Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Amendment to RSA Security Primitives in 14.2.2.2**
Date Submitted	**2007-03-15~~08~~**
Source(s)	Jung-Mo Moon, Jeehyeon Na, Mi-Young Yun, and Sangho Lee jhna@etri.re.kr ETRI 161 Gajeong-dong, Yuseong-gu Daejeon 305-700 Korea
Re:	Contribution on comments to IEEE 802.16g/D8
Abstract	Re-definition of RSA primitives in section 14.2.2.2
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." 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 RSA Security Primitives in 14.2.2.2

Jung Mo Moon, Jeehyeon Na, Mi Young Yun, and Sangho Lee

ETRI

1. Introduction

IEEE 802.16g Network reference model defines a NCMS and an 802.16 entity in an SS and a BS side. However Section 14.2.2.2 only describes RSA-based security primitives on the BS side. Therefore RSA-based security primitives on an SS side are also needed for consistency. They shall be used as an interface between an RSA authentication application and an 802.16 entity(SS).

This contribution adds RSA-based security primitives on an SS side and changes some texts which are related to them.

We propose to modify section 14.2.2.2 as follows.

1. Modification of figure 474 which illustrate security primitives on the SS side.
2. Modification of each subsection to clarify and describes on each side (SS and BS side)

2. Proposed Text Changes

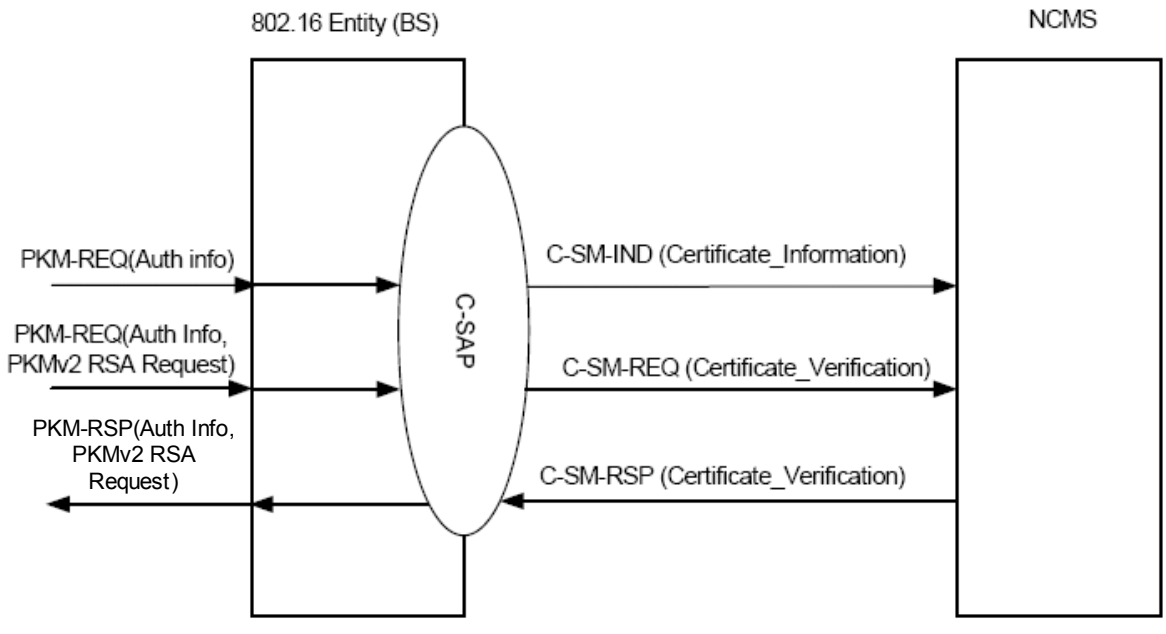
[*Modify Subclause 14.2.2.2 as follows*]

14.2.2.2 RSA-based authentication procedure

When an SS 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 an NCMS(SS) sends a C-SM-REQ/Certificate_Infomation primitive to an 802.16 entity(SS)sends a PKM-REQ message with Auth Info message type which includes a CA (Certificate Authority)'s certificate to the 802.16 entity(BS), the 802.16 entity(BS) informs of the NCMS(BS) ~~entity~~ as a C-SM-REQ/Certificate_Infomation primitive. The NC~~S~~MS(BS) verifies the CA's certificate if it has no information about the CA and keeps the certificate.

When an NCMS(SS) sends a C-SM-REQ/Certificate_Verification primitive to the 802.16 entity(SS) to authenticate the SS and the 802.16 entity (SS) ~~an SS~~ sends a PKM-REQ message with Auth Request or PKMv2 RSA-Request message type~~ to authenticate the SS~~, the 802.16 entity(BS)~~BS~~ informs of the NCMS(BS) ~~entity~~ as a C-SM-REQ/Certificate_Verification primitive. The NCMS(BS) ~~entity~~ verifies the SS's certificate through asking to a CA and an OCSP (Online Certificate Status Protocol) server. The NCMS returns the result of verification to the 802.16 entity(BS) ~~BS~~ whether the SS is authenticated or not as a C-SM-RSP/Certificate_Verification primitive. The 802.16 entity(BS) sends the result of authentication and security information to the 802.16 entity(SS) including security key information and the 802.16 entity(SS) returns the result as a C-SM-RSP/Certificate_Verification primitive.to the NCMS(SS)

Figure 474 shows a RSA-based authentication procedure between an 802.16 entity ~~a BS~~ and ~~the~~ an NCMS on the MS side and the BS side ~~entity~~ as follows:



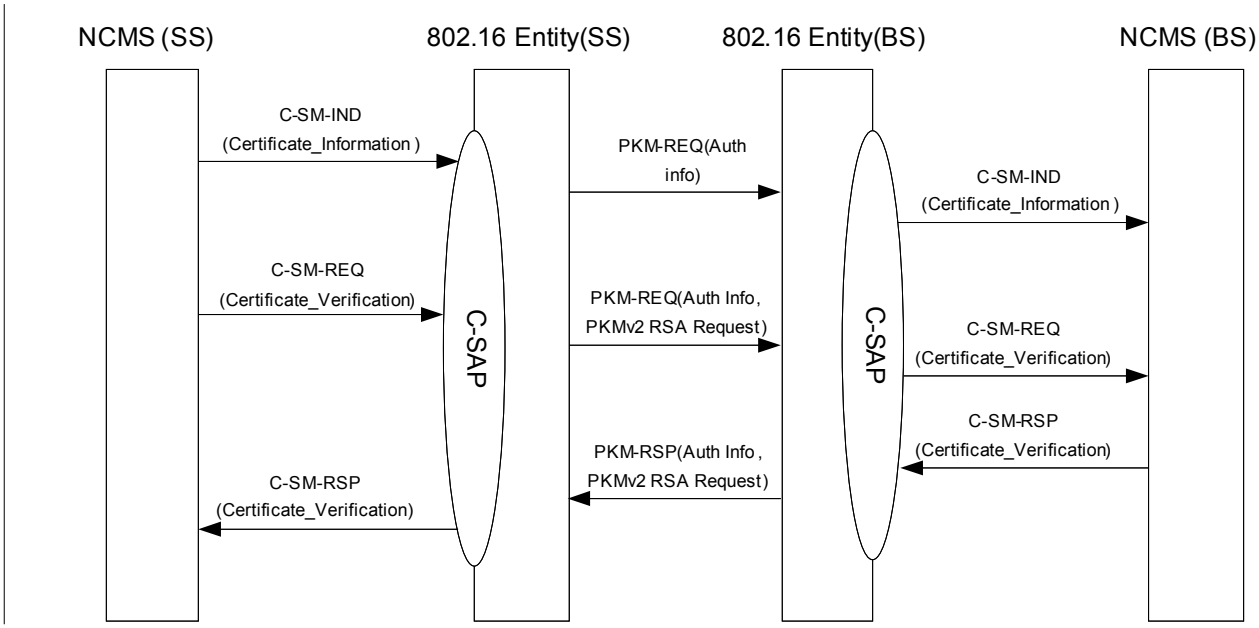


Figure 474 – RSA based Authentication Procedure

[*Modify Subclause 14.2.2.2.1 as follows*]

14.2.2.2.1 C-SM-IND

This primitive (or message) is used by an NCMS(SS) or an 802.16 entity(BS) 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 below:

Table 451—C-SM-IND Event_Types

Event_Type	Description
Certificate Information	Certificate Information request

Function

This primitive informs the 802.16 entity(SS) of the certificate of the CA that issued the SS's certificate. In addition, this primitive informs the NCMS ~~entity~~(BS) of the certificate of the CA that issued the SS's certificate.

Semantics of the service primitives

The parameters of the primitives are as follows:

C-SM-IND

(

Event_Type: Certificate_Information,

Destination: NCMS, SS,
Attribute_List:
~~MS~~ SS MAC Address,
Certificate
)

S~~M~~S MAC Address
48-bit unique identifier used for user identification between a BS and the NCMS
Certificate
Certificate of the CA that issues the SS's certificate

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 SS informs the BS of CA's certificate~~

- NCMS(SS) -> 802.16 Entity(SS) :
  This primitive is issued by the NCMS(SS) when the NCMS(SS) informs the BS of CA's certificate .
- 802.16 entity(BS) -> NCMS(BS) :
  This primitive is issued by an 802.16 entity(BS) (when the BS does not have CA's information that generates the certificate) when an SS informs the BS of CA's certificate

Effect of receipt

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

- NCMS(SS) -> 802.16 Entity(SS) :
  When received by the SS, the SS forwards a CA's ~~C~~certificate to BS via a PKM-REQ message.
- 802.16 entity(BS) -> NCMS(BS) :
  The NCMS(BS) has information for a CA's certificate and is able to verify an SS's certificate whether the SS's certificate is forged or not.

[*Modify Subclause 14.2.2.2.2 as follows*]

14.2.2.2.2 C-SM-REQ

This primitive (or message) is used by an NCMS(SS) or an 802.16 entity(BS) to trigger security procedure or request security information.

Table 452—C-SM-REQ Operation_Types

Operation_Type	Action_Type	Description
Action	Certificate Verification	Certificate Verification Request

Function

This primitive is used by an NCMS(SS) or an 802.16 entity(BS) ~~a BS~~ to inform an 802.16 entity(SS) or the NCMS(BS) of an SS's certificate to authenticate the SS ~~of the NCMS entity~~.

…

Semantics of the service primitives

The parameters of this primitive are as follows:

C-SM-IND

(
Operation_Type: Action,
Action_Type: Certificate_Verification,
Destination: BS, NCMS,
Attribute_List:
SMS MAC Address,
Certificate
)

SMS MAC Address

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

Certificate

SS's certificate which is issued by a trusted CA

When generated

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

- NCMS(SS) -> 802.16 Entity(SS) :
  This primitive is issued by an NCMS(SS) when an SS requests ~~the~~a BS for authentication to access the network.
- 802.16 entity(BS) -> NCMS(BS) :
  This primitive can be issued by 802.16 entity(BS) in RSA procedure to transfer a SS's certificate included in a ~~PKMv2~~ PKM-REQ message.

Effect of receipt:

~~The NCMS verifies the validity of the SS's certificate.~~

- NCMS(SS) -> 802.16 Entity(SS) :
  When received by an 802.16 entity(SS), the SS forwards SS's certification in a PKM-REQ message to the BS .
- 802.16 entity(BS) -> NCMS(BS) :
  The NCMS(BS) verifies the validity of the SS's certificate.

14.2.2.2.3 C-SM-RSP

This primitive (or message) is used by ~~the~~ an NCMS(BS) or an 802.16 entity(SS) to respond to the security information request. The Operation_Type included in this primitive defines the type of security operation in Authentication and Reauthentication procedure to be performed. The possible Operation_Types for this primitive are listed in Table below:

…

Function

This primitive informs the 802.16 entity(~~the~~ BS) or the NCMS(SS) of the result of the SS's authentication by the NCMS entity.

Semantics of the service primitives:

The parameters of the primitives are as follows:

C-SM-RSP
(
Operation_Type: Action,
Action_Type: Certificate_Verification,
Destination: BS, NCMS,
Attribute_List:
SMS MAC Address,
Result
)

SMS MAC Address
48-bit unique identifier used for user identification between a BS and the NCMS
Result
Result of authentication such as valid, forged or revoked

)

When generated:

This primitive informs the BS the result of the authentication.

- NCMS(BS) -> 802.16 Entity(BS) :
  This primitive informs the 802.16 entity(BS) the result of the authentication result.

- 802.16 entity(SS) -> NCMS(SS) :
  This primitive informs the NCMS(SS) of the result of the authentication result.

Effect of receipt:

The BS transmits the PKM-RSP message to the SS. If the result is successful, a pre-Primary AK is included in it.

- NCMS(BS) -> 802.16 Entity(BS) :
  The 802.16 entity(BS) transmits thea PKM-RSP message to the 802.16 entity(SS). If the result is successful, a pre-Primary AK is included in it.

- 802.16 entity(SS) -> NCMS(SS) :
  The NCMS(SS) receives this message and getand the authentication result.