

<b>IEEE 802.16 Broadband Wireless Access Working Group &lt;<a href="http://ieee802.org/16">http://ieee802.org/16</a>&gt;</b>	
Title	<b>MBS Security Support for PKMv2</b>
Date Submitted	<b>2004-06-24</b>
Source(s)	JUNHYUK SONG, Samsung <a href="mailto:junhyuk.song@SAMSUNG.COM">junhyuk.song@SAMSUNG.COM</a> David, Johnston, Intel <a href="mailto:dj.johnston@INTEL.COM">dj.johnston@INTEL.COM</a> Ypungman Park, Korea Telecom <a href="mailto:Youngman@kt.co.kr">Youngman@kt.co.kr</a>
Re:	Re: Security Adhoc PKMv2
Abstract	Proposal for MBS Security Support for PKMv2
Purpose	Discuss and Adopt as the baseline text
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 < <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, 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 < <a href="mailto:chair@wirelessman.org">mailto:chair@wirelessman.org</a> > 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 < <a href="http://ieee802.org/16/ipr/patents/notices">http://ieee802.org/16/ipr/patents/notices</a> >.

# PKM version 2

## MBS Security Baseline text proposal

*JUNHYUK SONG, Samsung Electronics  
David Johnston, INTEL Corp  
YoungMan Park, Korea Telecom*

### 1 MBS Security Functionality

#### 1.1 MBS Security Association and Key Management

MBS has a set of security information: MBS SA that multiple BS and one or more if its client SSs shares but not bind to any MSS connection state. Each MBS capable MSS may establish a MBS security association during the SS initialization process. MBS SAs shall be provisioned within the BS. (See figure-1)

Figure 1 MBS Security Association

MBS Authorization Key (MAK) is the basis of the service authorization for MBS. The MBS content server distributes the MAK to the MS via content subscription with appropriate user authentication. MAK provides access to one or more

multicast IP flows of a particular set of MBS programs for a certain amount of time (for example, one day, week or month). Each encrypted set of MBS programs shall have a different MAK and GTEK value.

MBS Authorization Key (MAK) establishment

The MAK establishment procedure in MSS and BS is outside of scope of this specification But it should include liveness/freshness guarantees.

Distribution of GTEKs

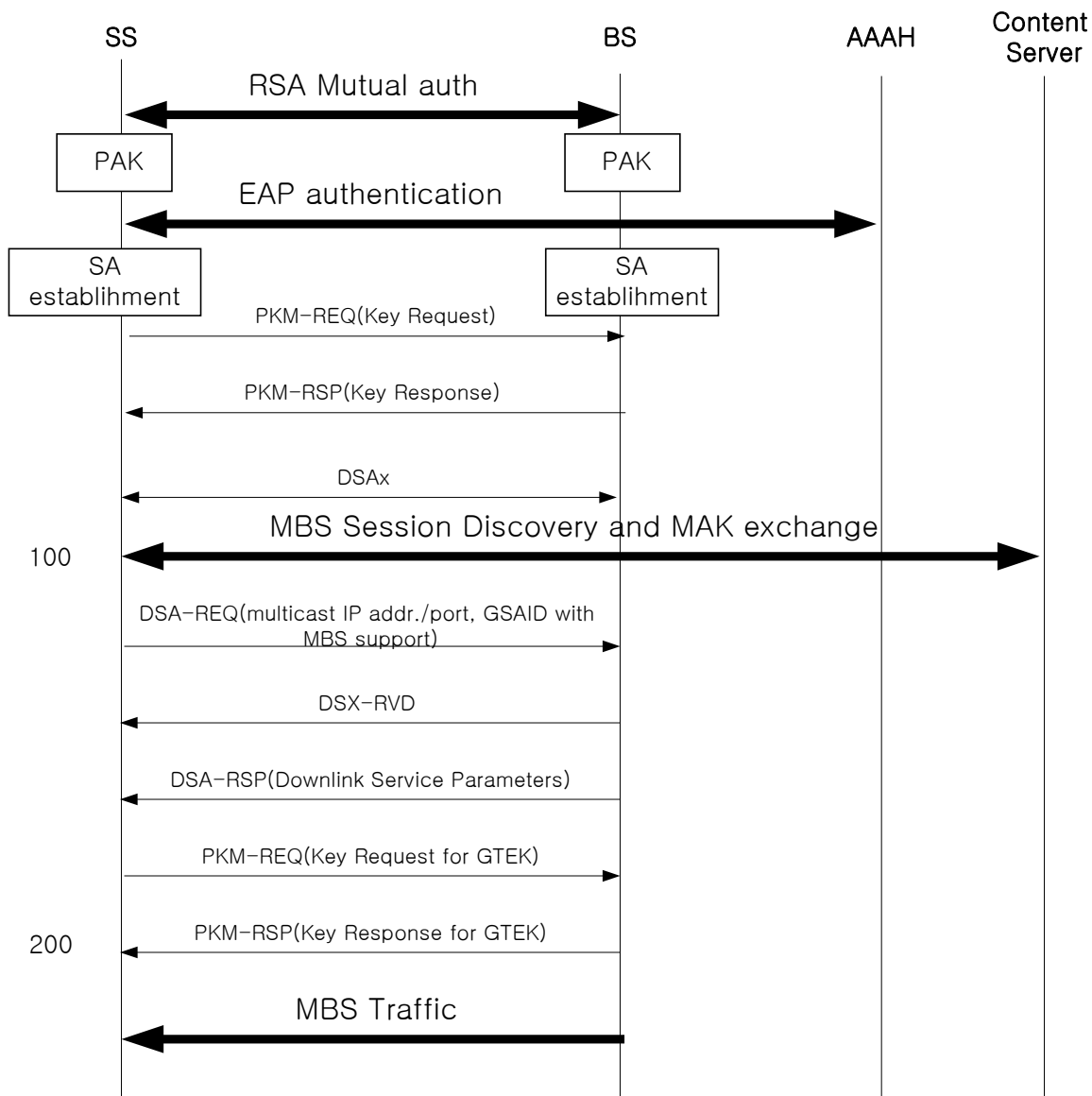
[See Group Security Association]

## **1.2 MBS callflow example**

MSS shall setup traffic connection with RSA mutual authentication and EAP user authentication for MBS session discovery (< step 100)

MSS shall send DSA REQ msg to indicate MBS channel and GSA that has MBS ciphersuits

MSS shall obtain GTEK of requested GSA with MBS support (= step 200)



### 1.3 MBS Data Encryption

Link Layer Data Encryption:

If lower layer encryption is enabled, encryption algorithm **AES-CTR** shall be applied and the MBS Content Encryption (MCE) function shall be in the BS

Application Layer Data Encryption:

If higher layer encryption is enabled, encryption algorithm such as **SRTP [RFC 3711]** shall be applied and the MBS Content Encryption (MCE) function shall be in the MBS content server

## 2 Changes to 802.16e D3 text

[Add section 7.x PKMv2 and add subsection 7.x.x for MBS as follows:]

### 7.x.x MBS (Multimedia Broadcast Service) support

MBS is an efficient and power saving mechanism that requires PKMv2 to send multimedia broadcast information. It provides subscribers with strong protection from thieves of service across broadband wireless mobile network by encrypting broadcast connections between SSs and BSs.

#### 7.x.1 MBS Security associations

In addition to existing three Security Association, MBS requires a MBS Security Association. It is the set of security information that multiple BS and one or more of its client SSs shares but not bind to any MSS connection state in order to support secure and access controlled MBS content reception across the IEEE Std 802.16 network, Each MBS capable MSS may establish a MBS security association during the SS initialization process. MBS SAs shall be provisioned within the BS. A MBS SA's shared information shall include the Cryptographic Suite employed within the SA and key material information such as MAKs (MBS Authorization Key) and GTEKs (Group Traffic Encryption Key). The exact content of the SA is dependent on the SA's Cryptographic Suite. As like any other Unicast SAs, MBS SA is also identified using 16bits SAIDs. Each MSS shall establish one or more MBS SA with its BS.

Using the PKMv2 protocol, an SS receives or establishes an MBS SA's keying material. The BS and MBS content server shall ensure that each client SS only has access to the SAs it is authorized to access.

An SA's keying material [e.g., MAK and GTEK] has a limited lifetime. When the MBS content server or BS delivers MBS SA keying material to an SS, it also provides the SS with that material's remaining lifetime. It is the responsibility of the SS to request new keying material from the MBS server or BS before the set of keying material that the SS currently holds expires at the MBS Server or BS.

#### 7.x.2 MBS Key Management

##### 7.x.2.1 MBS Authorization Key (MAK) establishment

The MAK establishment procedure in MSS and BS is outside of scope of this specification.

##### 7.x.2.2 MBS GTEK establishment

[See GROUP Key Management]

##### 7.x.2.3 MBS Encryption Key establishment

[See PKMv2 Key Management]

#### 7.x.x Cryptographic methods for PKMv2

##### 7.x.x.1 Data Encryption with AES in CTR mode

If the data encryption algorithm identifier in the cryptographic suite of an MBS SA equals 0x80, data on connections associated with that SA shall use the CTR mode of the US Advanced Encryption Standard (AES) algorithm [NIST Special Publication 800-38A, FIPS 197] to encrypt the MAC PDU payloads.

7.x.x.1.1 PDU Payload Format

The PDS payload shall be prepended with a 32/64/128 bits nonce randomly generated by base station. The nonce shall be transmitted in little endian byte order. The nonce shall not be encrypted.

The plaintext PDU shall be encrypted using the active MBS encryption key, according to CTR specification.

The processing yields a payload that is 32/64/128bits longer than the plaintext payload.

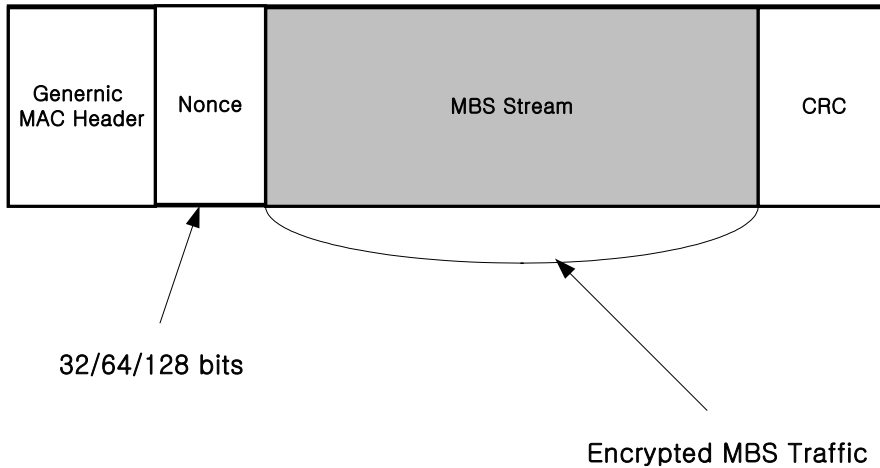


Figure-xxx- MBS MAC PDU Ciphertext Payload Format

11.9.14 Cryptographic suite

Table 287—Data encryption algorithm identifiers

Value	Description
0	No data encryption
1	CBC-Mode 56-bit DES
2	CCM-Mode 128bits AES
127	CTR- Mode 128bits AES for MBS with 32bits Nonce
128	CTR- Mode 128bits AES for MBS with 64bits Nonce
129	CTR- Mode 128bits AES for MBS with 128bits Nonce
2-126 & 130-255	Reserved

Table 288—Data authentication algorithm identifiers

Value	Description
0	No data Authentication
1	CCM-Mode 128bits AES

<u>2-255</u>	<u>Reserved</u>
--------------	-----------------

**Table 332a - Allowed Cryptographic suites**

Value	Description
0x000001	No data encryption, no data authentication & 3-DES, 128
0x010001	CBC-Mode 56-bit DES, no data authentication & 3-DES, 128
0x000002	No data encryption, no data authentication & RSA, 1024
0x020002	CBC-Mode 56-bit DES, no data authentication & RSA, 1024
0x020103	CCM-Mode 128-bit AES, CCM-Mode, 128-bit AES, ECB mode AES with 128-bit key
<u>0x800003</u>	<u>MBS CTR Mode 128bits AES with 32bits nonce, no data authentication, ECB mode AES with 128-bit key</u>
<u>0x810003</u>	<u>MBS CTR Mode 128bits AES with 64bits nonce, no data authentication, ECB mode AES with 128-bit key</u>
<u>0x820003</u>	<u>MBS CTR Mode 128bits AES with 128bits nonce, no data authentication, ECB mode AES with 128-bit key</u>

[ Modify 11.2.18 for AA, MBS and GSA as follows:]

11.2.18 SA Types

Type	Length	Value
24	1	A 1 byte code identifying the value of SA-type as defined in table 304
25	1	A 1 byte code identifying the value of SA-type as defined in table 305

Table 304-SA type attribute values

11.2.18 SA type

~~Description: This attribute identifies the type of SA. Privacy defines three SA types: Primary, Static, Dynamic~~

~~Description: This attribute identifies the type of SA. Privacy defines one AA type and five SA types: Primary, Static, Dynamic, Group and MBS~~

Value	Description
0	Primary
1	Static
2	Dynamic
<u>3</u>	<u>Group</u>

<u>4</u>	<u>MBS</u>
<u>5-127</u>	<u>Reserved</u>
<u>128-255</u>	<u>Vendor-specific</u>

Table 305- Authorization Association Type attribute values

<u>Value</u>	<u>Description</u>
<u>0</u>	<u>Main</u>
<u>1-255</u>	<u>Reserved</u>