Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**The Enhancement For Authorization Policy Negotiation In SBC Exchange**
Date Submitted	**2005-05-05**
Source(s)	Li Rui, Tian Feng, Chen JianYong, Zhao Jie, Li YuanWei Voice: [86-0755-26772016] Fax: [86-0755-26772004] [mailto:li.rui2@zte.com.cn] ZTE corporation ZTE Plaza , Keji Road South , Hi-tech Industrial Park , Nanshan District , Shenzhen , P.R.China , 518057 Seokheon Cho and Sungcheol Chang ETRI
Re:	Response to Sponsor Ballot on IEEE802.16e/D7 document
Abstract	This contribution describes the enhancement of authorization policy negotiation in SBC exchange.
Purpose	To incorporate the text changes proposed in this contribution into the 802.16e/D8 draft.
Notice	
Release	
Patent Policy and Procedures	

The Enhancement For Authorization Policy Negotiation In SBC Exchange

Li Rui, Tian Feng, Chen JianYong, Zhao Jie, Li YuanWei
ZTE corporation
Seokheon Cho and Sungcheol Chang
ETRI

1. Problem Statement

The authorization policies for initial network entry and re-entry are negotiated between MS and BS in the SBC exchange in current P802.16e/D7. But the re-authorization policy is not negotiated between MS and BS in current specification. MS and BS need to execute re-authorization procedure during the re-entry network. But re-authorization procedure between MS and BS will be taken place in some other cases besides the re-entry. MS will execute the authorization procedure according to the authorization policy negotiated in SBC exchange when MS is in re-entry network, such as in handover or in the new connection with BS. What is the re-authorization policy and how to execute re-authorization when the AK lifetime is expired or H/OMAC_PN_U is overflowing or H/OMAC_PN_D is overflowing?

2. Proposed solutions

We suggest that the authorization policy negotiation for re-entry in SBC exchange shall be changed to the authorization policy negotiation for re-authorization.

3. Specific text changes

=== Start text changes ====

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
25.1	1	Bit #0: PKM version 1 Bit #1: PKM version 2 Bit #2-7: R*eserved.* Set to 0

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 HO re-entry Bit# 5: EAP-based authorization at HO re-entry Bit# 6: Authenticated EAP-based authorization at HO re-entry Bits #7: R*eserved.* Set to 0

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.

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.

=== End text changes ====

4. References

[1] IEEE Standard 802.16e/D7-2004
[2] IEEE Standard 802.16-2004