

Project	<b>IEEE 802.16 Broadband Wireless Access Working Group</b> < <a href="http://ieee802.org/16">http://ieee802.org/16</a> >	
Title	<b>Authorization Policy Support Negotiation</b>	
Data Submitted	<b>2004-07-15</b>	
Source(s)	Seokheon Cho Chulsik Yoon SungCheol Chang, ETRI	Voice: +82-42-860-5524 Fax: +82-42-861-1966 <a href="mailto:chosh@etri.re.kr">chosh@etri.re.kr</a>
	161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea	
	David Johnston, Intel	
	Phillip Barber, BMT	
	Dongkie Lee, SK Telecom	
	Junhyuk Song, Samsung	
	Young-man, Korea Telecom	
Re:	Security Ad Hoc	
Abstract	PKM version negotiation in the SS basic capabilities negotiation procedure	
Purpose	The document is submitted for review by PKMv2 Working Group and/or by 802.16 Working Group members	
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:chiar@wirelessman.org">mailto:chiar@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> >.	

Authorization Policy Support Negotiation  
*Seokheon Cho, Chulsik Yoon, and SungCheol Chang*

*ETRI*

**David Johnston**

*Intel*

**Phillip Barber**

*BMT*

**Dongkie Lee**

*SK Telecom*

**Junhyuk Song**

*Samsung*

**Young-man Park**

*Korea Telecom*

## Introduction

The PKM version should be negotiated by introducing new PKM version 2.

In addition to the PKM version, since the EAP based authentication was already accepted as an authorization protocol, it is proper that the EAP based authentication as an authorization policy should be allocated

We propose the PKM version and authentication are allocated in the parameter, "Authorization Policy Support," used in the SBC-REQ and SBC-RSP messages. A method of negotiating PKM version and authentication is proposed as follows.

## Proposed changes to IEEE P802.16e/D3-May 2004

### 6.3.2.3.23 SS Basic Capability Request (SBC-REQ) message

*[Change and Insert in 6.3.2.3.23]*

Authorization Policy Support ([see 11.7.8.7](#)) (see 11.3.2.11)

### 6.3.2.3.24 SS Basic Capability Response (SBC-RSP) message

*[Change and Insert in 6.3.2.3.24]*

Authorization Policy Support ([see 11.7.8.7](#)) (see 11.3.2.11)

### 11.3.2.11 Authorization Policy Support

*[Change the table]*

Type	Length	Value	Scope
5.25	1	<del>Bit# 0: IEEE 80.216 essential privacy (Legacy PKM) - default</del> <del>Bit# 1-7: Reserved for open privacy. Set to 0.</del> Bit# 0: RSA Bit# 1: EAP Bit# 2: PHY frame number in authentication tuple Bit# 3: Mutual Auth / Unidirectional Auth Bit# 4: OMAC / HMAC Bit# 5 - 7: Reserved. Set to 0.	<a href="#">REG-REQ</a> SBC-REQ ( <a href="#">see 6.4.2.3.23</a> ) (see 6.3.2.3.23) <del><a href="#">REG-RSP</a></del> SBC-RSP ( <a href="#">see 6.4.2.3.24</a> ) (see 6.3.2.3.24)

### 11.4.2 Common encodings

*[Add to Table 295a]*

**Table 295a-MSS Capability encodings**

Type	Parameters
25	Authorization Policy Support
[TBD]	PKM Version Support

**11.8.3 Authorization Policy Support***[Change the table]*

Type	Length	Value	Scope
5.25	1	<del>Bit# 0: IEEE 80.216 essential privacy (Legacy PKM) — default</del> <del>Bit# 1 - 7: Reserved for open privacy. Set to 0.</del> Bit# 0: RSA Bit# 1: EAP Bit# 2: PHY frame number in authentication tuple Bit# 3: Mutual Auth / Unidirectional Auth Bit# 4: OMAC / HMAC Bit# 5 - 7: Reserved. Set to 0.	<a href="#">REG-REQ</a> SBC-REQ (see 6.4.2.3.23) (see 6.3.2.3.23) <a href="#">REG-RSP</a> SBC-RSP (see 6.4.2.3.24) (see 6.3.2.3.24)

**11.8.4 PKM Version Support***[Add this subsection]*

This field indicates a PKM version. A bit value of 0 indicates “not supported” while 1 indicates “supported.” Both an SS and a BS should negotiate only one PKM version.

Type	Length	Value	Scope
5.[TBD]	1	Bit# 0: PKM version 1 Bit# 1: PKM version 2 Bit# 2 - 7: Reserved. Set to 0.	SBC-REQ (see 6.3.2.3.23) SBC-RSP (see 6.3.2.3.24)