Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Corrections for SA Type**
Data Submitted	**2005-07-14**

Source(s)	Seokheon Cho Taeyong Lee Chul Park Chulsik Yoon ETRI 161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea Yongmao Li Huawei Technologies	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr

Re:	IEEE P802.16e/D9
Abstract	Several SAs are defined in the SA type attribute. However, the distinction among them is ambiguous. Only Primary SA, Static SA, and Dynamic SA can be mapped to a connection. Moreover, Group SA and MBS SA are subset of Static SA and Dynamic SA. Therefore, it is necessary to redefine the SA type attribute.
Purpose	Adoption of proposed changes into P802.16e/D9

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:chiar@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>.

Corrections for SA type

Seokheon Cho, Taeyong Lee, Chul Park, and Chulsik Yoon
ETRI

Yongmao Li
Huawei Technologies

Introduction

0.1 IEEE P802.16e/D9 Status and Problems

The SA type attribute specifies several SAs, such as Primary SA, Static SA, Dynamic SA, Group SA, and MBS SA.

Primary SA, Static SA, and Dynamic SA have characteristics as follows:

Primary SA is the fundamental SA. Static SA is an SA that the MS is authorized to obtain keying materials. Dynamic SA is an SA that the BS establishes and eliminates dynamically in response to the enabling or disabling of service flows.

The secondary management connection shall be mapped to Primary SA. The multicast transport connection shall be mapped to Static SA or Dynamic SA. The unicast transport connection shall be mapped to Primary SA, Static SA, and Dynamic SA.

Meanwhile, cell-based multicast service and MBS service are carried on the multicast transport connection, because those services are a kind of multicast service. So, cell-based multicast service and MBS service can be mapped to multicast transport connection.
In addition, those services can be authorized to the MS or provided dynamically.

Unicast service is carried on and mapped to the unicast transport connection. Also, unicast service can be authorized to the MS or provided dynamically.

That is, an SA for cell-based multicast service, MBS service, or unicast service is not independent from Static SA or Dynamic SA but a sub-SA of Static SA or Dynamic SA.

0.2 Solutions

There exists only Primary SA, Static SA, and Dynamic SA.

Unicast service, cell-based multicast service, and MBS service can be defined as the SA service type, because an SA for cell-based multicast service, MBS service, or unicast service is not an independent SA but a sub-SA of Static SA or Dynamic SA.

The SA service type shall be defined, only when SA type is Static SA or Dynamic SA.

Proposed Changes into IEEE P802.16e/D9

[Delete 11.9.18:]

~~**11.9.18 SA type**~~

~~Table 381 – SA type attribute values~~

~~**Value**~~	~~**Description**~~
~~3~~	~~Group~~
~~4~~	~~MBS~~
~~5-127~~	~~reserved~~
~~128-255~~	~~Vendor specific~~

[Insert new subclause 11.9.36:]

11.9.36 SA service type

Description: This attribute indicates service types of the corresponding SA type. This attribute shall be defined, only when the SA type is Static SA or Dynamic SA. The GTEK shall be used to encrypt connection for group multicast service. The MTK shall be used to encrypt connection for MBS service.

Table 381 – SA service type attribute values

Type	**Length**	**Description**

31	1	0: Unicast service 1: Group multicast service 2: MBS service 3-255: Reserved

[Change the Table 370 in sub-clause 11.9:]

11.9 PKM-REQ/RSP management message encodings

Table 370-PKM attribute types

Type	PKM attribute
29	Nonce
30	Auth Result Code
31	~~Reserved~~ SA service type
32	Reserved
33	SS_RANDOM
	… **Rest of the attributes of this table remains the same.**

[Change the Table 370 in sub-clause 11.9:]

11.9.17 SA-Descriptor

Description: The SA-Descriptor attribute is a compound attribute whose subattributes describe the properties of a Security Association (SA). These properties include the SAID, the SA type, the SA service type, and the cryptographic suite employed

within the SA.

Table 380-SA-Descriptor subattributes

Attribute	Contents
SAID	Security Association ID
SA-Type	Type of SA
SA service type	Service type of the corresponding SA type. This shall be defined, only when SA type is Static SA or Dynamic SA.
Cryptographic-Suite	Cryptographic suite employed within the SA

Type	Length	Description
23	variable	The Compound field contains the subattributes shown in Table 380.