

Project	IEEE 802.16 Broadband Wireless Access Working Group < <a href="http://ieee802.org/16">http://ieee802.org/16</a> >
Title	Editorial corrections for security parameters for consideration of the IEEE 802.16 Maintenance process
Date Submitted	2006-09-22
Source(s)	Dave Maas <a href="mailto:david.maas@motorola.com">david.maas@motorola.com</a> Mark Cudak <a href="mailto:mark.cudak@motorola.com">mark.cudak@motorola.com</a>  Motorola
Re:	IEEE Maintenance Project
Abstract	Three security parameters that had REG-REQ/RSP scope in 802.16-2004 were moved to SBC-REQ/RSP scope in Cor1, but it is not clear after the Cor1/802.16e merge what the correct new elements are in 802.16-2005. This contribution contains corrections to the affected sections to accompany comments submitted to MTG 802.16 Maintenance process
Purpose	Discuss and adopt
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 < <a href="http://ieee802.org/16/ipr/patents/policy.html">http://ieee802.org/16/ipr/patents/policy.html</a> >, 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 < <a href="mailto:chair@wirelessman.org">mailto:chair@wirelessman.org</a> > 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 < <a href="http://ieee802.org/16/ipr/patents/notices">http://ieee802.org/16/ipr/patents/notices</a> >.

### 6.3.2.3.23 SS basic capability request (SBC-REQ) message

<< Change section numbers as shown below, with strikethrough showing the old section number and red text showing the new section number >>

**PKM flow control** (see ~~11.7.8.6~~ 11.8.9)

**Authorization policy support** (see 11.8.4.2)

**Maximum number of supported security association** (see ~~11.7.8.8~~ 11.8.10)

### 6.3.2.3.23 SS basic capability response (SBC-RSP) message

<< Change section numbers as shown below, with strikethrough showing the old section number and red text showing the new section number >>

**PKM flow control** (see ~~11.8.4~~ 11.8.9)

**Authorization policy support** (see ~~11.8.5~~ 11.8.4.2)

**Maximum number of supported security association** (see ~~11.8.6~~ 11.8.10)

## 11.7.8 SS Capabilities encodings

<< Delete text shown in strikethrough >>

~~**Delete 11.7.8.3 MAC CRC support.**~~

~~**Change 11.7.8.6 to 11.8.4 and change its scope to SBC-REQ SBC-RSP.**~~

~~**Change 11.7.8.7 to 11.8.5, change its scope to SBC-REQ SBC-RSP and change the first paragraph as indicated:**~~

~~**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.” If this field is omitted, then both SS and BS shall use the IEEE 802.16 security, constituting X.509 digital certificates and the RSA public key encryption algorithm, as authorization policy. If this field is present and equal to 0, PKM shall be considered disabled.**~~

~~**Change 11.7.8.8 to 11.8.6 and change its scope to SBC-REQ SBC-RSP**~~

### 11.7.8.3 MAC CRC Support

This TLV has been deleted.

### 11.7.8.6 PKM Flow Control

This TLV has been moved in scope to SBC-REQ/RSP and can now be found at section 11.8.9.

#### 11.7.8.7 Authorization Policy Support

This TLV has been moved in scope to SBC-REQ/RSP under the 'Security Negotiation Parameters' compound TLV and can now be found at section 11.8.4.2.

#### 11.7.8.8 Maximum number of supported security associations

This TLV has been moved in scope to SBC-REQ/RSP and can now be found at section 11.8.10.

**<< The remaining text in 11.7.8 is unchanged. >>**

### 11.8

**<< At the end of 11.8: >>**

***Insert new subclause 11.8.9:***

#### 11.8.9 PKM Flow Control

This field specifies the maximum number of concurrent PKM transactions that may be outstanding.

Type	Length	Value	Scope
15	1	0 indicates no limit (default) 1–255 indicate maximum concurrent transactions	SBC-REQ SBC-RSP

***Insert new subclause 11.8.10:***

#### 11.8.10 Maximum number of supported security associations

This field specifies the maximum number of supported security association of the SS.

Type	Length	Value	Scope
17	1	Maximum number of security association supported by the SS (default = 1)	SBC-REQ SBC-RSP

**<< The remaining text in 11.8 is unchanged. >>**

#### 12.1.1.4.7 REG-REQ

**<< Delete text shown in strikethrough >>**

~~— PKM Flow Control (default = no limit)~~