Project	IEEE 802.16 Broadband Wireless Access Working Group <**http://ieee802.org/16**>
Title	Editorial corrections for security parameters for consideration of the IEEE 802.16 Maintenance process
Date Submitted	2006-09-22
Source(s)	Dave Maas david.maas@motorola.com Mark Cudak mark.cudak@motorola.com 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	
Release	
Patent Policy and Procedures	

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)~~