Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Authorization and Key Exchange in 802.16j system**
Date Submitted	**2007-01-08**
Source(s)	Yanling Lu, Ting Li Hisilicon Technologies Harbour Building, No.8, Dongbeiwang West Road, HaiDian District, Beijing, China Voice: 86-10-82829010 Fax: 86-10-82829075 mailto: luyanling@hisilicon.com
Re:	This contribution is a response to "IEEE 802.16j-06/034 Call for Technical Proposals regarding IEEE Project 802.16j" (2006-12-12) .
Abstract	This contribution described the proposed Authorization and Key Exchange in 802.16j system.
Purpose	This document is provided in response for Call for Technical Proposals regarding IEEE Project 802.16j .
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>.

Authorization and Key Exchange in 802.16j system

Yanling Lu, Ting Li
Hisilicon Technologies

1. Introduction

In the 802.16j system, the MR-BS and the new MS shall perform authorization and key exchange during the MS's network entry procedure. This contribution proposes the authorization and AK exchange procedures for the new MS, which need access into the network through RSs.

2. Proposed Solution

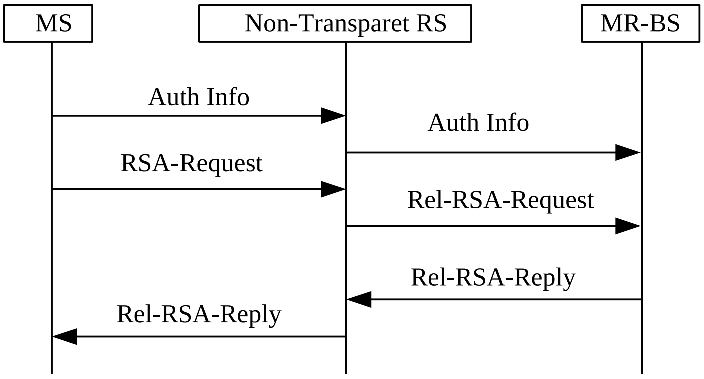

Figure 1-An example of a MS authorization and AK exchange

To perform the authorization and AK exchange via RSA authentication protocol in 802.16j system, a MS begins authorization by sending an Authentication Information message to its super ordinate node. This message is relayed to the MR-BS hop by hop.

Then the MS sends an Authorization Request message to its super ordinate node immediately after sending the Authentication Information message. The PKMv2 RSA-Request message includes:

a) MS_Random, a 64-bit random number generated in the MS;

b) MS_Certificate, containing the MS's user certificate;

c) SAID, MS's primary SAID equal to the Basic CID;

d) SigSS, An RSA signature over all the other attributes in the message.

If this request is received by a transparent RS, this RS only relays this request to its super ordinate node. While if this request is received by a non-transparent RS, this non-transparent RS shall check the SigSS/SigRS and initiate Rel-RSA-Request based on the received message by performing the following procedure:

1)Replace the MS_Random/RS_Random in the received request message with the RS_Random generated by the current node

2) Replace the SigSS/SigRS in the received request message with the SigRS, an RSA signature over all the other attributes in the new message generated by the current node.

Then PKMv2 Rel-RSA-Request message includes:

a) RS_Random, a 64-bit random number generated in the RS;

b) MS_Certificate, containing the MS's user certificate;

c) SAID, MS's primary SAID equal to the Basic CID;

d) SigRS, An RSA signature over all the other attributes in the message.

After the request message is received by the MR-BS, the MR-BS validates the requesting MS's identity, determines the encryption algorithm and protocol support it shares with the MS, activates an AK for the MS, encrypts it with the MS's public key, and sends it back to the MS in an Authorization Reply message. The PKMv2 Rel_RSA-Reply message generated by the MR-BS includes:

a) RS_Random, the 64-bit random number received by the MR-BS in the Rel_RSA-Request;

b) BS_Random, a 64-bit random number generated by the MR-BS;

c) Encrypted pre-PAK,

d) Key Lifetime, PAK Aging timer

e) Key Sequence Number ,PAK sequence number

f) BS_Certificate, Containing the BS/RS's X.509 certificate

g) SigBS. An RSA signature over all the other attributes in the message

If this reply is received by a transparent RS, this RS relays this reply to its sub ordinate node only. While if this reply is received by a non-transparent RS, this RS should validates its super ordinate node's identity, check the message signature and compare the RS_Random/MS_Random in the received reply message with the MS_Random/RS_Random in the request message sent before. Then this non-transparet RS shall initiate new Rel_RSA-Reply based on the received reply message by performing the following procedure:

1) Replace the RS_Random in the received reply for its super ordinate node with the RS _Random or MS _Random in the received request sent by its subordinate node.

2) Replace the BS_Random or RS_Random in the received reply with the RS_Random generated by the current node.

3) Replace the BS_Certificate or RS_Certificate with the RS_Certificate of the current node.

4) Replace SigBS or SigRS with the SigRS generated by the current node.

Then the PKMv2 Rel_RSA-Reply message generated by the RS includes:

a) RS_Random/MS_Random, the 64-bit random number received by the current node in the Rel_RSA-Request or in the RSA-Request;

b) RS_Random, a 64-bit random number generated by the current node;

c) Encrypted pre-PAK,

d) Key Lifetime, PAK Aging timer

e) Key Sequence Number ,PAK sequence number

f) RS_Certificate, Containing the RS's X.509 certificate

g) SigRS. An RSA signature over all the other attributes in the message

For Rel_RSA-Reply message's format is compliant with RSA-Reply message, the MS will consider the Rel_RSA-Reply is sent by the BS in 802.16j system. No change is required to the MS.

3. Proposed Text

6.3.2.3.MAC management message

6.3.2.3.9 Privacy key management(PKM) message (PKM-REQ/PKM-RSP)

Add two rows into Table 26:

Code	PKM message type	MAC Management message name
<TBD>	PKMv2 Rel-RSA-Request	PKM-REQ
<TBD>	PKMv2 Rel-RSA-Reply	PKM-RSP

[Insert new subclause 6.3.2.3.9.xx]

6.3.2.3.9.XX PKMv2 Rel-RSA-Request

A RS sends a PKMv2 Rel-RSA-Request to its super ordinate node in order to request the MS and MR-BS's mutual authentication in a RSA-based authorization.

Table 37x PKMv2 Rel-RSA-Request attributes

Attribute	Content
RS_Random	A 64-bit random number generated in the current RS
MS_Certificate	Contains the MS's user certificate
SAID	MS's primary SAID equal to the Basic CID
SigRS	An RSA signature over all the above attributes in the message

On receiving the Rel-RSA-Request, to originate new Rel-RSA-Request, the intermediate RS shall replace the RS_Random with the random generated by itself and replace the SigRS in the received message with the RSA new signature.

6.3.2.3.9.XX PKMv2 Rel-RSA-Reply

Sent by the MR-BS/RS to its subordinate node, the PKMv2 Rel-RSA-Reply contains an encrypted pre-PAK, the key s lifetime, and the key s sequence number. The pre-PAK shall be encrypted with the MS s public key.

Table 37x PKMv2 Rel-RSA-Reply attributes

Attribute	Content
RS_Random/MS_Random	the 64-bit random number received by the current node in the Rel_RSA-Request
BS_Random/RS_Random,	a 64-bit random number generated by the current node
Encrypted pre-PAK	RSA-OAEP-Encrypt(PubKey(MS), pre-PAK | MS MAC

	Address)
Key Lifetime	PAK Aging timer
Key Sequence Number	PAK sequence number
BS_Certificate/RS_Certificate	Containing the BS/RS's X.509 certificate
SigBS/SigRS	An RSA signature over all the other attributes in the message

When the Rel-RSA-Reply is generated by the MR-BS, the RS_Random number is returned from the PKMv2 Rel-RSA-Request message received by the MR-BS, along with a random number supplied by the MR-BS, thus enabling assurance of key liveness. The BS_Certificate is also included via which to verify the MR-BS's identity by the sub-ordinate RS. The SigBS is used to assure the authenticity of all the other attributed in Rel-RSA-Reply messages.

When the Rel-RSA-Reply is generated by the intermediate RS, the RS_Random or MS_Random number is returned from the Rel-RSA-Request message or the RSA-Request message received by the RS, along with a random number supplied by the RS, thus enabling assurance of key liveness. The RS_Certificate is also included via which to verify the RS identity by the sub-ordinate node. The SigRS is used to assure the authenticity of all the other attributed in Rel-RSA-Reply messages.

7.2.1.3 MS authorization and AK exchange overview

[Insert new subclause 7.2.1.3.2]

7.2.1.3.2 Authorization via RSA authentication protocol in MR system

To perform the authorization and AK exchange via RSA authentication protocol in 802.16j system, a MS begins authorization by sending an Authentication Information message to its super ordinate node. This message is relayed to the MR-BS hop by hop.

Then the MS sends an Authorization Request message to its super ordinate node immediately after sending the Authentication Information message.

If this request is received by a transparent RS, this RS only relays this request to its super ordinate node. While if this request is received by a non-transparent RS, this non-transparent RS shall initiate Rel_RSA-Request message, which includes:

a) RS_Random, a 64-bit random number generated in the RS;

b) MS_Certificate, containing the MS's user certificate;

c) SAID, MS's primary SAID equal to the Basic CID;

d) SigRS, An RSA signature over all the other attributes in the message.

After the request message is received by the MR-BS, the MR-BS validates the requesting MS's identity, determines the encryption algorithm and protocol support it shares with the MS, activates an AK for the MS, encrypts it with the MS's public key, and sends it back to the MS in an Authorization Reply message. The Rel_RSA-Reply generated by the MR-BS includes:

a) RS_Random, the 64-bit random number received by the MR-BS in the Rel_RSA-Request;

b) BS_Random, a 64-bit random number generated by the MR-BS;

c) Encrypted pre-PAK,

d) Key Lifetime, PAK Aging timer

e) Key Sequence Number ,PAK sequence number

f) BS_Certificate, Containing the BS/RS’s X.509 certificate

g) SigBS. An RSA signature over all the other attributes in the message

If this reply is received by a transparent RS, this RS relays this reply to its sub ordinate node only. While if the reply is received by a non-transparent RS, this non-transparent RS shall generate new Rel_RSA-Reply based on the received reply message. The Rel_RSA-Reply generated by the RS includes :

a) RS_Random/MS_Random, the 64-bit random number received by the current node in the Rel_RSA-Request or in the RSA-Request;

b) RS_Random, a 64-bit random number generated by the current node;

c) Encrypted pre-PAK,

d) Key Lifetime, PAK Aging timer

e) Key Sequence Number ,PAK sequence number

f) RS_Certificate, Containing the RS’s X.509 certificate

g) SigRS. An RSA signature over all the other attributes in the message

The Rel_RSA-Reply message is

For Rel_RSA-Reply message’s format is compliant with RSA-Reply message, when the Rel_RSA-Reply is received by the MS, the MS will consider its super-ordinate non-transparent RS as the BS.

A MS shall periodically refresh its AK by reissuing an Authorization Request to the MR-BS. Reauthorization is identical to authorization with the exception that the MS does not send Authentication Information messages during reauthorization cycles.

References

[1] IEEE 802.16mmr-06/002r1, “ Draft P802.16j PAR and Five Criteria: Mobile Multi-hop Reply "
[2] IEEE 802.16j-06/016r1, “ Proposed Technical Requirements Guideline for IEEE 802.16 Relay TG "
[3] IEEE 802.16j-06/017r2, “ Table of Contents of Task Group Working Document "