Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Authorization Policy Negotiation in the SS Basic Capability Negotiation Procedure**	
Data Submitted	**2004-01-02**	
Source(s)	Seokheon Cho Ae Soon Park Sun Hwa Lim Young Jin Kim Jee Hwan Ahn ETRI 161, Gajeong-dong,Yuseong-Gu, Daejeon, 305-350, Korea	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr aspark@etri.re.kr
Re:	This is a response to a Call for Comments IEEE 802.16e-03/58 on IEEE 802.16e-03/07r5	
Abstract	The document contains suggestions on the changes in IEEE 802.16e-03/07r5 that would support to negotiate authorization policy between the existing device authentication and the user authentication.	
Purpose	The document is submitted for review by Handoff/Sleep-mode Ad Hoc 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 <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:chiar@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 Policy Negotiation Process in the SS Basic Capability Negotiation Procedure

Seokheon Cho,Ae Soon Park, Sun Hwa Lim, Young Jin Kim, and Jee Hwan Ahn
ETRI

Introduction

The authorization procedure, the PKM protocol, specified by the IEEE 802.16 WirelessMAN Standard has to be necessarily executed to create service flows between SS and BS. An SS' device can be sufficiently authorized through this procedure, but individual users belonging to authorized SS cannot be authenticated by the PKM protocol. Moreover, it is imperative for the IEEE 802.16 system to be backwardly compatible with the current wireless LAN system and to be smoothly roamed with the heterogeneous network. However, the PKM protocol is valid only in the IEEE 802.16 network, because this PKM protocol is private protocol for the device authentication. That is, the device authentication method that the existing authorization policy supports is not appropriate for user authentication. The IEEE 802.16 system has to provide the method of choosing the existing authorization scheme or new authorization scheme accepting authorization protocol framework, in order to be satisfied with above conditions, especially from the aspect of authorization function.

Therefore, we propose a scheme being capable of choosing authorization policy among several authorization frameworks. An SS negotiates with BS on authorization scheme through both the SBC-REQ and SBC-RSP messages, before the authorization procedure is actually performed. For instance, an SS shall negotiate with BS on authorization policy between the existing device authentication and user authentication. The parameter about authorization policy should be included in those messages as a TLV. An SS notifies whole supportable authorization policy through the SBC-REQ message. Upon reception of this message, BS chooses only one authorization policy and returns the decision back to the SS in the SBC-RSP message. Both the SS and BS use the selected authorization policy from the SS basic capabilities negotiation process. If the parameter about authorization policy is omitted in either SBC-REQ or SBC-RSP message, both of them shall use the existing device authentication. On the contrary, if user authentication or device-user authentication scheme is accepted as the authorization policy, they should negotiate the authorization protocol which is used for user authentication. After all, the IEEE 802.16 authorization function can support more flexible authorization policy, by adding new parameters in both SBC-REQ and SBC-RSP messages.

Proposed changes to IEEE 802.16-REVd/D1-2003

6.4.2.3.23 SS Basic Capability Request (SBC-REQ) message
[Insert at the end of 6.4.2.3.23]

Authorization Policy Support (see 11.4.2.11)
User Authentication Suite (see 11.4.2.12)

6.4.2.3.24 SS Basic Capability Response (SBC-RSP) message
[Insert at the end of the comment "Bandwidth Allocation Support (see 11.4.2.6)" of 6.4.2.3.24]

Authorization Policy Support (see 11.4.2.11)
User Authentication Suite (see 11.4.2.12)

11.4.2 SS Capabilities encoding
[Add to Table 306]

Table 306-SS Capability encodings

Type	Parameters
5.25	Authorization Policy Support
5.26	User Authentication Suite

11.4.2.11 Authorization Policy Support
[Add this section]

This field indicates authorization policy that both SS and BS need to negotiate and synchronize. A bit value of 0 indicates "not supported" while 1 indicates "supported." In case of choosing device authentication, both SS and BS shall use the essential privacy method constituting X.509 digital certificates and the RSA public-key encryption algorithm. If this field is omitted, then both SS and BS shall perform only device authentication as the authorization procedure.

Type	Length	Value	Scope

5.25	1	Bit# 0: Device authentication Bit# 1: User authentication Bit# 2: Device-user authentication Bit# 3-7: Reserved. Set to 0	SBC-REQ (see 6.4.2.3.23) SBC-RSP (see 6.4.2.3.24)

11.4.2.12 User Authentication Suite
[Add this section]

This field indicates user authentication protocol that both SS and BS need to negotiate and synchronize. This field is defined only if user authentication or device-user authentication is used as authorization policy.

Type	Length	Value	Scope
5.26	1	Bit# 0: EAP-TLS Bit# 1: EAP-TTLS Bit# 2-7: Reserved	SBC-REQ (see 6.4.2.3.23) SBC-RSP (see 6.4.2.3.24)