8.
- 20 • If the access terminal cannot identify a valid PairwiseMasterKey that satisfies the above
21 condition, then the access terminal shall send a KeyComplete message with Result set
22 to 0x03, declare failure, return a KeyExchange.KeyExchangeCompleted(Result)
23 indication with Result set to Failed and stop performing the rest of the key exchange
24 procedure.
- 25 • The access terminal shall generate MICKey as specified in 4.5.1.6.
- 26 • The access terminal shall generate a MessageIntegrityCode as EHMAC-
27 SHA256(key=MICKey, message=Message, MAC_length=16), where Message is the
28 received KeyResponse message with the MessageIntegrityCode field set to zero, and the
29 EHMAC-SHA256 function is specified in 4.5.1.8.
- 30 • If the MessageIntegrityCode computed in the previous step does not match the
31 MessageIntegrityCode field of KeyResponse message, then the access terminal shall
32 declare failure, send a KeyComplete message with Result set to 0x01, return a
33 KeyExchange.KeyExchangeCompleted(Result) indication with Result set to Failed, and
34 stop performing the rest of the key exchange procedure.

- 1 • If the MessageIntegritySubtypes, CipheringSubtypes, KeyExchangeSubtypes~~supported~~
2 ProtocolSetIdentifiers sent by the access network in the KeyResponse message do not
3 match with the corresponding Subtypes of the Message Integrity Protocol, the Ciphering
4 Protocol, and the Key Exchange Protocol~~ProtocolSetIdentifiers~~ supported by the access
5 terminal (i.e., either all the Subtypes~~ProtocolSetIdentifiers~~ supported by the access
6 terminal are not included in the KeyResponse message or KeyResponse message
7 includes a Subtypes~~ProtocolSetIdentifiers~~ that is not supported by the access terminal),
8 then the access terminal shall declare failure, send a KeyComplete message with Result
9 set to 0x02, return a KeyExchange.KeyExchangeCompleted(Result) indication with
10 Result set to Failed, and stop performing the rest of the key exchange procedure.
- 11 • If the first MessageIntegritySubtype, CipheringSubtype, KeyExchangeSubtype
12 ProtocolSetIdentifier fields sent by the access network in the KeyResponse message do
13 not match with the Subtypes of the Message Integrity Protocol, the Ciphering Protocol,
14 and the Key Exchange Protocol~~ProtocolSetIdentifier~~ currently in use by the access
15 terminal, then the access terminal shall declare failure, send a KeyComplete message
16 with Result set to 0x04, return a KeyExchange.KeyExchangeCompleted(Result)
17 indication with Result set to Failed, and stop performing the rest of the key exchange
18 procedure.
- 19 • The access terminal shall generate Message Integrity Keys and Ciphering Keys as
20 specified in 4.5.1.7 for KeyIndex value specified in the KeyResponse message. The
21 access terminal shall set KeyIndex public data to KeyIndex value specified in the
22 KeyResponse message.
- 23 • The access terminal shall send a KeyComplete message with Result set to 0x00.
- 24 • Return a KeyExchange.KeyExchangeCompleted(Result) indication with Result set to
25 Successful.
- 26 ~~• If LatestPMKCreationTime is set to NULL or if creation time of PMK identified by the~~
27 ~~PairwiseMasterKeyID field of the received KeyResponse message is more recent than~~
28 ~~time indicated by LatestPMKCreationTime, then access terminal shall perform the~~
29 ~~following:~~
- 30 ~~–Set LatestPMK to PMK identified by the PairwiseMasterKeyID field of the received~~
31 ~~KeyResponse message.~~
- 32 ~~–Set LatestPMKCreationTime to creation time of LatestPMK.~~

33 4.5.1.4.3 Processing a KeyReject message

34 Upon receiving the KeyReject message with a TransactionID field that matches the
35 TransactionID field of the associated KeyRequest message, the access terminal shall return
36 a KeyExchange.KeyExchangeCompleted(Result) indication with Result set to Rejected, and
37 terminate the key exchange procedure.

38 4.5.1.4.4 Processing an ATSupportedSecuritySubtypesRequest message

39 Upon receiving the ATSupportedSecuritySubtypesRequest message, the access terminal
40 shall send a ATSupportedSecuritySubtypesResponse message.

1 4.5.1.5 Access Network Requirements

2 4.5.1.5.1 Initiating the key exchange

3 Access network may initiate the key exchange procedure by sending an InitiateKeyRequest
4 message.

5 4.5.1.5.2 Processing a KeyRequest message

6 Upon receiving the KeyRequest message, the access network shall perform the following in
7 the order in which the requirements are specified:

- 8 • The access network shall send a KeyResponse message or a KeyReject message.
- 9 • If a KeyResponse message was sent, the access network shall generate MICKey as
10 specified in 4.5.1.6.

11 4.5.1.5.3 Processing a KeyComplete message

12 After receiving a KeyComplete message with a TransactionID field that matches the
13 TransactionID field of the associated KeyResponse message, the access network shall
14 perform the following:

- 15 • The access network shall generate a MessageIntegrityCode as EHMAL-
16 SHA256(key=MICKey, message=Message, MAC_length=16), where Message is the
17 received KeyComplete message with the MessageIntegrityCode field set to zero, and the
18 EHMAL-SHA256 function is specified in 4.5.1.8.
- 19 • If the MessageIntegrityCode computed in the previous step does not match the
20 MessageIntegrityCode field of KeyComplete message, then the access network shall
21 declare failure, and shall not use Message Integrity Keys and Ciphering Keys generated
22 in this key exchange procedure.
- 23 • If the Result field of the KeyComplete message is not 0x00, then the access network
24 shall declare failure and shall not use Message Integrity Keys and Ciphering Keys
25 generated in this key exchange procedure.

26 4.5.1.6 MICKey Derivation

27 The access terminal and the access network shall derive MICKey as follows:

- 28 • Set MICKey to zero and its length to 128.
- 29 • Set MICKey to EHMAL-SHA256(key=PairwiseMasterKey, message=
30 "MICKey"|ATNonce|ANNonce, MAC_length=16), where "MICKey" is the ASCII encoded
31 value of the string, and the EHMAL-SHA256 function is specified in 4.5.1.8.

32 4.5.1.7 Message Integrity Key and Ciphering Key Generation

33 The access terminal and the access network shall generate a TSKey as specified in
34 4.5.1.7.1. The access terminal and the access network shall generate Message Integrity and
35 Ciphering keys from TSKey as specified in 4.5.1.7.2.

1 4.5.1.7.1 Temporary Security Key Derivation

2 The access terminal and the access network shall derive TSKey as follows:

- 3 • Set TSKey to zero and its length to $N_{\text{BKEPTKeyLen}}$.
- 4 • Set j to an 8-bit number with value zero.
- 5 • while $j < N_{\text{BKEPTKeyLen}}/256$
 - 6 – Set TSKey to $N_{\text{BKEPTKeyLen}}$ least significant bits of { TSKey | EHMAC-
 - 7 SHA256(key=PairwiseMasterKey, message= “TSK” | ATNonce | ANNonce | j ,
 - 8 MAC_length=32) }, where “TSK” is the ASCII encoded value of the string, j is
 - 9 represented as an 8-bit field, and the EHMAC-SHA256 function is specified in
 - 10 4.5.1.8.
 - 11 – Set j to $j+1$.

12 4.5.1.7.2 Message Integrity Key and Ciphering Keys Generation from TSKey

13 The keys used for Message Integrity and Ciphering are generated from the temporary
14 security key using the procedures specified in this section.

15 The access network and the access terminal shall compute and store Message Integrity
16 Keys and Ciphering Keys for KeyIndex i as follows:

- 17 • The access network and the access terminal shall set FACMIKey[i] to TSKey[127:0].
- 18 • The access network and the access terminal shall set RACMIKey[i] to TSKey[127:0].
- 19 • The access network and the access terminal shall set FACCIpheringKey[i] to
20 TSKey[255:128].
- 21 • The access network and the access terminal shall set RACCIpheringKey[i] to
22 TSKey[255:128].

23 4.5.1.8 EHMAC-SHA256(key, message, MAC_length)

24 The EHMAC-SHA256 procedure shall call ehmacsha256 procedure as specified in [13] with
25 following inputs:

- 26 • Set the *key_length* to the length of the key in bits,
- 27 • Set the *key* to the key,
- 28 • Set the *message* to the message, and
- 29 • Set the *message_length* to the length of the message in bits,
- 30 • Set the *message_offset* to 0,
- 31 • Set the *MAC_length* to $8 \times \text{MAC_length}$.

32 The output of the EHMAC-SHA256 function shall be set to the output of the ehmacsha256
33 procedure.

1 4.5.2 Message Formats

2 4.5.2.1 KeyRequest

3 The access terminal sends the KeyRequest message to initiate the session key exchange.

4 **Table 4-1. KeyRequest Message**

Field	Length (bits)
MessageID	8
TransactionID	8
ATNonce	128

5 MessageID The access terminal shall set this field to 0x00.

6 TransactionID The access terminal shall increment this value for each new
7 KeyRequest message sent.8 ATNonce The access terminal shall set this field to a 128-bit random
9 number.

10

Channels	RTC
Addressing	unicast

RLP	Reliable
AuthTag	Required when key is available

11 4.5.2.2 KeyResponse

12 The access network may send the KeyResponse message in response to the KeyRequest
13 message.
14

Field	Length (bits)
MessageID	8
TransactionID	8
KeyIndex	2
Reserved	6
PairwiseMasterKeyID	64
ANNonce	128
<u>NumProtocolSetIdentifiers</u>	<u>8</u>
<u>NumProtocolSetIdentifiers occurrences of the following field:</u>	
<u>ProtocolSetIdentifier</u>	<u>16</u>
<u>MessageIntegritySubtypeCount</u>	<u>8</u>
<u>MessageIntegritySubtypeCount occurrences of the following field:</u>	
<u>MessageIntegritySubtype</u>	<u>8</u>
<u>CipheringSubtypeCount</u>	<u>8</u>
<u>CipheringSubtypeCount occurrences of the following field:</u>	
<u>CipheringSubtype</u>	<u>8</u>
<u>KeyExchangeSubtypeCount</u>	<u>8</u>
<u>KeyExchangeSubtypeCount occurrences of the following field:</u>	
<u>KeyExchangeSubtype</u>	<u>8</u>
MessageIntegrityCode	128

- | | | |
|----|---------------|--|
| 1 | MessageID | The access network shall set this field to 0x01. |
| 2 | TransactionID | The access network shall set this field to the value of the TransactionID field of the KeyRequest message to which the access network is responding. |
| 3 | | |
| 4 | | |
| 5 | KeyIndex | The access network shall set this field to key index for which this key exchange is being initiated. Valid values for this field are '01' through '11'. The access network shall not set this field to KeyIndex public data. |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | Reserved | The access network shall set all the bits in this field to '0'. The access terminal shall ignore this field. |
| 10 | | |

1	PairwiseMasterKeyID	The access network shall set this field to EHMACHMAC-SHA256(key=PairwiseMasterKey, message="PairwiseMasterKeyID", MAC_length=8), where PairwiseMasterKey is a PairwiseMasterKey to be used, "PairwiseMasterKeyID" is the ASCII encoded value of the string, and the EHMACHMAC-SHA256 function is specified in 4.5.1.8.
2		
3		
4		
5		
6		
7		
8	ANNonce	The access network shall set this field to a 128-bit random number.
9		
10	NumProtocolSetIdentifiers	The access network shall set this field to the number of ProtocolSetIdentifiers supported by the access terminal. ProtocolSetIdentifiers supported by the access terminal are known to the access network through session information.
11		
12		
13		
14	ProtocolSetIdentifier	The access network shall set this field to the ProtocolSetIdentifier supported by the access terminal. The access network shall include the ProtocolSetIdentifier currently in use at the beginning. Protocol subtypes supported by the access terminal are known to the access network through session information.
15		
16		
17		
18		
19		
20	<u>MessageIntegritySubtypeCount</u>	<u>The access network shall set this field to the number of Subtypes of the Message Integrity Protocol supported by the access terminal.</u>
21		
22		
23		
24	<u>MessageIntegritySubtype</u>	<u>The access network shall set this field to the Subtype of the Message Integrity Protocol supported by the access terminal. The access network shall include Subtype of the Message Integrity Protocol currently in use at the beginning.</u>
25		
26		
27		
28	<u>CipheringSubtypeCount</u>	<u>The access network shall set this field to the number of Subtypes of the Ciphering Protocol supported by the access terminal.</u>
29		
30		
31	<u>CipheringSubtype</u>	<u>The access network shall set this field to the Subtype of the Ciphering Protocol supported by the access terminal. The access network shall include Subtype of the Ciphering Protocol currently in use at the beginning.</u>
32		
33		
34		
35	<u>KeyExchangeSubtypeCount</u>	<u>The access network shall set this field to the number of Subtypes of the Key Exchange Protocol supported by the access terminal.</u>
36		
37		

1 KeyExchangeSubtype The access network shall set this field to the Subtype of the
 2 Key Exchange Protocol supported by the access terminal. The
 3 access network shall include Subtype of the Key Exchange
 4 Protocol currently in use at the beginning.

5 MessageIntegrityCode The access network shall set this field to EHMAL-
 6 SHA256(key=MICKey, message=Message, MAC_length=16),
 7 where Message is set to all fields of this message with this
 8 field set to zero, and the EHMAL-SHA256 function is specified
 9 in 4.5.1.8.

Channels	FTC
Addressing	unicast

RLP	Reliable
AuthTag	Required when key is available

11 4.5.2.3 KeyComplete

12 The access terminal sends the KeyComplete message in response to the KeyResponse
 13 message.

Field	Length (bits)
MessageID	8
TransactionID	8
Result	8
MessageIntegrityCode	0 or 128

15 MessageID The access terminal shall set this field to 0x02.

16 TransactionID The access terminal shall set this field to the value of the
 17 TransactionID field of the corresponding KeyRequest message.

18 Result The access terminal shall set this field according to Table 4-1.

1

Table 4-2. Definition of Result field

Value	Meaning
0x00	Key exchange successful.
0x01	MessageIntegrityCode failed
0x02	MessageIntegrityCode successful, but <u>ProtocolSetIdentifiers</u> <u>SupportedSecuritySubtypes</u> verification failed.
0x03	PairwiseMasterKey not found.
0x04	MessageIntegrityCode successful, <u>SupportedSecuritySubtypes</u> <u>ProtocolSetIdentifier</u> s verification successful, but verification of <u>SupportedSecuritySubtypes</u> <u>ProtocolSetIdentifier</u> in use failed.
All other values	Reserved

2 MessageIntegrityCode If Result is 0x00, then the access terminal shall set this field
3 to EHMACH-SHA256(key=MICKey, message=*Message*,
4 MAC_length=16), where *Message* is set to all fields of this
5 message with this field set to zero, and the EHMACH-SHA256
6 function is specified in 4.5.1.8. Otherwise, the access terminal
7 shall omit this field.
8

Channels	RTC
Addressing	unicast

RLP	Reliable
AuthTag	Required when key is available

9 4.5.2.4 KeyReject

10 The access network may send the KeyReject message in response to the KeyRequest
11 message.
12

Field	Length (bits)
MessageID	8
TransactionID	8

13 MessageID The access network shall set this field to 0x03.

14 TransactionID The access network shall set this field to the value of the
15 TransactionID field of the KeyRequest message to which the
16 access network is responding.

1

Channels	FTC	RLP	Reliable
Addressing	unicast	AuthTag	Required when key is available

2 4.5.2.5 InitiateKeyRequest

3 The access network may send the InitiateKeyRequest message to request the access
4 terminal to send a KeyRequest message.

5

Field	Length (bits)
MessageID	8

6 MessageID The access network shall set this field to 0x04.

7

Channels	FTC	RLP	Reliable
Addressing	unicast	AuthTag	Required when key is available

8 4.5.2.6 ATSupportedSecuritySubtypesRequest

9 The access network may send the ATSupportedSecuritySubtypesRequest message to
10 request the access terminal to send a ATSupportedSecuritySubtypesResponse message.

11

<u>Field</u>	<u>Length (bits)</u>
<u>MessageID</u>	<u>8</u>

12 MessageID The access network shall set this field to 0x05.

13

<u>Channels</u>	<u>FTC</u>	<u>RLP</u>	<u>Reliable</u>
<u>Addressing</u>	<u>unicast</u>	<u>AuthTag</u>	<u>Required when key is available</u>

14 4.5.2.7 ATSupportedSecuritySubtypesResponse

15 The access terminal sends the ATSupportedSecuritySubtypesResponse message in
16 response to the ATSupportedSecuritySubtypesRequest message.

17

<u>Field</u>	<u>Length (bits)</u>
<u>MessageID</u>	<u>8</u>
<u>MessageIntegritySubtypeCount</u>	<u>8</u>
<u>MessageIntegritySubtypeCount occurrences of the following field:</u>	
<u>MessageIntegritySubtype</u>	<u>8</u>
<u>CipheringSubtypeCount</u>	<u>8</u>
<u>CipheringSubtypeCount occurrences of the following field:</u>	
<u>CipheringSubtype</u>	<u>8</u>
<u>KeyExchangeSubtypeCount</u>	<u>8</u>
<u>KeyExchangeSubtypeCount occurrences of the following field:</u>	
<u>KeyExchangeSubtype</u>	<u>8</u>

1	<u>MessageID</u>	The access terminal shall set this field to 0x06.
2	<u>MessageIntegritySubtypeCount</u>	
3		<u>The access terminal shall set this field to the number of</u>
4		<u>Subtypes of the Message Integrity Protocol supported by the</u>
5		<u>access terminal.</u>
6	<u>MessageIntegritySubtype</u>	The access terminal shall set this field to the Subtype of the
7		Message Integrity Protocol supported by the access terminal.
8	<u>CipheringSubtypeCount</u>	The access terminal shall set this field to the number of
9		Subtypes of the Ciphering Protocol supported by the access
10		terminal.
11	<u>CipheringSubtype</u>	The access terminal shall set this field to the Subtype of the
12		Ciphering Protocol supported by the access terminal.
13	<u>KeyExchangeSubtypeCount</u>	The access terminal shall set this field to the number of
14		Subtypes of the Key Exchange Protocol supported by the
15		access terminal.
16	<u>KeyExchangeSubtype</u>	The access terminal shall set this field to the Subtype of the
17		Key Exchange Protocol supported by the access terminal.
18		

<u>Channels</u>	<u>RTC</u>
<u>Addressing</u>	<u>unicast</u>

<u>RLP</u>	<u>Reliable</u>
<u>AuthTag</u>	<u>Required when key is available</u>

1 4.5.3 Interface to Other Protocols

2 4.5.3.1 Commands

3 This protocol does not issue any commands.

4 4.5.3.2 Indications

5 This protocol does not register to receive any indications.

6 **4.6 Configuration Attributes**

7 The following attributes and default values are defined (see [1] for attribute record
8 definition).

9 4.6.1 Simple Attributes

10 This protocol does not define any simple attributes.

11 4.6.2 Complex Attributes

12 4.6.2.1 ATSupportedSecuritySubtypes Attribute

13 The sender shall set AttributeID field to 0x8000.

14

<u>Field</u>	<u>Length (bits)</u>	<u>Default Value</u>
<u>MessageIntegritySubtypeCount</u>	<u>8</u>	<u>0x00</u>
<u>MessageIntegritySubtypeCount occurrences of the following field:</u>		
<u>MessageIntegritySubtype</u>	<u>8</u>	<u>N/A</u>
<u>CipheringSubtypeCount</u>	<u>8</u>	<u>0x00</u>
<u>CipheringSubtypeCount occurrences of the following field:</u>		
<u>CipheringSubtype</u>	<u>8</u>	<u>N/A</u>
<u>KeyExchangeSubtypeCount</u>	<u>8</u>	<u>0x00</u>
<u>KeyExchangeSubtypeCount occurrences of the following field:</u>		
<u>KeyExchangeSubtype</u>	<u>8</u>	<u>N/A</u>

15 MessageIntegritySubtypeCount

16 The access terminal shall set this field to the number of

1		<u>Subtypes of the Message Integrity Protocol supported by the</u>
2		<u>access terminal.</u>
3	<u>MessageIntegritySubtype</u>	<u>The access terminal shall set this field to the Subtype of the</u>
4		<u>Message Integrity Protocol supported by the access terminal.</u>
5	<u>CipheringSubtypeCount</u>	<u>The access terminal shall set this field to the number of</u>
6		<u>Subtypes of the Ciphering Protocol supported by the access</u>
7		<u>terminal.</u>
8	<u>CipheringSubtype</u>	<u>The access terminal shall set this field to the Subtype of the</u>
9		<u>Ciphering Protocol supported by the access terminal.</u>
10	<u>KeyExchangeSubtypeCount</u>	<u>The access terminal shall set this field to the number of</u>
11		<u>Subtypes of the Key Exchange Protocol supported by the</u>
12		<u>access terminal.</u>
13	<u>KeyExchangeSubtype</u>	<u>The access terminal shall set this field to the Subtype of the</u>
14		<u>Key Exchange Protocol supported by the access terminal.</u>
15		

<u>Commit</u>	<u>Soft</u>
---------------	-------------

<u>Scope</u>	<u>Static</u>
--------------	---------------

16 4.7 Non-Attribute Data

17 This protocol does not define any non-attribute data.

18 4.8 Protocol Numeric Constants

19 **Table 4-3. Protocol Numeric Constants**

Constant	Meaning	Value
$N_{KEPType}$	Type field for this protocol	[1]
N_{BKEP}	Subtype field for this protocol	0x00
$N_{BKEPSTKeyLen}$	Length of Temporary Security Key in units of bits	256

20 4.9 Session State Information

21 The Session State Information record (see [1]) consists of parameter records.

22 All configuration attributes and Non-attribute data are Session State Information records.
 23 This protocol defines the following parameter record in addition to the configuration
 24 attributes for this protocol.

25 4.9.1 PMK-DerivedMSK Parameter

26 The sender shall set DataID field to 0x0000.

1 **Table 4-4. The Format of the Parameter Record for the DerivedMSK PMK Parameter**

Field	Length (bits)
<u>ValidPMKExistsValidMSKExists</u> <u>s</u>	1
Reserved	7
<u>PMKCountDerivedMSKCount</u>	8

DerivedMSKCountPMKCount occurrences of the following five fields:

<u>DerivedMSKPMKLength</u>	8
<u>DerivedMSKPMK</u>	<u>DerivedMSKPMKLength</u> h × 8
<u>DerivedMSKExpiryTime</u>	<u>32</u>
<u>PMKGenerationTime</u>	<u>24</u>
<u>PMKMinLifeTime</u>	<u>24</u>
<u>PMKMaxLifeTime</u>	<u>24</u>

2 ValidPMKExistsValidMSKExists If a valid PMK-MSK exists, then this field shall be set to
3 '1'; otherwise, this field shall be set to '0'.

4 Reserved All the bits in this field shall be set to '0'.

5 DerivedMSKPMKCount This field shall be set to the number of occurrences of the
6 DerivedMSKPMK field in this parameter record.

7 DerivedMSKPMKLength This field shall be set to the length of the DerivedMSKPMK
8 field in units of octets.

9 DerivedMSKPMK This field shall be set to a Derived
10 MasterSessionKeyPairwiseMasterKey.

11 DerivedMSKExpiryTime This field shall be set to 32 MSBs of time at which the Derived
12 MasterSessionKey will expire, specified in the NTP timestamp
13 format (see [18]).

14 PMKGenerationTime This field shall be set to $X \text{ mod } 2^{24}$; where X is the time, in
15 units of seconds, at which the PairwiseMasterKey was
16 generated.

17 PMKMinLifeTime This field shall be set to minimum lifetime of the
18 PairwiseMasterKey in units of seconds.

19 PMKMaxLifeTime This field shall be set to maximum lifetime of the
20 PairwiseMasterKey in units of seconds.

- 1 No text.