Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	Clarification for Authorization Policy
Date Submitted	**2005-07-14**
Source(s)	Junhyuk Song junhyuk.song@samsung.com Jicheol Lee jicheol.lee@samsung.com Samsung Electronics
Re:	IEEE P802.16e/D9
Abstract	Remedy of EAP-in-EAP mode Authentication
Purpose	Adopt this contribution as a remedy of EAP-in-EAP mode
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

Junhyuk Song (junhyuk.song@samsung.com)
Jicheol Lee (Jicheol.lee@samsung.com)
Samsung Electronics

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 many 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>
Case 1: MS can support “EAP only and RSA only”.
If MS sends SBC REQ with authorization policy set to (bit0 = 1, bit1 = 1, bit2 = 0), the BS perceive the MS supporting “RSA+EAP” authentication. In this case, MS can not show which methods MS support actually.

Case 2: 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

In SBC-REQ message, MS send with “authorization capability list” to BS
In SBC-RSP message, BS send with current Authorization Policy to MS.

So, we introduce “authorization capability” including capability list for combinations of authentication method as following:

Type	Length	Value
25.x	1	Bit#0 : No authorization Bit#1 : RSA only authorization Bit#2 : EAP only authorization Bit#3 : EAP after RSA authorization Bit#4 : Authenticated EAP after RSA authorization Bit#5 : Authenticated EAP after EAP authorization Bit#6 : Reserved Bit#7 : Reserved

3. Proposed Text Changes

[Insert the highlighted blue text into the table of page 536 of P802.16e/D8 as follows]

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

[Insert the following subsection section 7.8.4.2 in page 536 of P802.16e/D9]

11.8.4.2 Authorization capability

In initial network entry, MS must include this authorization capability TLV in SBC-REQ.

Type	Length	Value	Scope
25.x	1	Bit#0 : No authorization Bit#1 : RSA only authorization Bit#2 : EAP only authorization Bit#3 : EAP after RSA authorization Bit#4 : Authenticated EAP after RSA authorization Bit#5 : Authenticated EAP after EAP authorization Bit#6 : Reserved Bit#7 : Reserved	SBC-REQ

If a bit is set to 1, it means that MS support the authentication or the sequential combination of methods. MS must set at least one bit.

[Change the following subsection 7.8.4.2 in page 537 of P802.16e/D9]

11.8.4.~~2~~ 3 Authorization policy support

The 'Authorization policy support' field indicates authorization policy ~~used by the MS and BS to negotiate and synchronize.~~that BS selects for the MS. A bit value of 0 indicates "not supported" while 1 indicates "supported."

Authenticated EAP-based authorization basically means that a message containing EAP payload is protected by CMAC Digest. The OMAC_KEY_U and OMAC_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.

Type	Length	Value	Scope
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: Reserved. Set to 0	SBC-REQ

The MS should support at least one authorization policy and inform BS of all supportable authorization policies by the SBC-REQ message with 'authorization capability'. 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.

[Modify subsection number properly from 11.8.4.3 and 11.8.4.4 of P802.16e/D9]

11.8.4.~~3~~4 MAC (Message Authentication Code) Mode
11.8.4.~~4~~5 PN window size