| | |
|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>** |
| Title | **Amendment to Security Primitives in Section 14.2.2.1, 14.2.2.2** |
| Date Submitted | **2007-03-08** |
| Source(s) | Jung-Mo Moon, JeeHyeon Na, Mi-Young Yun, and Sangho Lee jhna@etri.re.kr<br><br>ETRI<br><br>161 Gajeong-dong, Yuseong-gu Daejeon 305-700 Korea |
| Re: | Contribution on comments to IEEE 802.16g/D8 |
| Abstract | Re-definition of EAP primitives in section 14.2.2.1 |
| Purpose | Adoption |
| Notice | This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor grants a free, irrevocable license to the IEEE to incorporate text contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16. |
| Patent Policy and Procedures | The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing the standard."<br><br>Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:r.b.marks@ieee.org> as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>. |

# Amendment to EAP Security Primitives

*Jung Mo Moon, JeeHyeon Na, Mi Young Yun, and Sangho Lee*

*ETRI*

## 1. Motivation

IEEE 802.16g Network reference model defines a NCMS and an 802.16 entity in each side. However Section 14.2.2.1 only describes security primitives on an BS side. Therefore security primitives on an MS side are also needed for consistency.

This contribution adds security primitives on an MS side and changes some texts which are related to them.

We propose to modify section 14.2.2.1 as follows.

1. add a figure to illustrate security primitives on MS side.
2. change each subsection to clarify and describes on each side (SS(MS) and BS side)

## 2. Proposed Text Changes

[*Modify Subclause 14.2.2.1 as follows*]

When an ~~SS~~ MS tries to initiate an EAP-based authentication or re-authentication procedure with a BS, NCMS(MS) sends C-SM_IND/EAP_Start primitive to 802.16 Entity(MS) and MS ~~it~~ sends a PKMv2 EAP_Start message. The 802.16 Entity(BS)~~BS~~ informs the AAA Services entity in NCMS (i.e. the authenticator) by sending the C-SM-IND/EAP_Start primitive.

Figure XXX and 473 shows EAP-based authentication procedure between a ~~BS~~ 802.16 entity and a NCMS on MS and BS sides ~~and an AAA Services entity in NCMS~~ as follows:

[*Insert the figure XXX to the following figure Section 142.2.1*]

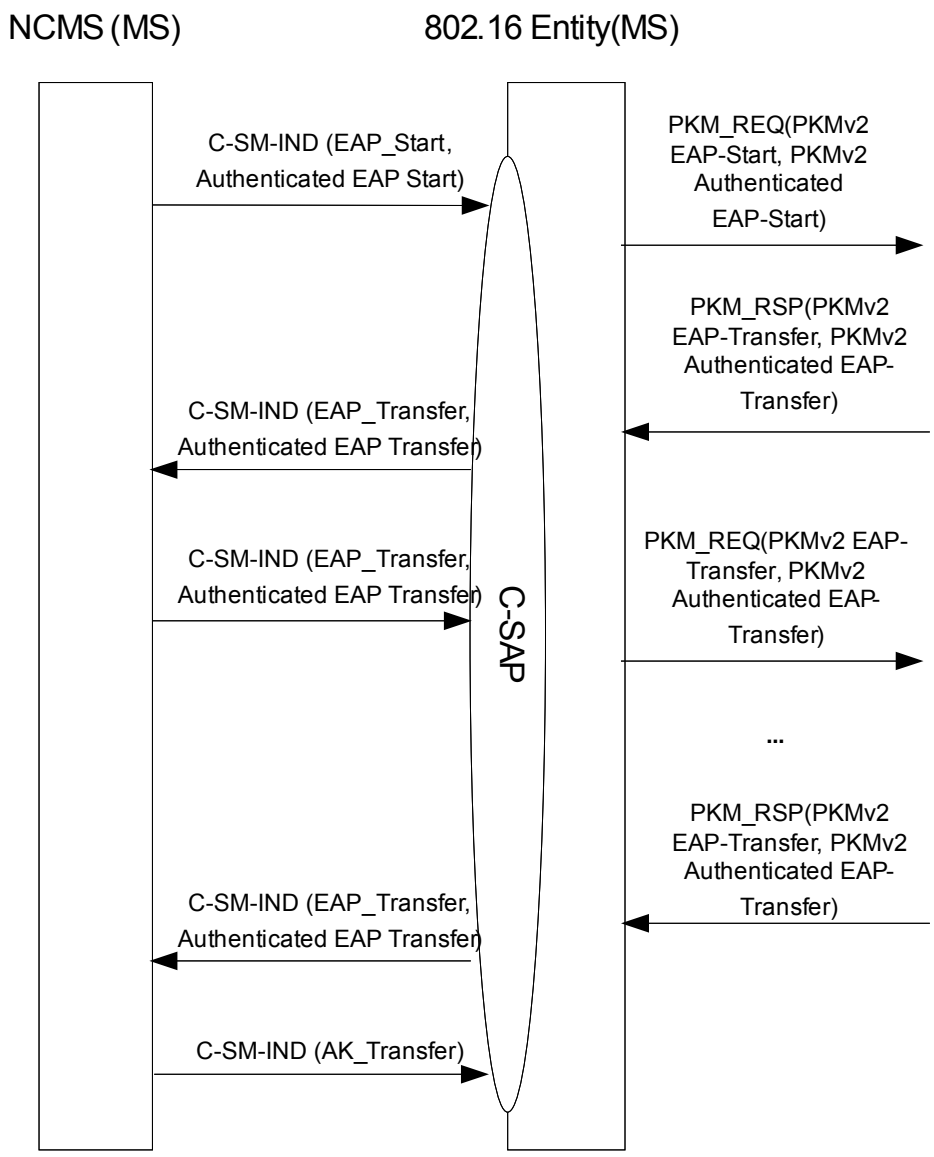


Figure XXX – EAP based Authentication Procedure on MS side

Figure 473 – EAP based Authentication Procedure on BS side

[*Modify Subclause 14.2.2.1.1.1 as follows* ]

#### 14.2.4.2.1 C-SM-IND (Event_Type = EAP_Start)

### Function

This primitive informs ~~the authenticator in the NCMS~~a 802.16 entity(MS) or a NCMS(BS) that an SS is going to start an EAP-based authentication. The PKMv2 EAP_Start is sent by the SS to initiate either an initial EAP authentication or EAP re-authentication exchange.

### Semantics of the service primitives

The parameters of the primitives are as follows:

**C-SM-IND**

(

Destination: NCMS, MS

)

### When generated

This primitive is issued by a ~~BS~~ NCMS(MS) or a 802.16 entity(BS) when a SS wants to initiate EAP-based authentication procedure.

### Effect of receipt

EAP payloads are forwarded for the authentication between the ~~BS~~ 802.16 entity and the ~~AAA~~ NCMS entity ~~(authenticator).~~

[*Modify Subclause 14.2.2.1.1.2 as follows* ]

#### 14.2.2.1.1.2 C-SM-IND (Event_Type = Authenticated EAP_Start)

### Function

This primitive informs a 802.16 entity(MS) or a NCMS(BS) ~~the authenticator in the NCMS~~ that an SS is starting a second round of EAP during double EAP authentication and authorization.

### Semantics of the service primitives

The parameters of this primitive are as follows:

**C-SM-IND**

(

Destination: NCMS, MS

)

### When generated

The NCMS(MS) shall send a notification message with this event type to the 802.16 entity(MS) whenever an SS is starting a second round of EAP during double EAP authentication and authorization.. The 802.16 entity(BS) ~~BS~~ shall send a notification message with this event type to the ~~NCMS~~ the NCMS(BS) whenever it received from the the 802.16 entity(BS) MS a PKMv2 Authenticated EAP_Start message, equipped with a valid "HMAC digest/CMAC digest" attribute value.

### Effect of receipt

Reception of an Authenticated_EAP_Start primitive from the 802.16 entity(BS)~~BS~~ informs the NCMS(BS) of the ~~MS~~ MS having initiated second round EAP by means of a PKMv2 Authenticated EAP_Start message with a valid "HMAC digest/CMAC digest" attribute value. This triggers the NCMS to send Authenticated EAP_Transfer primitives to the the 802.16 entity~~BS~~ carrying EAP payloads for second round EAP

#### 14.2.2.1.1.3 C-SM-IND (Event_Type = AK Transfer)

### Function

A ~~SS~~ NCMS derives the key from the EAP payloads, yield PMK from the MSK, then yield AK from the PMK, and ~~the NCMS entity~~ informs the 802.16 entities~~BS~~ of ~~it~~ the AK when the EAP exchanges are successfully completed by the AAA service entities, ~~and yield PMK from the MSK, then yield AK from the PMK~~.

### Semantics of the service primitives

The parameters of the primitives are as follows:

**C-SM-IND**

(

Event_Type: AK_Transfer,

Destination: BS, MS

Attribute_List:

MS MAC Address,

AK,

AK Lifetime,

AK Sequence Number,

AKID

)

### When generated

This primitive is issued by the NCMS (the AAA Services entity, i.e. Authenticator) when the EAP exchange finishes.

### Effect of receipt

The 802.16 entities ~~BS~~ could derive other AK context (HMAC/CMAC_KEY_U, HMAC/CMAC_KEY_D, HMAC/CMAC_PN_U, HMAC/CMAC_PN_D, KEK).

#### 14.2.2.1.1.4 C-SM-IND (Event_Type = EAP_Transfer)

### Function

After the C-SM-IND/EAP_Start primitive, EAP payloads are exchanged between 802.16 entities~~an SS and NCMS~~. The EAP payloads are encapsulated in the C-SM-IND/EAP_Transfer because it is not interpreted in the MAC. C-SM-IND/EAP_Transfer is used between the NCMS and the 802.16 entity~~BS~~.

### Semantics of the service primitives

The parameters of the primitives are as follows:

**C-SM-IND**

(

Destination: MS, BS or NCMS,

)

### When generated

This primitive can be issued by an 802.16 entity ~~BS~~ in EAP procedure to transfer EAP Message included in PKMv2 PKM-REQ message. This primitive can also be issued by a NCMS in EAP procedure to transfer EAP Message to an 802.16 entity~~BS~~.

### Effect of receipt

When received by NCMS, the NCMS could derive PMK and optional EIK from the MSK , then AK context from PMK after a successful authentication procedure.

When received by an 802.16 entity~~BS~~, ~~the BS~~it forwards EAP payload to ~~SS~~ peer in PKM-REQ or PKM-RSP message.

#### 14.2.2.1.1.5 C-SM-IND (Event_Type = Authenticated EAP_Transfer)

### Function

After the C-SM-IND/Authenticated_EAP_Start primitive, EAP payloads are exchanged between an 802.16 entity~~SS~~ and NCMS. The EAP payloads are encapsulated in C-SM-IND/Authenticated_EAP_Transfer because they are not interpreted in the MAC and because they are exchanged during second round EAP in double EAP authentication and authorization. C-SM-IND/Authenticated_EAP_Transfer is used between an NCMS and an 802.16 entity~~BS~~.

### Semantics of the service primitives

The parameters of this primitive are as follows:

**C-SM-IND**

(

Destination: MS, BS~~ID~~ or NCMS,

)

### When generated

The NCMS shall a notification message with this event type to an 802.16 entity after successful initial authentication procedure. The an 802.16 entity(BS) shall send a notification message with this event type to the NCMS(BS) whenever it received from the MS a PKMv2 Authenticated EAP_Transfer message, equipped with a valid "HMAC digest/CMAC digest" attribute value. This way, the an 802.16 entity(BS) shall relay the EAP payload contained in the PKMv2 Authenticated EAP_Transfer message to the NCMS(BS).

~~The NCMS shall send a notification message with this event type to the BS in order to response to an Authenticated_EAP_Transfer primitive received from the BS.~~

**Effect of receipt**

When received by an 802.16 entity~~BS~~: When the 802.16 entity ~~BS~~ receives a Authenticated_EAP_Transfer primitive from NCMS, it generates a PKMv2 Authenticated EAP_Transfer message carrying the EAP contained in the primitive to the ~~MS~~peer.

When received by NCMS: When the NCMS receives an Authenticated_EAP_Transfer primitive, it generates either a response primitive of the same type and sends it to the an 802.16 entity~~BS~~, or - after successful completion of the second EAP round - derives PMK2 from MSK2, then AK from PKM and PMK2, and an AK context.