### 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  

### 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

### 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 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.
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

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>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Group</td>
</tr>
<tr>
<td>4</td>
<td>MBS</td>
</tr>
<tr>
<td>5-127</td>
<td>reserved</td>
</tr>
<tr>
<td>128-255</td>
<td>Vendor-specific</td>
</tr>
</tbody>
</table>

[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 single-BS MBS service. The MTK shall be used to encrypt connection for multi-BS MBS service.
Table 370-PKM attribute types

<table>
<thead>
<tr>
<th>Type</th>
<th>PKM attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>Nonce</td>
</tr>
<tr>
<td>30</td>
<td>Auth Result Code</td>
</tr>
<tr>
<td>31</td>
<td>Reserved</td>
</tr>
<tr>
<td>32</td>
<td>Reserved</td>
</tr>
<tr>
<td>33</td>
<td>SS_RANDOM</td>
</tr>
</tbody>
</table>

… Rest of the attributes of this table remains the same.

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

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAID</td>
<td>Security Association ID</td>
</tr>
<tr>
<td>SA-Type</td>
<td>Type of SA</td>
</tr>
<tr>
<td>SA service type</td>
<td>Service type of the corresponding SA type. This shall be defined, only when SA type is Static SA or Dynamic SA.</td>
</tr>
<tr>
<td>Cryptographic-Suite</td>
<td>Cryptographic suite employed within the SA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>variable</td>
<td>The Compound field contains the subattributes shown in Table 380.</td>
</tr>
</tbody>
</table>