Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	Clarification for Authorization Policy	
Date Submitted	**2005-07-21**	
Source(s)	Kyoung-Tae Do Junhyuk Song Jicheol Lee Samsung Electronics Chulsik Yoon Seokheon Cho ETRI Yongmao Li Huawei Technologies	kyeongtae.do@samsung.com junhyuk.song@samsung.com jicheol.lee@samsung.com csyoon@etri.re.kr chosh@etri.re.kr lymao@huawei.com
Re:	IEEE P802.16e/D9	
Abstract	Clarification for Authorization Policy	
Purpose	Clarification for Authorization Policy	
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>.	

Clarification for Authorization Policy

Kyoung-Tae Do, Junhyuk Song, Jicheol Lee (Samsung Electronics)
Chulsik Yoon, Seokheon Cho (ETRI)
Yongmao Li (Huawei Technologies)

1. Problem

In current P802.16e/D9, there is a authorization policy defined between MS and BS in order to select one of combinations of RSA, EAP and Authenticated EAP.

However, MS can not inform BS of capability list of authentication methods which MS supports. Although a MS supports all authentication method combinations (such as RSA only, EAP only, RSA+EAP, EAP+EAP), all that MS can do is just to select one of combination methods with authorization policy in SBC-REQ.

<examples>
MS can support all combination of RSA, EAP, Authenticated EAP.
If MS can not send this information to MS because current authorization policy with all three bit set to 1 is "N/A."

2. Proposed solution

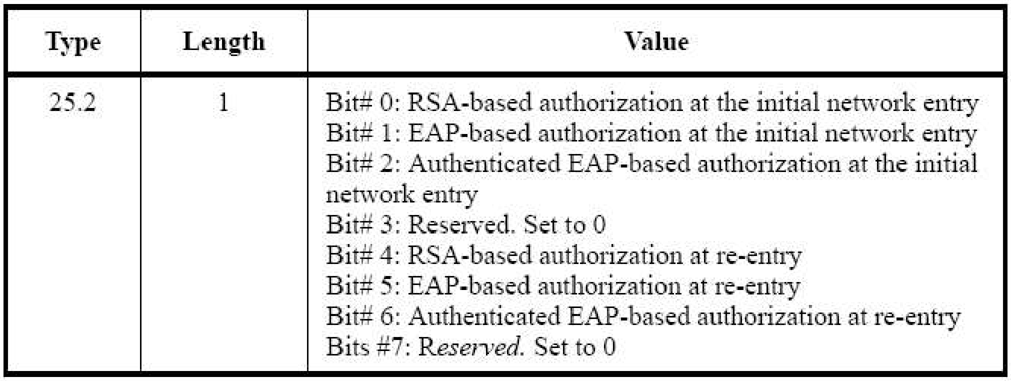
Explain the authorization policy bit representation which is included in SBC-REQ.

3. Proposed Text Changes

[Please modify the section 11.8.4.2 in page 546 as follows:]

11.8.4.2 Authorization policy support

The ‘Authorization policy support’ field indicates authorization policy used by the MS and BS to negotiate and synchronize. A bit value of 0 indicates “not supported” while 1 indicates “supported.”



Type	Length	Value
25.2	1	Bit# 0: RSA-based authorization at the initial network entry Bit# 1: EAP-based authorization at the initial network entry Bit# 2: Authenticated EAP-based authorization at the initial network entry Bit# 3: Reserved. Set to 0 Bit# 4: RSA-based authorization at re-entry Bit# 5: EAP-based authorization at re-entry Bit# 6: Authenticated EAP-based authorization at re-entry Bits #7: R*eserved.* Set to 0

Authenticated EAP-based authorization basically means that a message containing EAP payload is protected by CMAC Digest. The CMAC_KEY_U and CMAC_KEY_D are generated with the EIK obtained from RSA-based authorization or EAP-based authorization.
The PKMv2 Auth-Request/Reply/Reject/Acknowledgement messages shall be used in the RSA-based authorization procedure.
The PKMv2 EAP-Transfer message shall be used in the EAP-based authorization procedure. The PKMv2 Authentication EAP-Transfer message shall be used in the Authenticated EAP-based authorization procedure.
Bit# 4–6 are only applied to the SBC-REQ message. Those bits shall be set to 0 in the SBC-RSP message.
MS and BS will execute the re-authorization procedure according to the authorization policy negotiated in current BS when AK lifetime is expired and so on. After MS moves into another BS, MS and target BS will execute the re-authorization procedure according to the authorization policy of HO re-entry negotiated in the target BS when the lifetime of AK which is negotiated between MS and target BS is expired and so on.
The MS should support at least one authorization policy and inform BS of all supportable authorization policies by the SBC-REQ message. The BS negotiates the authorization policy. If all bits of this attribute included in the SBC-RSP message are 0, then no authorization is applied. Both BS and MS shall not use the authorization function.

~~The following tables shows possible authorization policies at initial network entry.~~
~~The table shows the bit representation of Bit #0~2 and Bit #4~6 of 'Authorization Policy Support' field in SBC-RSP.~~

~~Value~~			~~Description~~	~~Scope~~
~~Bit #0~~	~~Bit #1~~	~~Bit #2~~		
~~0~~	~~0~~	~~0~~	~~No Authorization~~	~~SBC-RSP,~~
~~0~~	~~0~~	~~1~~	~~N/A~~	

Value			Description	Scope
Bit #0 / Bit #4	Bit #1 / Bit #5	Bit #2 / Bit #6		
0	0	0	No authorization (MS cannot support any authorization)	SBC-REQ, PKM-REQ
0	0	1	N/A	
0	1	0	Only EAP-based authorization	
0	1	1	Only EAP-based authorization or authenticated EAP-based authorization after EAP-based authorization	
1	0	0	Only RSA-based authorization	
1	0	1	Only RSA-based authorization or authenticated EAP-based authorization after RSA-based authorization	
1	1	0	Only RSA-based authorization or Only EAP-based authorization or EAP-based authorization after RSA-based authorization	
1	1	1	Only RSA-based authorization or Only EAP-based authorization or EAP-based authorization after RSA-based authorization or authenticated EAP-based authorization after RSA-based authorization or authenticated EAP-based authorization after EAP-based authorization	

~~0~~	~~1~~	~~0~~		~~PKM-RSP~~
~~0~~	~~1~~	~~1~~	~~EAP-based authorization and Authenticated EAP-based authorization~~	
~~1~~	~~0~~	~~0~~	~~RSA-based authorization~~	
~~1~~	~~0~~	~~1~~	~~RSA-based authorization and Authenticated EAP-based authorization~~	
~~1~~	~~1~~	~~0~~	~~RSA-based authorization and Authenticated EAP-based authorization~~	
~~1~~	~~1~~	~~1~~	~~N/A~~	

The following table shows possible authorization policies which MS can support.
The table shows the bit representation of Bit #0~2 and Bit #4 ~ 6 in 'Authorization Policy Support' field in an SBC-REQ and a PKMv2 SA-TEK-Reqeust messages..

The table shows the bit representation of Bit #0~2 in 'Authorization Policy Support' field in an SBC-RSP and a PKMv2 SA-TEK-Response messages..

Value			**Description**	**Scope**
Bit #0	**Bit #1**	**Bit #2**		
0	0	0	No Authorization	SBC-RSP, PKM-RSP
0	0	1	N/A	
0	1	0	Only EAP-based authorization	
0	1	1	~~EAP-based authorization and Authenticated EAP-based authorization~~ Authenticated EAP-based authorization after EAP-based authorization	
1	0	0	Only RSA-based authorization	
1	0	1	~~RSA-based authorization and Authenticated EAP-based authorization~~ Authenticated EAP-based authorization after RSA-based authorization	
1	1	0	~~RSA-based authorization and Authenticated EAP-based authorization~~ EAP-based authorization after RSA-based authorization	
1	1	1	N/A	