Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Security Negotiation Parameters in the SBC-REQ/RSP Procedure**	
Data Submitted	**2005-03-16**	
Source(s)	Seokheon Cho Taeyong Lee Sunhwa Lim Chulsik Yoon ETRI Sanjay Bakshi, Yigal Eliaspur, Intel Corporation Junhyuk Song, Jicheol Lee Samsung	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr
Re:	IEEE P802.16e/D6	
Abstract	The document contains suggestions on the changes into IEEE 802.16e/D6 that would provide privacy capabilities parameters to negotiate between a MS and the BS.	
Purpose	Adoption of proposed changes into P802.16e/D6	
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>.	

Security Negotiation Parameters in the SBC-REQ/RSP Procedure

Seokheon Cho, Taeyong Lee, Sunhwa Lim, and Chulsik Yoon
ETRI

Sanjay Bakshi and Yigal Eliaspur
Intel Corporation

Junhyuk Song and Jicheol Lee
Samsung

Introduction

Both MS and BS shall negotiate the authorization policy by using the Authorization Policy Support field. Both of them shall also know message authentication code mode, e.g. selecting one of OMAC and HMAC from the Authorization Policy Support field. However, the negotiation of message authentication code mode should be performed by other field that is independent from the Authorization Policy Support field, since the message authentication code mode level is lower than the authorization key level obtained through the authorization procedure.

In addition, there are two modes related to the EAP, e.g. EAP transfer mode and Authenticated EAP transfer mode.

It is necessary to make a filed to contain parameters related to privacy capabilities.

This contribution proposed a way to solve the above problems.

Proposed changes to IEEE 802.16e/D6

6.3.2.3.23 MS Basic Capability Request (SBC-REQ) message

[Insert at the end of 6.3.2.3.23:]

Security Negotiation Parameters (see 11.8.4)
~~**Authorization Policy Support (see 11.8.4)**~~

6.3.2.3.24 MS Basic Capability Response (SBC-RSP) message

[Insert at the end of 6.3.2.3.24:]

Security Negotiation Parameters (see 11.8.4)
~~**Authorization Policy Support (see 11.8.4)**~~

[Change sub-clauses 11.8.4 - 11.8.6 as follows]

11.8.4 Security Negotiation Parameters

This field is a compound attribute indicating security capabilities to negotiate before performing the initial authorization procedure and the reauthorization procedure.

Type	Length	Value (compound)	Scope
25	Variable	The compound field contains the sub-attributes as defined in Table xxx.	SBC-REQ SBC-RSP

Attribute	Contents
PKM Version Support	Version of privacy sublayer supported
Authorization Policy Support	Authorization policy to support
Message Authentication Code Mode	Message authentication code to support
PN Window Size	Size capability of the receiver PN window per SAID

~~11.8.5~~ 11.8.4.1 PKM Version Support

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~~
~~26~~ 25.1	1	Bit# 0: PKM version 1 Bit# 1: PKM version 2 Bit# 2-7: Reserved. Set to 0	~~SBC-REQ~~ ~~SBC-RSP~~

~~11.8.4~~ 11.8.4.2 Authorization Policy Support

This 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	~~Scope~~
~~5.25~~ 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: OMAC supported (if set to 0, HMAC is the default)~~ 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 Bit# ~~3~~ 7: Reserved. Set to 0	~~SBC-REQ~~ ~~SBC-RSP~~

Authenticated EAP-based authorization basically means that a message containing EAP payload is protected by OMAC Digest. The OMAC_KEY_U and OMAC_KEY_D are generated with the EIK obtained from RSA-based authorization or EAP-based authorization.

Bit# 4 – 6 are only applied to the SBC-REQ message. Those bits shall be set to 0 in the SBC-RSP message.

11.8.4.3 Message Authentication Code Mode

This field indicates a MAC (Message Authentication Code) mode that MS supports. Both MS and BS shall determine and use a MAC mode. A bit value of 0 indicates "not supported" while 1 indicates "supported." If this attribute is not present, only HMAC is supported.

Type	Length	Value
25.3	1	Bit# 0: HMAC Bit# 1: OMAC Bit# 2: 64-bit short-HMAC* Bit# 3: 80-bit short-HMAC* Bit# 4: 96-bit short-HMAC* Bit# 5-7: Reserved. Set to 0

* Note: If the short-HMAC mode is selected, then the short-HMAC tuple shall be applied to the following messages: MOB_SLP-REQ/RSP, MOB_SCAN-REQ/RSP, MOB_MSHO-REQ, MOB_BSHO-REQ/RSP, MOB_HO-IND, RNG-REQ/RSP. Otherwise, the HMAC tuple shall be applied.

~~11.8.6~~ 11.8.4.4 PN Window Size

Specifies the size capability of the receiver PN window per SAID. The receiver shall track PNs within this window to prevent replay attacks (see 7.5.1.2.4).

Type	Length	Value	~~Scope~~
~~44.~~ 25.4	2	PN Window Size in PNs	~~SBC-REQ, SBC-RSP~~

[Change one row in Table 368 in the section 11.9 as follows]
11.9 PKM-REQ/RSP management message encodings

Table 368-PKM attributes types

Type	~~PKM attribute~~
22	~~Version~~ reserved

[Change the sub-clause 11.9.13 as follows]
11.9.13 Security capabilities

Description: The Security-Capabilities attribute contains ~~is a compound attribute whose subattributes identify the version of PKM an SS supports and~~ the cryptographic suite(s) an SS supports.

Type	Length	Value (compound)
19	Variable	The Compound field contains the subattributes as defined in Table 372.

Table 372-Security-capabilities subattributes

Attribute	Contents
Cryptographic-Suite-List	List of supported cryptographic suites
~~Version~~	~~Version of Privacy supported~~

[Delete the sub-clause 11.9.16]

~~11.9.16 Version~~

~~Table 372-Security-capabilities subattributes~~

~~Value~~	~~Description~~
~~0~~	~~Reserved~~
~~1~~	~~PKM(Initial statndard release)~~
~~2-255~~	~~Reserved~~

~~Type~~	~~Length~~	~~Value (compound)~~
~~22~~	~~1~~	~~A 1-byte code identifying a version of PKM security as defined in Table 377.~~