

Project	<b>IEEE 802.16 Broadband Wireless Access Working Group</b> < <a href="http://ieee802.org/16">http://ieee802.org/16</a> >
Title	<b>Amendment to EAP Security Primitives in 14.2.2.1</b>
Date Submitted	<b>2007-03-1508</b>
Source(s)	Jung-Mo Moon, Jee_Hyeon Na, Mi-Young Yun, and Sangho Lee <a href="mailto:jhna@etri.re.kr">jhna@etri.re.kr</a> ETRI 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 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) < <a href="http://ieee802.org/16/ipr/patents/policy.html">http://ieee802.org/16/ipr/patents/policy.html</a> >, 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."  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 < <a href="mailto:r.b.marks@ieee.org">mailto:r.b.marks@ieee.org</a> > 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 < <a href="http://ieee802.org/16/ipr/patents/notices">http://ieee802.org/16/ipr/patents/notices</a> >.

# Amendment to EAP Security Primitives in 14.2.2.1

*Jung\_Mo Moon, Jee\_Hyeon Na, Mi\_Young Yun, and Sangho Lee*

*ETRI*

## 1. Motivation

IEEE 802.16g Network reference model defines an NCMS and an 802.16 entity on an SS and a BS side. However, section 14.2.2.1 only describes EAP-based authentication procedures on a BS side. Therefore, EAP-based security primitives on an SS side are also needed for consistency. They shall be used as an interface between an EAP authentication application and an 802.16 entity(SS).

This contribution adds EAP-based security primitives on an [SMS](#) side and changes some texts which are related to them.

We propose to modify section 14.2.2.1 as follows.

1. Modification of figure 473 to illustrate EAP-based security primitives on SS side.
2. Modification of each subsection to clarify and describe on each side (SS and BS side)

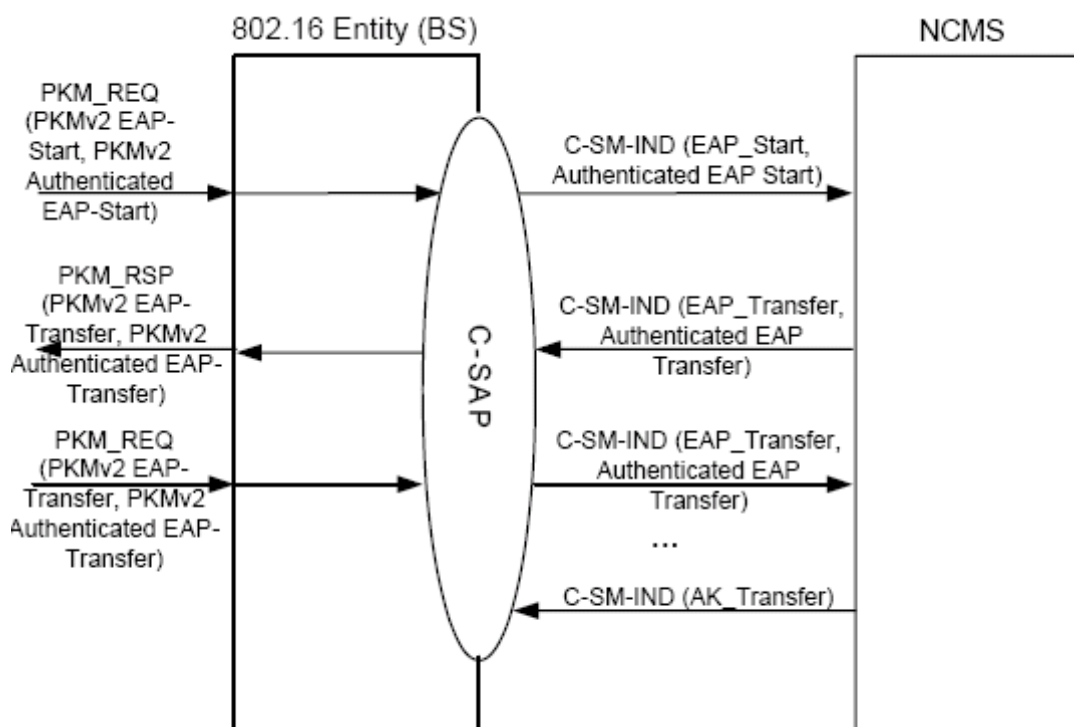
## 2. Proposed Text Changes

[*Modify Subclause 14.2.2.1 as follows* ]

### 14.2.2.1 EAP-based authentication procedure

When an SS tries to initiate an EAP-based authentication or re-authentication procedure with a BS, an NCMS(SS) sends C-SM\_IND/EAP\_Start primitive to the 802.16 entity(SS) and the 802.16 entity(SS) it sends a PKMv2 EAP\_Start message. The BS informs the AAA Services entity in NCMS (i.e. the authenticator) by sending the C-SM\_IND/EAP\_Start primitive. If the SS receives EAP-Request/Identity messages, then it sends the EAP-Response/Identity message with SS MAC Address to the AAA Services entity. After the EAP-Response/Identity message, the EAP methods are negotiated between the SS and the AAA server and the EAP messages are exchanged several times. The EAP encapsulated messages are exchanged between the SS and the AAA Services entity. If the EAP authentication procedure is finished successfully and also yields an MSK (Master Session Key), the BS which does not know EAP protocols receives the AK and a key lifetime from the authenticator, which is part of the AAA Services entity, in the C-SM\_IND/AK\_Transfer primitive. The MSK is already shared between the AAA server and the SS through the EAP exchanges. The MSK is used by the SS and authenticator for derivation of the PMK (Pairwise Master Key) and optional EIK (EAP Integrity Key).

Figure 473 shows EAP-based authentication procedures between an BS-802.16 entity and an NCMS on SS and BS sides and an AAA Services entity in NCMS as follows:



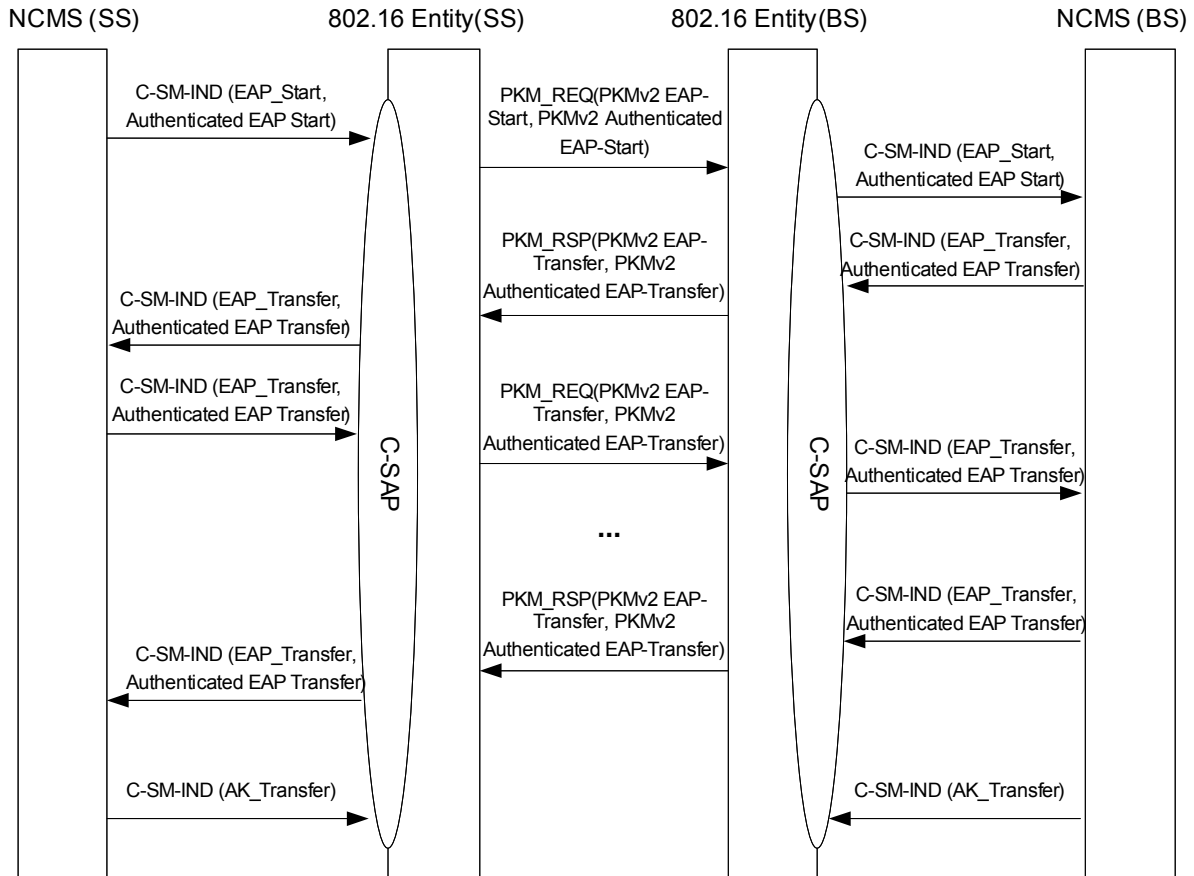


Figure 473 – EAP based Authentication Procedure

14.2.2.1.1 C-SM-IND

This primitive is used by an 802.16 entity or NCMS to notify security procedures. The Event\_Type included in this primitive defines the type of security operation in Authentication and Re-authentication procedure to be performed. The possible Event\_Types for this primitive are listed in the following table:

Table 450—C-SM-IND Event\_Types

Event_Type	Description
EAP_Start	EAP Start
Authenticated EAP_Start	Authenticated EAP Start
AK Transfer	AK Transfer notification
EAP_Transfer	Transfer EAP Payload
Authenticated EAP_Transfer	Authenticated EAP Transfer

[Modify Subclause 14.2.1.1.1 as follows ]

#### 14.2.2.1.1.1 C-SM-IND (Event\_Type = EAP\_Start)

##### Function

This primitive informs ~~the authenticator in the NCMS~~ an 802.16 entity(SS) or an 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

```
(
  Event_Type: EAP_Start,
  Destination: NCMS, MSS,
  Attribute_List:
    SMS MAC Address,
    BSID
)
```

###### SMS MAC Address

48-bit unique identifier used for user identification between BS and NCMS

###### **BSID**

48-bit unique identifier used for BS

##### When generated

- NCMS(SS) -> 802.16 Entity(SS) :  
This primitive is issued by an NCMS (SS) when an SS wants to initiate EAP-based authentication procedure.
- 802.16 entity(BS) -> NCMS(BS) :  
This primitive is issued by an 802.16 entity(BS) in EAP procedure when an 802.16 Entity(BS) receives a PKM-REQ message with PKMv2 EAP\_Start.

##### Effect of receipt

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

- NCMS(SS) -> 802.16 Entity(SS) :  
When received by the 802.16 Entity(SS), the 802.16 Entity(SS) forwards a PKM-REQ message with PKMv2 EAP\_Start.
- 802.16 entity(BS) -> NCMS(BS) :  
When received by the NCMS(BS), the NCMS(BS) requests an AAA Authenticator to initiate an EAP-based authentication.

[*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 an 802.16 entity(SS) or an 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**

(  
 Event\_Type: Authenticated\_EAP\_Start,  
 Destination: NCMS, SMS,  
 Attribute\_List:  
     MS-SS MAC Address,  
     BSID  
 )

**SMS MAC Address**

48-bit unique identifier used for user identification between BS and NCMS

**BSID**

48-bit unique identifier used for BS

**When generated**

~~The BS shall send a notification message with this event type to the NCMS whenever it received from the MS a PKMv2 Authenticated EAP\_Start message, equipped with a valid "HMAC digest/CMAC digest" attribute value.~~

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

**Effect of receipt**

~~BS informs the NCMS of the 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 BS carrying EAP payloads for second round EAP~~

- NCMS(SS) -> 802.16 entity (SS):  
When the 802.16 entity(SS) receives Authenticated\_EAP\_Start primitive from NCMS(SS), the 802.16 entity(SS) shall transfer a **PKM\_REQ message with** PKMv2 Authenticated EAP-Start to the 802.16 entity(BS).
- 802.16 entity(BS) -> NCMS(BS):  
When the NCMS(BS) receives an Authenticated\_EAP\_Start primitive from the 802.16 entity(BS), the NCMS(BS) shall inform an **AAA authenticator** of the MS having initiated second round EAP. This triggers the NCMS(BS) to send Authenticated EAP\_Transfer primitives to the 802.16 entity(BS) carrying EAP payloads for second round EAP

[*Modify Subclause 14.2.2.1.1.3 as follows* ]

**14.2.2.1.1.3 C-SM-IND (Event\_Type = AK Transfer)****Function**

~~An SS-NCMS derives the key from the EAP payloads, yields PMK from the MSK, then yields AK from the PMK, and the NCMS entity informs the 802.16 entity 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, SMS,
  Attribute_List:
    SMS MAC Address,
    AK,
    AK Lifetime,
    AK Sequence Number,
    AKID
)
```

### SMS MAC Address

48-bit unique identifier used for user identification between BS and NCMS

### AK

AK is the product of PMK after successful EAP exchanges. It is used for protecting air interface messages and KEK.

### AK Lifetime

AK Lifetime shall be set in accordance with PMK and MSK Lifetime. PMK and MSK Lifetime shall be transferred from the EAP method and could also be configured by the AAA Services.

### AK Sequence Number

AK Sequence Number shall be derived from PMK Sequence Number.

### AKID

It should be derived according to subclause 7.2.2.4.1 of the IEEE 802.16e-2005 specification

## When generated

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

- NCMS(SS) -> 802.16 entity(SS) :  
This primitive is issued by the NCMS (SS) when the EAP procedure is finished.
- NCMS(BS) -> 802.16 entity(BS) :  
This primitive is issued by the NCMS(BS) (the AAA Services entity, i.e. Authenticator) when the EAP procedure is finished.

## Effect of receipt

~~The BS could derive other AK context (HMAC/CMAC\_KEY\_U, HMAC/CMAC\_KEY\_D, HMAC/CMAC\_PN\_U, HMAC/CMAC\_PN\_D, KEK):~~

- NCMS(SS) -> 802.16 entity(SS) :  
The 802.16 entity(SS) could derive other AK context (HMAC/CMAC\_KEY\_U, HMAC/CMAC\_KEY\_D, HMAC/CMAC\_PN\_U, HMAC/CMAC\_PN\_D, KEK).
- NCMS(BS) -> 802.16 entity(BS) :  
The 802.16 entity(BS) could derive other AK context (HMAC/CMAC\_KEY\_U, HMAC/CMAC\_KEY\_D, HMAC/CMAC\_PN\_U, HMAC/CMAC\_PN\_D, KEK).

[Modify Subclause 14.2.2.1.1.4 as follows ]

### 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 an SS and an AAA server ~~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

```
(
  Event_Type: EAP TRANSFER,
  Destination: SMS_BS or NCMS,
  Attribute_list:
    SS MAC Address,
    EAP Payload
)
```

### SMS MAC Address

48-bit unique identifier used for user identification between BS and NCMS.

### EAP Payload

~~Contains~~ The EAP authentication data.

## When generated

~~This primitive can be issued by a 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 BS.~~

- NCMS(SS) -> 802.16 entity(SS) :  
This primitive can be issued by a NCMS(SS) in an EAP procedure to transfer an EAP Message to an 802.16 entity.
- 802.16 entity(BS) -> NCMS(BS) :  
This primitive can be issued by 802.16 entity(BS) in an EAP procedure to transfer an EAP Message included in PKMv2 PKM-REQ message.
- NCMS(BS) -> 802.16 entity(BS) :  
This primitive can be issued by a NCMS(BS) in EAP procedure to transfer an EAP Message to an 802.16 entity(SS).
- 802.16 entity(BS) -> NCMS(BS) :  
This primitive can be issued by 802.16 entity(BSS) in EAP procedure to transfer an EAP Message included in PKMv2 PKM-REQ message.

## 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 BS, the BS forwards EAP payload to SS in PKM-RSP message.~~

- NCMS(SS) -> 802.16 entity(SS) :  
When received by an 802.16 entity(SS), the BSS forwards EAP payload to the other in a PKM-REQ message
- 802.16 entity(BS) -> NCMS(BS) :  
When received by NCMS(BS), the NCMS(BS) generates a next EAP payload or can derive PMK and optional EIK from the MSK , then AK context from PMK after a successful authentication procedure.
- NCMS(BS) -> 802.16 entity(BS) :  
When received by an 802.16 entity(BS), the BS forwards EAP payload to the other in an PKM-RSP message.
- 802.16 entity(SS) -> NCMS(SS) :  
When received by NCMS(SS), the NCMS(SS) generates a next EAP payload or can derive PMK and optional EIK from the MSK , then AK context from PMK after a successful authentication procedure.



[*Modify Subclause 14.2.2.1.1.5 as follows* ]

#### 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 [SMS and an AAA server 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 [the NCMS and the 802.16 entity BS](#).

##### Semantics of the service primitives

The parameters of this primitive are as follows:

###### C-SM-IND

```
(
  Event_Type: Authenticated_EAP_Transfer,
  Destination: SMS\_BS or NCMS,
  Attribute list:
    SMS MAC Address,
    EAP Payload
)
```

###### [SMS MAC Address](#)

48-bit unique identifier used for user identification between BS and NCMS, may be [SMS MAC Address](#)

###### EAP Payload

~~Contains~~ The EAP authentication data.

##### When generated

~~The BS shall send a notification message with this event type to the NCMS 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 BS shall relay the EAP payload contained in the PKMv2 Authenticated EAP\_Transfer message to the NCMS. 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.~~

- [NCMS\(SS\) -> 802.16 entity\(SS\) :](#)  
~~This primitive can be issued by a NCMS(SS) to transfer an EAP Message to an 802.16 entity(SS) after successful initial authentication procedure.~~
- [802.16 entity\(BS\) -> NCMS\(BS\) :](#)  
~~The 802.16 entity(BS) shall send an EAP message to the NCMS(BS) whenever it received from the MS a PKM-REQ with PKMv2 Authenticated EAP\_Transfer message, equipped with a valid "HMAC digest/CMAC digest" attribute value. This way, the 802.16 entity(BS) shall relay the EAP payload contained in the PKMv2 Authenticated EAP\_Transfer message to the NCMS(BS).~~
- [802.16 entity\(SS\) -> NCMS\(SS\) :](#)  
~~The 802.16 entity(SS) shall send an EAP message to the NCMS(SS) whenever it received from the BS a PKMv2 Authenticated EAP\_Transfer message, equipped with a valid "HMAC digest/CMAC digest" attribute value. This way, the 802.16 entity(SS) shall relay the EAP payload contained in the PKMv2 Authenticated EAP\_Transfer message to the NCMS(SS).~~
- [NCMS\(BS\) -> 802.16 entity\(BS\) :](#)  
~~An NCMS(BS) shall send an EAP message to an 802.16 entity(BS) after successful initial authentication procedure.~~

##### Effect of receipt

~~When received by BS: When the 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.~~

~~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 BS, or - after successful completion of the second EAP round - derives PMK2 from MSK2, then AK from PKM and PMK2, and an AK context.~~

- NCMS(SS) -> 802.16 entity(SS) :  
When received by an 802.16 entity(SS), the SS forwards EAP payload to the other in a PKM-REQ message with PKMv2 Authenticated EAP\_Transfer, equipped with a valid "HMAC digest/CMAC digest" attribute value
- 802.16 entity(BS) -> NCMS(BS) :  
When received by NCMS(BS), the NCMS(BS) generates a next EAP payload or can derive PMK and optional EIK from the MSK, then AK context from PMK after a successful authentication procedure.
- NCMS(BS) -> 802.16 entity(BS) :  
When received by an 802.16 entity(BS), the BS forwards EAP payload to the other in an PKM-RSP message with PKMv2 Authenticated EAP\_Transfer, equipped with a valid "HMAC digest/CMAC digest" attribute value
- 802.16 entity(SS) -> NCMS(SS) :  
When received by NCMS(SS), the NCMS(SS) generates a next EAP payload or can derive PMK and optional EIK from the MSK, then AK context from PMK after a successful authentication procedure.