Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Cleanup for security section**	
Date Submitted	**2006-01-11~~05~~**	
Source(s)	Changhong Shan Huawei Num 98, Long 91, Road Eshan, Pudong, Shanghai, China 200127	Voice: +86-21-68644808ext23277 Fax: mailto:ritatv@huawei.com
Re:	Section 14.5.5 Security Management, IEEE802.16g-05/008r2	
Abstract	In security section of current 802.16g-05/008r2 baseline document, there are some ambiguous or unreasonable description and definition. We do some modification in order to make it clear.	
Purpose	The purpose of this contribution is to describe a universal naming schema for ~~NSP List TLV and NSP Count TLV~~section 14.5.5 defined in 802.16g baseline document and modify some unreasonable primitives or messages.	
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 material 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 <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of 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 <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

1 Problem Statement

First, we describe security primitive or message with universal naming schema. SM is the abbreviation of Security Management.

Secondly, we change the C-SM-NOTFY/EAP_Key into C-SM-NOTFY/AK_Transfer, for it is not appropriate to transfer MSK to BS from NAS in NCMS. MSK shall be transferred to NAS from Authentication Server (such as AAA Server), then NAS will yield AK and part of its context and send them to BS.

Thirdly, BS shall tell NAS of Authorization Policy Support (Single EAP or EAP after EAP, etc..) which is negotiated in SBC-REQ/RSP procedure. So we add Authorization Policy Support attribute into C-SM-REQ/EAP_Start.

2 Proposed Text

[Change section 14.5.5 as follows]

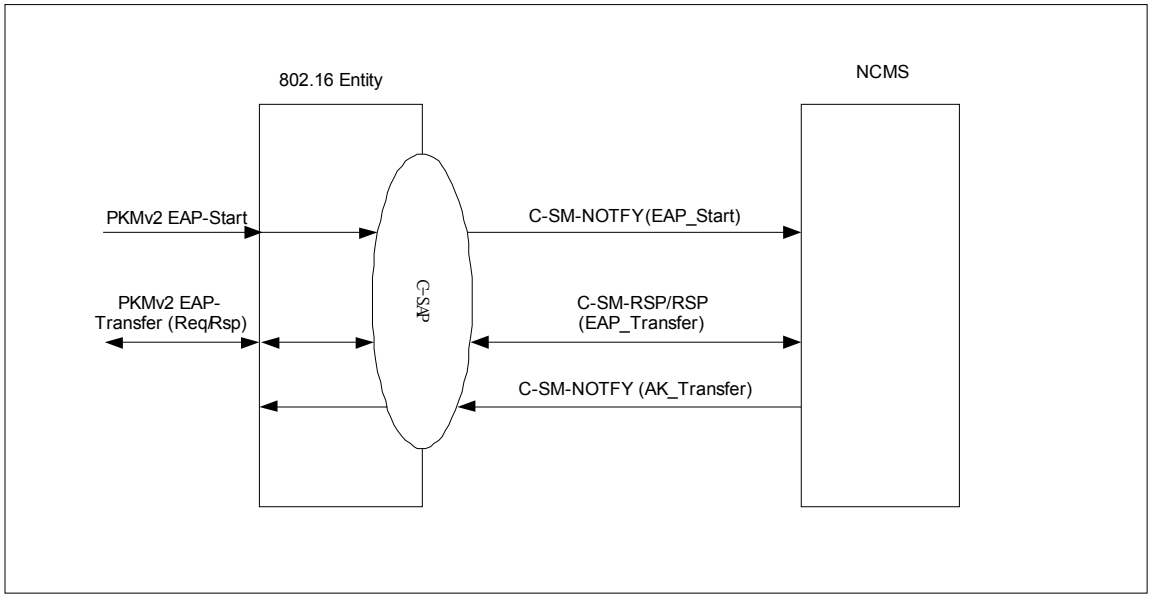
14.5.5 Security Management

14.5.5.1 EAP-based authentication procedure

When an MS try to initiate an EAP-based authentication or re-authentication procedure with a BS, it sends a PKMv2 EAP Start message. The BS informs of an NAS (Network Access Server) entity in NCMS as an C-SM-REQ/EAP_Start~~EAP_start.request~~ primitive. If the MS receives EAP-Request/Identity messages, then it sends the EAP-Response/Identity message with MN's identifier to the NAS entity. After the EAP-Response/Identity message, the EAP methods are negotiated between the MS and the AAA server and the EAP messages are exchanged several times. The EAP messages encapsulated are exchanged between the MS and the NAS 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 MSK and a key lifetime from the EAP client entity as an C-SM-NOTFY/EAP_Key~~EAP_Key_Notification.indication~~ primitive. It is already shared between the AAA

server and the MS through the EAP exchanges. The MSK is used for derivation for a PMK (Pair wise Master Key) and optional EIK (EAP Integrity Key).

Figure 311 shows EAP-based authentication procedure between a BS and an NAS entity in NCMS as follows



~~NCMS~~

Figure 311 EAP based Authentication Procedure

14.5.5.1.1 Service Primitives

14.5.5.1.1.1 C-SM-NOTFY

This primitive (or message) is used by an 802.16 entity 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 Operation Types for this primitive are listed in Table xxx

Event Type	Description
EAP_Start	EAP Start
AK_Transfer	AK transfer notification

14.5.5.1.1.1.1 Function

14.5.5.1.1.1.1.1 EAP_Start

This primitive inform an AAA Client entity in NCMS that an MS is going to start EAP-based authentication.

14.5.5.1.1.1.1.2 AK Transfer

A MS derives the key from the EAP payloads and the NCMS entity informs the BS of it when the EAP exchanges are successfully completed in NAS and yield PMK from MSK, then yield AK from PMK.

14.5.5.1.1.1.2 Semantics of the Service Primitives

14.5.5.1.1.1.2.1 EAP_Start

The parameters of the primitives are as follows:

C-SM-REQ
(
Operation Type : Action,
Action Type : EAP_Start,
Object ID : NCMS,
Attribute List :
MS ID
Authorization Policy Support,
)

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

Authorization Policy Support
Authorization policy negotiated by MSS and BS in SBC-REQ/RSP procedure

14.5.5.1.1.1.2.2 AK Transfer

The parameters of the primitives are as follows:
C-SM-NOTFY
(
Operation Type : Action,
Action Type : AK_Transfer,
Object ID : BS,
Attribute List :
MS ID
AK
AK Lifetime
AK Sequence Number
AKID,
)
MS ID
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 accordance with PMK and MSK Lifetime. PMK and MSK Lifetime shall be transferred from the EAP method or be set by a vendor in NAS.
AK Sequence Number
AK Lifetime shall be derived from PMK Sequence Number.
AKID
It should be derived according to IEEE802.16e specification.

14.5.5.1.1.1.3 When generated

14.5.5.1.1.1.3.1 EAP_Start
This primitive is issued by a BS when a MS wants to initiate EAP-based authentication procedure.

14.5.5.1.1.1.3.2 AK Transfer
This primitive is issued by a NCMS (a NAS entity) when the EAP exchange finishes.

14.5.5.1.1.1.4 Effect of receipt

14.5.5.1.1.1.4.1 EAP_Start

EAP payloads are forwarded for the authentication between BS and NCMS entity.

14.5.5.1.1.1.4.2 AK Transfer
The BS could derive other AK context (HMAC/CMAC_KEY_U, HMAC/CMAC_KEY_D, HMAC/CMAC_PN_U, HMAC/CMAC_PN_D, KEK).

14.5.5.1.1.~~2~~1 C-SM-REQ
This primitive (or message) is used by an 802.16 entity to trigger security procedure or request security information. The Operation Type included in this primitive defines the type of `security` operation in Authentication and Re-authentication procedure to be performed. The possible Operation Types for this primitive are listed in Table xxx.

Operation Type	Action Type	Description
~~Set~~	~~EAP_Start~~	~~EAP start request~~
~~Set~~Action	EAP_Transfer	EAP transfer request

~~**14.5.5.1.1.1 EAP_Start.request**~~

14.5.5.1.1.~~2~~1.1 Function

~~**14.5.5.1.1.1.1.1 EAP_Start**~~

~~This primitive inform an AAA Client entity in NCMS that an MS is going to start EAP-based authentication.~~

14.5.5.1.1.~~2~~1.1.~~1~~2 EAP_Transfer
This primitive is used by BS to carry EAP message to an NAS after EAP_Start.

14.5.5.1.1.~~2~~1.2 Semantics of the Service Primitives

~~**14.5.5.1.1.1.2.1 EAP_Start**~~

~~The parameters of the primitives are as follows:~~

~~**C-SM-REQ**~~

~~EAP_Start.request~~

~~(~~
~~Operation Type : Action,~~
~~Action Type : EAP_Start,~~
~~Object ID : NCMS,~~

~~Attribute List :~~

~~MS ID~~

~~Authorization Policy Support,~~

~~)~~

~~MS ID~~

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

~~**Authorization Policy Support**~~

~~Authorization policy negotiated by MSS and BS in SBC-REQ/RSP procedure~~

14.5.5.1.1.~~1~~.2.2.~~12~~ EAP_Transfer

The parameters of the primitives are as follows:

C-SM-REQ

(

Operation Type : Set,

Action Type : EAP_Transfer,

Object ID : NCMS,

Attribute List :

MS ID

EAP Payload,

)

MS ID

48-bit unique identifier used for user identification between BS and NCMS, may be MSS MAC Address

EAP Payload

Contains the EAP authentication data

14.5.5.1.1.~~2~~1.3 When generated

~~**14.5.5.1.1.1.3.1 EAP_Start**~~

~~This primitive is issued by a BS when a MS wants to initiate EAP-based authentication procedure.~~

14.5.5.1.1.~~2~~1.3.~~12~~ EAP_Transfer

This primitive is issued by a BS in EAP procedure to transfer EAP Message included in PKMv2 PKM-REQ/EAP-Transfer message.

14.5.5.1.1.~~2~~1.~~4~~ Effect of receipt

~~**14.5.5.1.1.1.4.1 EAP_Start**~~

~~EAP payloads are forwarded for the authentication between BS and NCMS entity.~~

14.5.5.1.1.~~2~~1.4.~~12~~ EAP_Transfer

The NAS could derive PMK and optional EIK from the MSK , then AK context from PMK after a

successful authentication procedure.

~~**14.5.5.1.1.2 EAP_Transfer**~~

~~**14.5.5.1.1.2.1 Function**~~

~~After the EAP_start primitive, EAP payloads are exchanged between an MS and an NAS entity. The EAP payloads are encapsulated in the EAP Transfer because it is not interpreted in the MAC.~~

~~**14.5.5.1.1.2.2 Semantics of the Service Primitives**~~

~~The parameters of the primitives are as follows:~~

~~EAP_Transfer~~

~~(~~

~~MS ID~~

~~EAP Payload~~

~~)~~

~~MS ID~~

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

~~EAP Payload~~

~~Contains the EAP authentication data~~**~~14.5.5.1.1.3.3 When generated~~**

~~This primitive is issued by a NCMS (a NAS entity) when the EAP exchange are successfully completed and yield the MSK.~~

~~**14.5.5.1.1.3.4 Effect of receipt**~~

~~The BS could derive a PMK and optional EIK from the MSK.~~

14.5.5.1.1.3~~2~~ C-SM-RSP

This primitive (or message) is used by an 802.16 entity to response security information request. The Operation Type included in this primitive defines the type of `security` operation in Authentication and Re-authentication procedure to be performed. The possible Operation Types for this primitive are listed in Table xxx

Operation Type	Action Type	Description
Action	EAP_Transfer	EAP transfer response

14.5.5.1.1.3~~2~~.1 Function

After the C-SM-REQ/EAP_Start primitive, EAP payloads are exchanged between an MS and an NAS entity. The EAP payloads are encapsulated in the C-SM-REQ/EAP_Transfer and C-SM-RSP/EAP_Transfer because it is not interpreted in the MAC. C-SM-RSP/EAP_Transfer is used from NAS in NCMS to BS.

14.5.5.1.1.~~32~~.2 Semantics of the Service Primitives

The parameters of the primitives are as follows:

C-SM-RSP

(
Operation Type : Action,
Action Type : EAP_Transfer,
Object ID : BS,
Attribute List :
MS ID
EAP Payload,

)

MS ID

48-bit unique identifier used for user identification between BS and NCMS, may be MSS MAC Address

EAP Payload

Contains the EAP authentication data

14.5.5.1.1.~~32~~.3 When generated

14.5.5.1.1.2.3.1 EAP_Transfer

This primitive is issued by a NAS in NCMS in EAP procedure to transfer EAP Message to BS.

14.5.5.1.1.~~32~~.4 Effect of receipt

14.5.5.1.1.~~23~~.4.1 EAP_Transfer

The NAS could derive PMK and optional EIK from the MSK , then AK context from PMK after a successful authentication procedure.

~~14.5.5.1.1.3 C-SM-NOTFY~~

~~This primitive (or message) is used by an 802.16 entity to response security information request. The Operation Type included in this primitive defines the type of security operation in Authentication and Re-authentication procedure to be performed. The possible Operation Types for this primitive are listed in Table xxx~~

~~Operation Type~~	~~Action Type~~	~~Description~~
~~Action~~	~~AK_Transfer~~	~~AK transfer notification~~

~~14.5.5.1.1.3.1 Function~~

~~A MS derives the key from the EAP payloads and the NCMS entity informs the BS of it when the EAP exchanges are successfully completed in NAS and yield PMK from MSK, then yield AK from PMK.~~

~~14.5.5.1.1.3.2 Semantics of the Service Primitives~~

~~The parameters of the primitives are as follows:~~

C-SM-NOTFY
(
Operation Type : Action,
Action Type : AK_Transfer,
Object ID : BS,
Attribute List :
MS ID
AK
AK Lifetime
AK Sequence Number
AKID,
)
MS ID
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 accordance with PMK and MSK Lifetime. PMK and MSK Lifetime shall be transferred from the EAP method or be set by a vendor in NAS.
AK Sequence Number
AK Lifetime shall be derived from PMK Sequence Number.
AKID
It should be derived according to IEEE802.16e specification.

14.5.5.1.1.3.3 When generated

This primitive is issued by a NCMS (a NAS entity) when the EAP exchange finishes.

14.5.5.1.1.3.4 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).**14.5.5.1.1.3 EAP_Key_Notification.indication**

14.5.5.1.1.3.1 Function

A MS derives the key from the EAP payloads and the NCMS entity informs the BS of it when the EAP exchanges are successfully completed and yield the MSK.

14.5.5.1.1.3.2 Semantics of the Service Primitives

The parameters of the primitives are as follows:
EAP_Key_Notification.indication
(

~~MS ID~~

~~MSK~~

~~MSK Lifetime~~

~~)~~

~~MS ID~~

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

~~MSK~~

~~MSK is the product of EAP exchanges. It is used for the derivation of PMK (Pair wise Master Key) and EIK.~~

~~MSK Lifetime~~

~~It may be transferred from the EAP method or may be set by a vendor.~~

~~**14.5.5.1.1.3.3 When generated**~~

~~This primitive is issued by a NCMS (a NAS entity) when the EAP exchange are successfully completed and yield the MSK.~~

~~**14.5.5.1.1.3.4 Effect of receipt**~~

~~The BS could derive a PMK and optional EIK from the MSK.~~

14.5.5.2 RSA-based authentication procedure

When an MS tries to initiate an RSA-based authentication or re-authentication procedure with a BS, it sends PKM-REQ messages with Auth Info, Auth Request or PKMv2 RSA-Request message type. When a MS sends a PKM-REQ message with Auth Info message type which includes a CA (Certificate Authority)'s certificate to the BS, the BS informs of an NCMS entity as a C-SM-REQ/Certificate_Infomation~~Certificate_Infomation~~ primitive. The NCSM entity verifies the CA's certificate if it has no information about the CA and keeps the certificate.

When an MS sends a PKM-REQ message with Auth Request or PKMv2 RSA-Request message type to authenticate the MS, the BS informs of an NCMS entity as a C-SM-REQ/Certificate_Verification~~Certificate_Verification_Request~~ primitive. An NCMS entity

verifies the MS's certificate through asking to a CA and an OCSP (Online Certificate Status Protocol) server. The NCMS returns the result of verification to the BS whether the MS is authenticated or not as a C-SM-RSP/Certificate_Verification~~Certificate_Verification_Response~~ primitive. The BS sends the result of authentication and security information to the MS including security key information.

Figure 312 shows a RSA-based authentication procedure between a BS and an NCMS entity as follows:

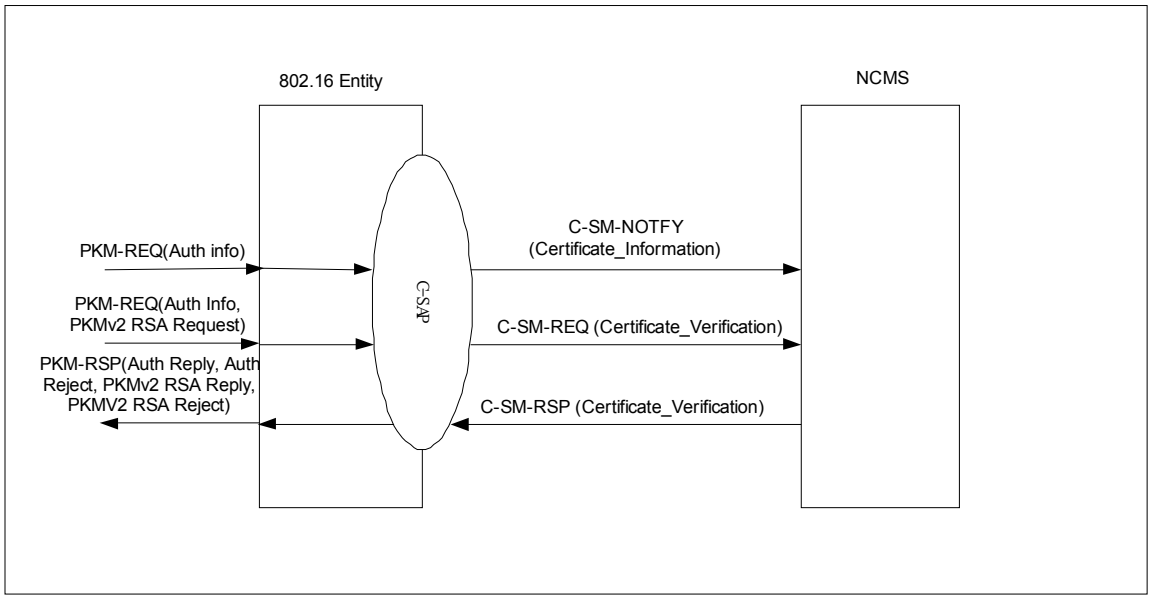


Figure 312 RSA based Authentication Procedure

14.5.5.2.1 Service Primitives

14.5.5.2.1.1 C-SM-NOTFY

This primitive (or message) is used by an 802.16 entity 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 Table xxx.

Event Type	Description
Certificate_Information	Certificate Information request

14.5.5.2.1.1.1 Function

This primitive informs of an NCMS entity that a CA's certificate which issues an MS's certificate.

14.5.5.2.1.1.2 Semantics of the Service Primitives

The parameters of the primitives are as follows:

C-SM-NOTFY

(
Event_Type : Certificate_Information,
Object ID : NCMS,
Attribute List :

MS ID

Certificate

)

MS ID

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

Certificate

CA's certificate which issues an MS's certificate

14.5.5.2.1.1.3 When generated

This primitive is issued by a 802.16 entity (when the BS does not have CA's information that generates the certificate) when an MS informs the BS of CA's certificate.

14.5.5.2.1.1.4 Effect of receipt

The NCMS has information for a CA's certificate and is able to verify an MS's certificate whether the MS's certificate is forged or not.

14.5.5.2.1.2~~1~~ C-SM-REQ

This primitive (or message) is used by an 802.16 entity to trigger security procedure or request security information. The Operation Type included in this primitive defines the type of `security` operation in Authentication and Re-authentication procedure to be performed. The possible Operation Types for this primitive are listed in Table xxx.

Operation Type	Action Type	Description
~~Action~~	~~Certificate_Information~~	~~Certificate Information request~~
Action	Certificate_Verification	Certificate Verification request

14.5.5.2.1.2~~1~~.1 Function

~~**14.5.5.2.1.1.1.1 Certificate_Information**~~

~~This primitive informs of an NCMS entity that a CA's certificate which issues an MS's certificate.~~

14.5.5.2.1.2~~1~~.1.2 Certificate_Verification

This primitive is used by a BS to inform an MS's certificate to authenticate the MS of an NCMS entity.

14.5.5.2.1.~~1~~2.2 Semantics of the Service Primitives

~~**14.5.5.2.1.1.2.1 Certificate_Information**~~

~~The parameters of the primitives are as follows:~~

~~Certificate_Information~~

~~(~~
~~Operation Type : Action,~~
~~Action Type : Certificate_Information,~~
~~Object ID : NCMS,~~
~~Attribute List :~~

~~MS ID~~

~~Certificate~~

~~)~~

~~MS ID~~

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

~~Certificate~~

~~CA's certificate which issues an MS's certificate~~

~~**14.5.5.2.1.1.2.2 Certificate_Verification**~~
The parameters of the primitives are as follows:
C-SM-REQ/Certificate_Verification
(
Operation Type : Set,
Action Type : EAP_Transfer,
Object ID : NCMS,
Attribute List :
MS ID
Certificate,
)
MS ID
48-bit unique identifier used for user identification between a BS and an NCMS, may be MSS MAC Address
Certificate
MS's certificate which is issued by a trust CA

14.5.5.2.1.2~~1~~.3 When generated

~~**14.5.5.2.1.1.3.1 Certificate_Information**~~

~~This primitive is issued by a BS (when the BS does not have CA's information that generates the certificate) when an MS informs the BS of CA's certificate.~~

~~**14.5.5.2.1.1.3.2 Certificate_Verification**~~
This primitive is issued by a BS (when the BS does not have CA information that generates the certificate) when an MS requests the BS for authentication to access the network.

14.5.5.2.1.2~~1~~.4 Effect of receipt

~~**14.5.5.2.1.1.4.1 Certificate_Information**~~

~~The NCMS has information for a CA's certificate and is able to verify an MS's certificate whether the MS's certificate is forged or not.~~

14.5.5.2.1.~~2~~1.4.2 Certificate_Verification

The NCMS verifies an MS's certificate whether the MS's certificate is forged or not, and is revoked or good.

~~**14.5.5.2.1.2 Certificate_Verification_Request**~~

~~**14.5.5.2.1.2.1 Function**~~

~~This primitive is used by a BS to inform an MS's certificate to authenticate the MS of an NCMS entity.~~

~~**14.5.5.2.1.2.2 Semantics of the Service Primitives**~~

~~The parameters of the primitives are as follows:~~

~~Certificate_Verification_Request~~

~~(~~

~~MS ID~~

~~Certificate~~

~~)~~

~~MS ID~~

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

~~Certificate~~

~~MS's certificate which is issued by a trust CA~~ ~~14.5.5.2.1.2.3 When generated~~

~~This primitive is issued by a BS (when the BS does not have CA information that generates the certificate) when an MS requests the BS for authentication to access the network.~~

~~**14.5.5.2.1.2.4 Effect of receipt**~~

~~The NCMS verifies an MS's certificate whether the MS's certificate is forged or not, and is revoked or good.~~

~~**14.5.5.2.1.3 Certificate_Verification_Response**~~

14.5.5.2.1.~~3~~2 C-SM-RSP

This primitive (or message) is used by an 802.16 entity to response security information request. The Operation Type included in this primitive defines the type of security operation in Authentication and Re-authentication procedure to be performed. The possible Operation Types for this primitive are listed in Table xxx

Operation Type	Action Type	Description
Action	Certificate_Verification	Certificate Verification Response

14.5.5.2.1.323.1 Function

14.5.5.2.1.32.1.1 Certificate_Verification

This primitive informs a BS a result of MS's authentication by an NCMS entity.

This primitive informs a BS a result of MS's authentication by an NCMS entity.

14.5.5.2.1.323.2 Semantics of the Service Primitives

14.5.5.2.1.32.2.1 Certificate_Verification

The parameters of the primitives are as follows:

Certificate_Verification_Response

(
Operation Type : Action,
Action Type : EAP_Transfer,
Object ID : BS,
Attribute List :

MS ID

Result

)

MS ID

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

Result

Result of authentication such as valid, forged or revoked

14.5.5.2.1.323.3 When generated

14.5.5.2.1.2.3.1 Certificate_Verification

This primitive informs the authentication result of a BS by a NCMS.

14.5.5.2.1.323.4 Effect of receipt

14.5.5.2.1.32.4.1 Certificate_Verification

The BS transmits the PKM-RSP message to the MS. If the result is success, a pre-PAK

is included in it.

14.5.5.3 Authentication, Authorization and Accounting (AAA) Guidelines

<Section Note: Recommendations for utilizing EAP, RADIUS protocols>

14.5.5.4 Security Context and Key Management

<Section Note: Recommendations for establishment and management of Security Associations, Key establishment and caching policies.>

14.5.5.5 Security for Handoffs (EAP only)

In the handover procedure, if an MS tries to process the network re-entry to a target BS, but the target BS has not an MS information, then the target BS may request the MS information to a serving BS and the serving BS may give a response of it.

Figure 313 shows the context transfer primitives initiated by a serving BS between a BS and an NCMS entity.

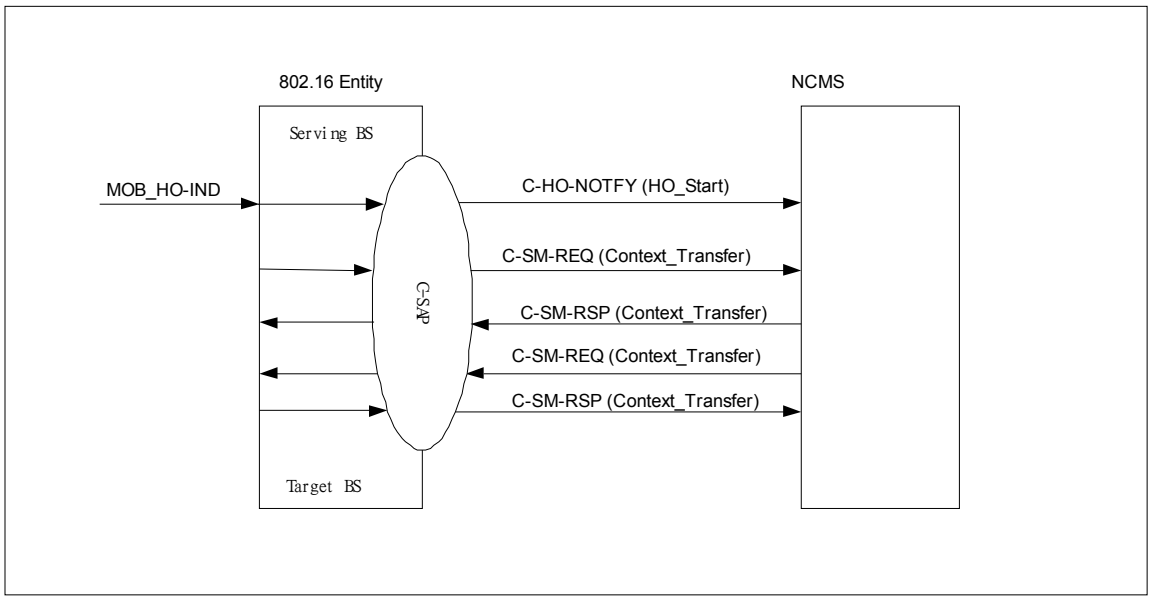


Figure 313 Context transfer primitives initiated by a serving BS

If an MS tries to process the network re-entry to a target BS, but the target BS has not an MS information, then the target BS may request the MS information to a serving BS and the serving BS may give a response of it. Figure 314 shows the context transfer procedure initiated by a target BS between a BS and an NCMS entity as follows.

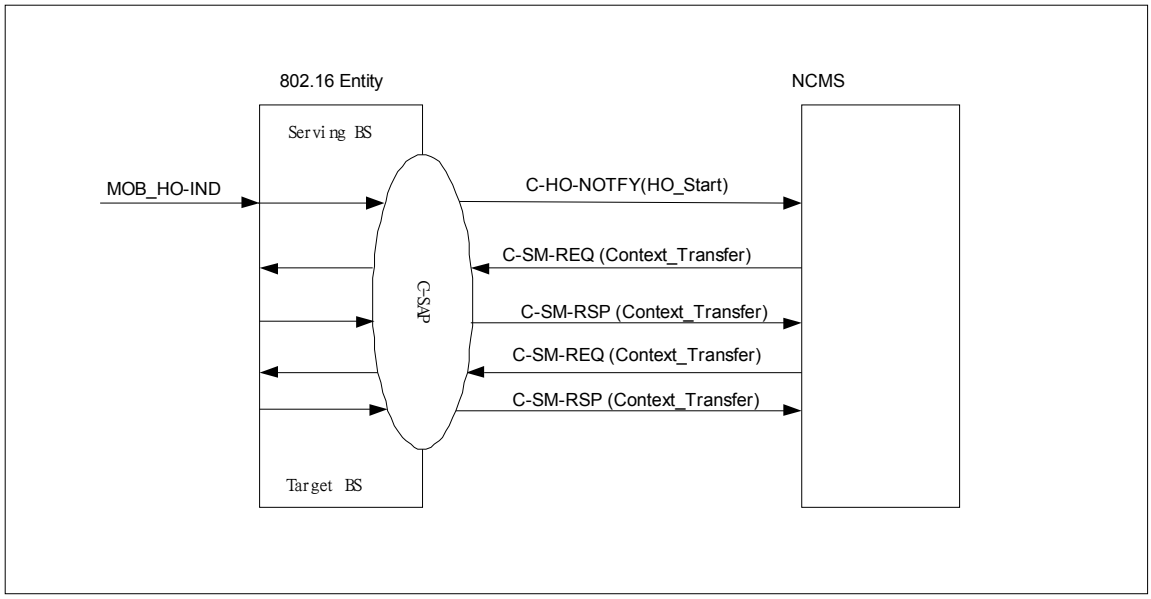


Figure 314 Context transfer procedure initiated by a target BS

14.5.5.5.1 Service Primitives

14.5.5.5.1.1 C-SM-REQ~~IND~~

This primitive (or message) is used by an 802.16 entity or NCMS to indicate to transfer security context. The Operation Type included in this primitive defines the type of security operation handover procedure to be performed. The possible Operation Types for this primitive are listed in Table xxx

Operation Type	Action Type	Description
Action	Context_Transfer	Context Transfer indication

~~Context Transfer.indication~~

14.5.5.5.1.1.1 Function

14.5.5.5.1.1.1.1 Context_Transfer

This primitives is issued by the serving BS or the NCMS entity in order to give the target BS the security context information of the MS. It is transmitted only to the real target after the handover procedure. The MS information what they have could be included.

14.5.5.5.1.1.2 Semantics of the Service Primitives

14.5.5.5.1.1.2.1 Context_Transfer

The parameters of the primitives are as follows:

C-SM-REQ~~IND~~

~~Context Transfer.indication~~

(

Operation Type : Action,

Action Type : Context_Transfer,
Object ID : NCMS or BS,
Attribute List:

Serving BS ID,

Target BS ID,

MS ID,

Security Information

)

MS ID

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

Serving BS ID

Base station unique identifier of the serving BS (same as in the DL-MAP)

Target BS ID

Base station unique identifier of the target BS (same as in the DL-MAP)

Security Information

The information negotiated during PKM procedure. It presents when the information could be provided. AK and AK sequence number transmitted by NCMS, TEK, TEK key lifetime, TEK sequence number, CBC Initialize Vector (the reuse of IV is TBD because of the security issue), SAID, GKEK, GKEK lifetime, GKEKKID, SAID, SA-type, SA service type and Cryptographic-Suite

14.5.5.5.1.1.3 When generated

14.5.5.5.1.1.3.1 Context_Transfer

This primitive is issued by a BS or the NCMS when the handover procedure is successfully processed. The actual trigger point may be different according to the security sharing policy. One example is a serving BS issues this primitive after it generates HO start primitive.

14.5.5.5.1.1.4 Effect of receipt

14.5.5.5.1.1.4.1 Context_Transfer

The entity receiving this primitive shall response with C-SM-IND/Context_Transfer~~-confirmation~~ primitive. In addition, if the serving BS issues this primitive for the MS security information, the NCMS entity shall forwards the MS information to the target BS or another NCMS entity using C-SM-IND/Context_Transfer~~Context~~

~~Transfer.indication~~ primitive.

14.5.5.5.1.2 C-SM-RSP~~CONFM~~

This primitive (or message) is used by an 802.16 entity or NCMS to ~~confirm~~respond the C-SM-REQ~~IND~~ . The Operation Type included in this primitive defines the type of `security` operation handover procedure to be performed. The possible Operation Types for this primitive are listed in Table xxx

Operation Type	Action Type	Description
Action	Context_Transfer	Context Transfer confirm

14.5.5.5.1.2.1 Function

14.5.5.5.1.2.1.1 Context_Transfer

This primitive is issued by the target BS or the NCMS in order to response the C-SM-IND/Context_Transfer~~Context Transfer.indication~~.

14.5.5.5.1.2.2 Semantics of the Service Primitives

14.5.5.5.1.2.2.1 Context_Transfer

The parameters of the primitives are as follows:

C-SM-RSP~~CONFM~~~~Context Transfer.confirmation~~

(
Operation Type : Action,
Action Type : Context_Transfer,
Object ID : NCMS or BS,
Attribute List:

Serving BS ID,

Target BS ID,

MS ID,

Result Code

)

MS ID

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

Serving BS ID

Base station unique identifier of the serving BS (same as in the DL-MAP).

Target BS ID

Base station unique identifier of the target BS (same as in the DL-MAP).

Result Code

The result of context transfer procedure.

14.5.5.5.1.2.3 When generated

14.5.5.5.1.2.3.1 Context_Transfer

This primitive is issued by the target BS or the NCMS when the C-SM-IND/Context_Transfer~~Context Transfer.indication~~ is successfully processed.

14.5.5.5.1.2.4 Effect of receipt

14.5.5.5.1.2.4.1 Context_Transfer

This primitive informs the result of context transfer for the handover

~~**14.5.5.5.1.3** C-SM-REQ~~

~~This primitive (or message) is used by an 802.16 entity to request security information. The Operation Type included in this primitive defines the type of security operation handover procedure to be performed. The possible Operation Types for this primitive are listed in Table xxx~~

~~**Operation Type**~~	~~**Action Type**~~	~~**Description**~~
~~Action~~	~~Context_Transfer~~	~~Context Transfer request~~

~~**Context Transfer.request**~~

~~14.5.5.5.1.3.1 Function~~

~~14.5.5.5.1.3.1.1 Context_Transfer~~

~~After the successful handover procedure, the Target BS can re-establish the session information of MS in old BS.~~

~~14.5.5.5.1.3.2 Semantics of the Service Primitives~~

~~14.5.5.5.1.3.2.1 Context_Transfer~~

~~The parameters of the primitives are as follows:~~

~~C-SM-REQ~~

~~Context Transfer.request~~

~~(~~

~~Operation Type : Action,~~

~~Action Type : Context_Transfer,~~

~~Object ID : NCMS,~~

~~Attribute List:~~

~~Serving BS ID,~~

~~Target BS ID,~~

~~MS ID~~

~~)~~

~~MS ID~~

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

~~Serving BS ID~~

Base station unique identifier of the serving BS (same as in the DL-MAP)
Target BS ID
Base station unique identifier of the target BS (same as in the DL-MAP)
14.5.5.5.1.3.3 When generated
14.5.5.5.1.3.3.1 Context_Transfer

This primitive is issued by the target BS or the NCMS entity to request the MS's security context information.

14.5.5.5.1.3.4 Effect of receipt
14.5.5.5.1.3.4.1 Context_Transfer

The NCMS entity or the BS receiving this primitive provides the security context information using C-SM-RSP/Context_Transfer.response primitive.

14.5.5.5.1.4 C-SM-RSP
This primitive (or message) is used by an 802.16 entity to response C-SM-REQ/Context_Transfer. The Operation Type included in this primitive defines the type of security operation handover procedure to be performed. The possible Operation Types for this primitive are listed in Table xxx

Operation Type	**Action Type**	**Description**
Action	Context_Transfer	Context Transfer response

Context Transfer.response

14.5.5.5.1.4.1 Function
14.5.5.5.1.4.1.1 Context_Transfer
This primitive is issued by the serving BS or the NCMS to response the C-SM-REQ/Context_Transfer.request.

14.5.5.5.1.4.2 Semantics of the Service Primitives
14.5.5.5.1.4.2.1 Context_Transfer

The parameters of the primitives are as follows:

C-SM-RSP
Context Transfer.response
(
Operation Type : Action,
Action Type : Context_Transfer,
Object ID : NCMS,
Attribute List:
Serving BS ID,
Target BS ID,
MS ID,
Result Code,
Security Information
)
MS ID
48-bit unique identifier used for user identification between BS and NCMS
Serving BS ID
Base station unique identifier of the serving BS (same as in the DL-MAP)
Target BS ID
Base station unique identifier of the target BS (same as in the DL-MAP)
ResultCode
The result of context transfer procedure
Security Information
The information negotiated during PKM procedure. AK and AK sequence number transmitted by an NCMS, TEK, TEK key lifetime, TEK sequence number, CBC Initialize Vector (the reuse of IV is TBD because of the security issue), SAID, SA-type, SA service type and Cryptographic-Suite
14.5.5.5.1.4.3 When generated
14.5.5.5.1.4.3.1 Context_Transfer

This primitive is issued by the serving BS or the NCMS entity after receiving C-SM-REQ/Context_ Transfer.request primitive.

14.5.5.5.1.4.4 Effect of receipt
14.5.5.5.1.4.4.1 Context_Transfer
This primitive informs the result of context transfer for the handover
14.5.5.6 Protecting Management Messages
<Section Note: Recommendations for protecting management messages.>
14.5.6 Service Flow Management
14.5.6.1 BS Service Provisioning
<Section Note: Provisioning of the services on the BS are described. Ex: Setting and retrieval of Operator IDs, BS IDs etc. and type of convergence layers supported and their configuration parameters are described.>
14.5.6.2 SS/MS Provisioning

~~<Section Note: Provisioning. Configuration and management for BS initiated connections and service flow creations for static and dynamic QoS>~~