Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Security Capabilities Confirmation**	
Date Submitted	**2005-06-15**	
Source(s)	Haixiang He Nortel 600 Technology Park Drive Billerica, MA 01821 USA	Voice: [+1 978-288-7482] Fax: [+1 978-288-0620] [mailto: haixiang@nortel.com]
Re:	Response to Sponsor Ballot on IEEE802.16e/D8 document	
Abstract	This contribution proposes a mechanism to securely confirm the negotiated security capabilities.	
Purpose	To incorporate the text changes proposed in this contribution into the 802.16e/D9 draft.	
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>.	

Security Capabilities Confirmation

Haixiang He

Nortel

1. Problem Statement

During the IETF EAP review, one issue was raised. According to http://www.drizzle.com/~aboba/EAP/review.txt , the issue is:

```
“6. Secure Ciphersuite Negotiation

[AAAKEY] states:

"         The selection of the "best" ciphersuite MUST be securely
          confirmed.  The mechanism MUST detect attempted roll back
          attacks."

IEEE 802.16e securely confirms selection of the "best" ciphersuite
within the 3-way handshake, but it does not securely confirm other
"security-relevant" capabilities such as the MAC algorithm or
replay window size.”
```

This contribution proposes a mechanism to securely confirm the secure capabilities negotiated during SBC-REQ/RSP so that roll back attacks or downgrade attacks can be prevented.

2. Proposed solutions

Add “Security Negotiation Parameters” as new attribute to message SA-TEK-Request and SA-TEK-Response. Both BS and MS verify the security capabilities exchanged during 3-way handshake against the security capabilities negotiated during the SBC-REQ/RSP. If the security capabilities don’t match, the BS and MS should log the identified problems. The BS and MS may continue the communication using security capabilities negotiated during the 3-way handshake.

3. Specific text changes

=== Start text changes ====

6.3.2.3.9.18 SA-TEK-Request message

[Replace the table 37h with following new table]

Table 37h—SA-TEK-Request message attributes

Attribute	Contents
NonceMS	A 64-bit number chosen by the MS (once per protocol run). This can be a counter or a random number.
RandomBS	The 64-bit random number from the SA Challenge

AKID	This identifies the AK to the BS that was used for protecting this message
Security Negotiation Parameters	Describes requesting MS's security capabilities (see 11.8.4)
CMAC/HMAC	Message integrity code of this message

6.3.2.3.9.19 SA-TEK-Response message

[Replace the table 37i with following new table]

Table 37i—SA-TEK-Reponse message attributes

Attribute	Contents
NonceMS	The number received from the MS
BS_Random	The random number included in the SA-TEK-Challenge message or SA-Challenge TLV.
AKID	This identifies the AK to the MS that was used for protecting this message.
Security Negotiation Parameters	Describes requesting MS's security capabilities (see 11.8.4)
SA_TEK_Update	A compound TLV list each of which specifies an SA identifier (SAID) and additional properties of the SA that the MS is authorized to access. This compound field may be present at the reentry. Additionally, in case of HO, for each active SA in previous serving BS, corresponding TEK, GTEK and GKEK parameters are also included.
CMAC/HMAC	Message integrity code of this message

6.3.2.3.23 SS basic capability request (SBC-REQ) message

[Insert at the end of 6.3.2.3.23:]
Security Negotiation Parameters (see ~~11.8.7~~ 11.8.4)

6.3.2.3.24 SS basic capability response (SBC-RSP) message

[Insert at the end of 6.3.2.3.24:]
Security Negotiation Parameters (see ~~11.8.7~~ 11.8.4)

7.8.1 SA-TEK 3-way handshake

[Add at the end of step 3]

The MS must include, through the Security Negotiation Parameters attribute, the security capabilities that it includes in SBC-REQ message during the basic capabilities negotiation phase.

[Add at the end of step 4]

In addition, the BS must verify the MS's security capabilities encoded in the Security Negotiation Parameters attribute against the security capabilities provided by the MS through the SBC-REG message. If security capabilities don't match, the MS should log the problem and the differences of the security capabilities. The BS may choose to continue the communication with the MS. In this case, the BS should redo the security negotiation based on the security capabilities provided in SA-TEK-Request message and return the negotiated security capabilities in SA-TEK-Response message through the Security Negotiation Parameters attribute.

[Add at the end of step 5]

In addition, the BS must include, through the Security Negotiation Parameters attribute, the security capabilities that it includes in SBC-RSP message during the basic capabilities negotiation phase. In the case that security capabilities mismatch were found and the BS decides to continue the communication with the MS, the BS must include the newly negotiated security capabilities.

[Add at the end of step 6]

The MS also must verify the BS's security capabilities encoded in the Security Negotiation Parameters attribute against the security capabilities provided by the BS through the SBC-RSP message. If security capabilities don't match, the MS should log the problem and the differences of the security capabilities. The MS may choose to continue the communication with the BS. In this case, the MS should adopt the security capabilities encoded in SA-TEK-Response message.

11.8.4 Security Negotiation Parameters

[Replace the corresponding table with the following new table]

Type	Length	Value	Scope
25	Variable	The compound field contains the sub-attributes as defined in Table xxx.	SBC-REQ, SBC-RSP SA-TEK-Request, SA-TEK-Response

[Label the corresponding table and replace the "xxx" in the above "value" field with the correct label]

=== End text changes ====

4. References

[1] IEEE Standard 802.16e/D8-2005

[2] IEEE Standard 802.16-2004