Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**RSA-based Authentication Procedure and Primitives**
Date Submitted	**2005-09-13**

Source(s)	Jung Mo Moon, PhD	jmmoon@etri.re.kr
	Mi-Young Yun	myyun@etri.re.kr
	Jaesun Cha	jscha@etri.re.kr
	Sang Ho Lee, PhD	leesh@etri.re.kr
	ETRI	
	161, Gajeong-dong,Yuseong-gu,	Voice: 82-42-860-4821
	Daejeon, 305-700, Korea	Fax: 82-42-861-1966

Re:	Contribution on comments to IEEE 802.16g-05/008
Abstract	In this contribution, we describe the RSA authentication procedure and service primitives that could be exchanged between the BS and the NCMS entities.
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>.

RSA-based Authentication Procedure and Primitives

Jung Mo Moon, Mi Young Yun, Jaesun Cha and Sang Ho Lee

ETRI

1. Problem Statement

The purpose of this contribution is to describe the RSA-based authentication procedure and service primitives that could be exchanged between the BS and the NCMS entities. This proposal makes it possible to perform the authentication as specified in the remainder of this document.

A RSA-based authentication method is used for authenticating an MS with MS's certificate. A certificate has a public key of MS and is guaranteed by a trust CA (Certification Authority). When an MS submits its certificate to access the network, the network should verify the certificate whether the certificate is issued by a trust CA and whether the certificate is revoked by interrogating an OSCP (Online Certificate Status Protocol) server. In IEEE 802.16, the certificate of MS will not become obsolete because validation time is long enough (at lease 10 years old). However, it may be stolen or lost, so a verification procedure of the certificate is required. Therefore, we define primitives that a BS transfers a MS's certificate to prove validity of it when the MS accesses to the BS.

2. Summary of the Proposed Remedy

In this contribution, we define 3 primitives to support authentication management between a BS and an access network (NCMS) which are described briefly in the following table.

Primitive	Direction	Primitive Contents
Certificate_Information	BS -> NCMS	MS ID, Certificate
Certificate_Verification_Request	BS -> NCMS	MS ID, Certificate
Certificate_Verification_Response	BS <- NCMS	MS ID, Result

Figure1 shows the RSA-based authentication procedure. An MS may inform a BS of CA's certificate to indicate who issues the MS's certificate. When a BS receives a CA's certificate, it asks validation of the certificate to a NCMS through network nodes such as a CA if the NCMS has no information about the CA.

When a BS receives a certificate from an MS for authentication, it checks whether the certificate is forged or revoked through network nodes such as an NCMS, CAs and an OSCP server. A certificate request procedure in figure 1 is omitted if the NCMS has a public key of CA which issues the MS's certificate. The NCMS should request the validation of the MS's certificate to an OSCP server whether it is revoked or not.

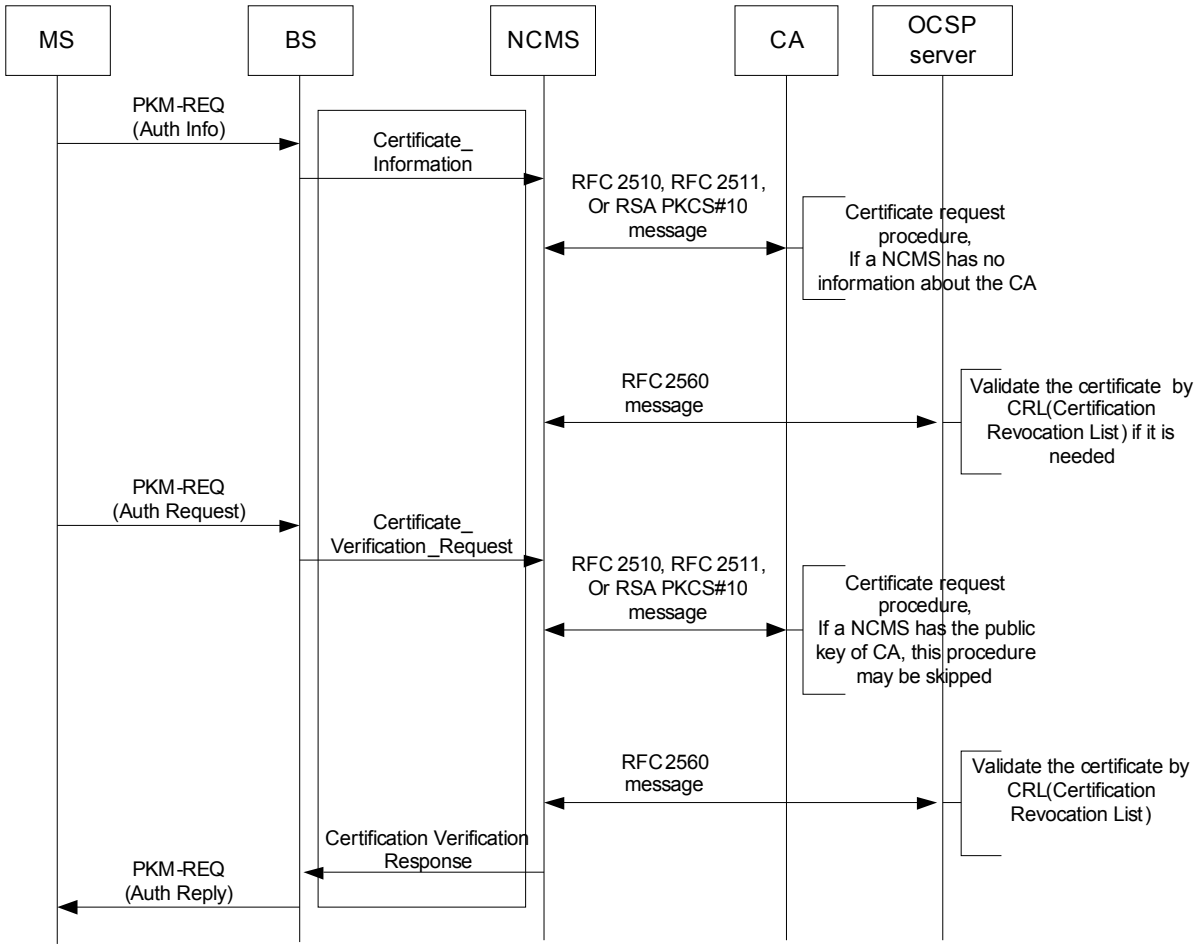

Figure 1. RSA-based authentication procedure

3. Proposed Text Changes

[*Insert section 14.5.5.5 as follow*]
14.5.5 Security Management

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 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 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 Certificate_Verification_Response primitive. The BS sends the result of authentication and security information to the MS including security key information.

Figure X1 shows a RSA-based authentication procedure between a BS and an NCMS entity as follows

.

Figure X1. RSA-based authentication procedure

14.5.5.2.1 Service Primitives

14.5.5.2.1.1 Certificate_Information

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:

Certificate_Information
{

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 BS (when the BS does not have CA's information that generates the certificate) when an MS informs the BS of CA's certificate.

14.5.5.2.1.1.4 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 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

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

14.5.5.2.1.3.2 Semantics of the Service Primitives

The parameters of the primitives are as follows:

Certificate_Verification_Response
{
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

14.5.5.2.1.3.3 When generated

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

14.5.5.2.1.3.4 Effect of receipt

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

References

[1] C. Adams and S. Farrell, " Internet X.509 Public Key Infrastructure Certificate Management Protocols," RFC2510, March 1999.
[2] M. Myers et. al., " Internet X.509 Certificate Request Message Format," RFC2510, March 1999.
[3] M. Myers et. al., " X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," RFC2510, June 1999.
[4] IEEE-Std 802.16-2004
[5] IEEE 802.16e/D10