Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Proposal for Adding BS SecurityManagementFunction Attributes**
Date Submitted	**2006-03-06**
Source(s)	Zou Lan Wu Jian Jun Huawei Technologies. No.98,Lane91, Eshan Road, Pudong , Shanghai, China Pudong Lujiazui Software Park Voice: +86-21-68644808-24657 Fax: +86-21-50898375 Mailto: zlan@huawei.com
Re:	Contribution to IEEE 802.16i
Abstract	This contribution proposed to add BS security management information model attributes.
Purpose	Adoption
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>.

Proposal for Adding BS SecurityManagementFunction Attributes

Huawei Technologies.

Introduction

With mobility feature is introduced into WiMAX system, PKMV2 mechanism is adopted in 16e. This contribution proposes to add BS security management related configuration attributes to the current standard.

Proposed Text

15.1.2.3.5 IOC SecurityManagmentFunction
15.1.2.3.5.1 Definition
This IOC represents a SecurityManagmentFunction object. It is derived from ManagedFunction.
15.1.2.3.5.2 Attributes

Attributes of `SecurityManagmentFunction`

Attribute name	Visibility	Support Qualifier	Read Qualifier	Write Qualifier

15.1.2.3.6 IOC PkmBase
15.1.2.3.6.1 Definition
This IOC represents a PkmBase object. It is derived from ManagedFunction.
15.1.2.3.6.2 Attributes

Attributes of `PkmBase`

Attribute name	Visibility	Support Qualifier	Read Qualifier	Write Qualifier
wmanIfBsPkmDefaultAuthLifetime	+	M	M	M
wmanIfBsPkmDefaultTekLifetime	+	M	M	M
wmanIfBsPkmDefaultSelfSigManufCertTrust	+	M	M	M
wmanIfBsPkmCheckCertValidityPeriods	+	M	M	M
wmanIfBsPMKDefaultPreHandshakeLifetime	+	M	M	M
wmanIfBsPMKDefaultLifetime	+	M	M	M
wmanIfBsDefaultSAChallengeTimer	+	M	M	M
wmanIfBsDefaultSaChallengeMaxResends	+	M	M	M
wmanIfBsDefaultSATEKTimer	+	M	M	M
wmanIfBsDefaultSATEKRequestMaxResends	+	M	M	M

15.1.2.3.7 IOC PkmTek
15.1.2.3.7.1 Definition

This IOC represents a PkmTek object. It is derived from ManagedFunction.

15.1.2.3.7.2 Attributes

Attributes of PkmTek

Attribute name	Visibility	Support Qualifier	Read Qualifier	Write Qualifier
wmanIfBsPkmTekSAId	+	M	-	-
wmanIfBsPkmTekSAType	+	M	M	-
wmanIfBsPkmTekDataEncryptAlg	+	M	M	-
wmanIfBsPkmTekDataAuthentAlg	+	M	M	-
wmanIfBsPkmTekEncryptAlg	+	M	M	-
wmanIfBsPkmTekLifetime	+	M	M	-
wmanIfBsPkmTekKeySequenceNumber	+	M	M	-
wmanIfBsPkmTekExpiresOld	+	M	M	-
wmanIfBsPkmTekExpiresNew	+	M	M	-
wmanIfBsPkmTekReset	+	M	M	M
wmanIfBsPkmAssociatedGKEKSequenceNumber	+	M	M	-
wmanIfBsPkmSAServiceType	+	M	M	-

15.1.2.3.8 IOC MS/SSPkmAuth

15.1.2.3.8.1 Definition

This IOC represents a MS/SSPkmAuth object. It is derived from ManagedFunction.

15.1.2.3.8.2 Attributes

Attributes of MSPkmAuth

Attribute name	Visibility	Support Qualifier	Read Qualifier	Write Qualifier
wmanIfBsSsPkmAuthMacAddress	-	M	-	-
wmanIfBsSsPkmAuthKeySequenceNumber	+	M	M	-
wmanIfBsSsPkmAuthExpiresOld	+	M	M	-
wmanIfBsSsPkmAuthExpiresNew	+	M	M	-
wmanIfBsSsPkmAuthLifetime	+	M	M	-
wmanIfBsSsPkmAuthReset	+	M	M	M
wmanIfBsSsPkmAuthPrimarySAId	+	M	M	-
wmanIfBsSsPkmAuthValidStatus	+	M	M	-
wmanIfBsMsCMACPacketNumbercounter	+	M	M	
wmanIfBsMsCMAC_PN_UL	+	M	M	
wmanIfBsMsCMAC_PN_DL	+	M	M	
wmanIfBsMsCMACValue	+	M	M	
wmanIfBsMsPkmAuthResultCode	+	M	M	
wmanIfBsMsPkmAKId	+	M	M	
wmanIfBsKeyPushMode	+	M	M	
wmanIfBsKeyPushCounter	+	M	M	

Appending following description into section 15.1.2.6.1 Definition and legal values:

Attribute Name	Definition	Legal Values
wmanIfBsPkmDefaultAuthLifetime	The value of this object is the default lifetime, in seconds, the BS assigns to a new authorization key.	
wmanIfBsPkmDefaultTekLifetime	The value of this object is the default lifetime, in seconds, the BS assigns to a new Traffic Encryption Key(TEK).	
wmanIfBsPkmDefaultSelfSigManufCertTrust	This object determines the default trust of all (new) self-signed manufacturer certificates obtained after setting the object.	trusted (1), untrusted (2)

wmanIfBsPkmCheckCertValidityPeriods	Setting this object to TRUE causes all certificates received thereafter to have their validity periods (and their chain's validity periods) checked against the current time of day. A FALSE setting will cause all certificates received Thereafter to not have their validity periods (nor their chain's validity periods) checked against the current time of day.	TRUE FALSE
wmanIfBsPMKDefaultPreHandshakeLifetime	The lifetime assigned to PMK when created	
wmanIfBsPMKDefaultLifetime	If MSK lifetime is unspecified (i.e. by AAA server), PMK lifetime shall be set to this value.(in seconds)	
wmanIfBsDefaultSAChallengeTimer	Time prior to re-send of SA-TEK-Challenge (in seconds)	
wmanIfBsDefaultSaChallengeMaxResends	Maximum number of transmissions of SATEK-Challenge	
wmanIfBsDefaultSATEKTimer	Time prior to re-send of SA-TEK-Request (in seconds)	
wmanIfBsDefaultSATEKRequestMaxResends	Maximum number of transmissions of SATEK-Request	
wmanIfBsPkmTekSAId	The value of this object is the Security Association ID (SAID).	
wmanIfBsPkmTekSAType	The value of this object is the type of security association. Dynamic does not apply to SSs running in PKM mode.	primarySA(0), staticSA(1), dynamicSA(2)
wmanIfBsPkmTekDataEncryptAlg	The value of this object is the data encryption algorithm being utilized.	
wmanIfBsPkmTekDataAuthentAlg	The value of this object is the data authentication algorithm being utilized.	
wmanIfBsPkmTekEncryptAlg	The value of this object is the TEK key encryption algorithm being utilized.	
wmanIfBsPkmTekLifetime	The value of this object is the lifetime, in seconds, the BS assigns to keys for this TEK association.	
wmanIfBsPkmTekKeySequenceNumber	The value of this object is the most recent TEK key sequence number for this SAID.	
wmanIfBsPkmTekExpiresOld	The value of this object is the actual clock time for expiration of the immediate predecessor of the most recent TEK for this FSM. If this FSM has only one TEK, then the value is the time of activation of this FSM.	
wmanIfBsPkmTekExpiresNew	The value of this object is the actual clock time for expiration of the most recent TEK for this FSM.	
wmanIfBsPkmTekReset	Setting this object to TRUE causes the BS to invalidate the current active TEK(s) (plural due to key transition periods), and to generate a new TEK for the associated SAID; the BS MAY also generate an unsolicited TEK Invalid message, to optimize the TEK synchronization between the BS and the SS. Reading this object always returns FALSE.	TRUE FALSE
wmanIfBsPkmAssociatedGKEKSequenceNumber	Associated GKEK sequence number with this TEK-Parameters	
wmanIfBsPkmSAServiceType	This attribute indicates service types of the corresponding SA type.	0: Unicast service 1: Group multicast service 2: MBS service 3-255: Reserved.

wmanIfBsSsPkmAuthMacAddress	The value of this object is the physical address of the SS to which the authorization association applies.	
wmanIfBsSsPkmAuthKeySequenceNumber	The value of this object is the most recent authorization key sequence number for this SS.	
wmanIfBsSsPkmAuthExpiresOld	The value of this object is the actual clock time for expiration of the immediate predecessor of the most recent authorization key for this FSM. If this FSM has only one authorization key, then the value is the time of activation of this FSM.	
wmanIfBsSsPkmAuthExpiresNew	The value of this object is the actual clock time for expiration of the most recent authorization key for this FSM	
wmanIfBsSsPkmAuthLifetime	The vaue of this object is the lifetime, in seconds, the BS assigns to an authorization key for this SS.	
wmanIfBsSsPkmAuthReset	Setting this object to invalidateAuth(2) causes the BS to invalidate the current SS authorization key(s), but not to transmit an Authorization Invalid message nor to invalidate unicast TEKs. Setting this object to sendAuthInvalid(3) causes the BS to invalidate the current SS authorization key(s), and to transmit an Authorization Invalid message to the SS, but not to invalidate unicast TEKs. Setting this object to invalidateTeks(4) causes the BS to invalidate the current SS authorization key(s), to transmit an Authorization Invalid message to the SS, and to invalidate all unicast TEKs associated with this SS authorization. Reading this object returns the most-recently-set value of this object, or returns noResetRequested(1) if the object has not been set since the last BS reboot.	noResetRequested(1), invalidateAuth(2), sendAuthInvalid(3), invalidateTeks(4)
wmanIfBsSsPkmAuthPrimarySAId	The value of this object is the Primary Security Association identifier.	
wmanIfBsSsPkmAuthValidStatus	Contains the reason why a SS's certificate is deemed valid or invalid. Return unknown if the SS is running PKM mode. ValidSsChained means the certificate is valid because it chains to a valid certificate. ValidSsTrusted means the certificate is valid because it has been provisioned to be trusted. InvalidSsUntrusted means the certificate is invalid because it has been provisioned to be untrusted. InvalidCAUntrusted means the certificate is invalid because it chains to an untrusted certificate. InvalidSsOther and InvalidCAOther refer to errors in parsing, validity periods, etc, which are attributable to the SS certificate or its chain respectively.	unknown (0), validSsChained (1), validSsTrusted (2), invalidSsUntrusted (3), invalidCAUntrusted (4), invalidSsOther (5), invalidCAOther (6)
wmanIfBsMsCMACPacketNumbercounter		
wmanIfBsMsCMAC_PN_UL		
wmanIfBsMsCMAC_PN_DL		
wmanIfBsMsCMACValue		

wmanIfBsMsPkmAuthResultCode	Contains the result code of the RSA-based authorization(only for PKMv2)	
wmanIfBsMsPkmAKId	Identify the AK as defined in Table 133	
wmanIfBsKeyPushMode	Distinguish usage code of a PKMv2 Group Key Update Command message	
wmanIfBsKeyPushCounter	Protect for replay attack.	