|  |  |
| --- | --- |
| Project | **IEEE 802.21 MIHS****<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **Proposed remedy for Comment #51** |
| DCN | **21-14-0xxx-00-MuGM** |
| Date Submitted | **March 18, 2014** |
| Source(s) | Yoshihiro Ohba (Toshiba) |  |
| Re: | IEEE 802.21 Session #61 in Beijing |
| Abstract | This document describes a proposed remedy for LB7b Comment #51 about protected PDU format. |
| Purpose | To addresses LB7b Comment #51. |
| Notice | This document has been prepared to assist the IEEE 802.21 Working Group. 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 IEEE 802.21 may make this contribution public. |
| Patent Policy | The contributor is familiar with IEEE patent policy, as stated in [Section 6 of the IEEE-SA Standards Board bylaws](http://standards.ieee.org/guides/opman/sect6.html#6.3) <[http://standards.ieee.org/guides/bylaws/sect6-7.html#6](http://127.0.0.1:4664/cache?event_id=757737&schema_id=1&s=5X0vID10lu_E6yrIkWkNd4Wz2H8&q=hancock)> and in *Understanding Patent Issues During IEEE Standards Development* <http://standards.ieee.org/board/pat/faq.pdf> |

[1] *Change second paragraph of Clause 8.4.2 as follows.*

A protected MIH PDU is an MIH PDU that has an MIH header with S bit set to one indicating that the MIH service specific TLVs in this PDU are encrypted or the PDU is digitally signed. When the MIH service specific TLVs in this PDU are encrypted, each security association is defined for a pair or group of MIHFs and is identified by a security association identifier (SAID). In this case, an SAID TLV shall be carried in the PDU. Source and Destination MIHF Identifier TLVs may not be present when an SA is defined for a pair of MIHFs. When a PDU is digitally signed, a Signature TLV shall be carried in the PDU. Figure 29 shows a protected MIH protocol frame. Table XX shows valid combinations of S bit and security-related TLVs. ~~Therefore, for a protected MIH PDU, when a security association identifier is defined and the PDU is not digitally signed, the Source and Destination MIHF identifier TLVs may not be present.~~ ~~In this case, an MIH header is followed by an SAID TLV, which is followed by a security TLV. When no SAID TLV is carried, Service Specific TLVs shall be carried without encryption and therefore no Security TLV is carried. A Signature TLV is carried when a multicast PDU is digitally signed. When an MIH message is multicast and the S bit is set, Source and Destination Identifier TLVs and an SAID TLV shall be carried~~

[2] *Add the following table in Clause8.4.2.*

Table XX: Valid Combinations of S-bit and Security-related TLVs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S bit | Source and Destination MIHF Identifier TLVs | SAID TLV | Security TLV or Service Specific TLVs | Signature TLV |
| 0 | Present | Not Present | Service Specific TLVs | Not Present |
| 1 | Present | Not Present | Service Specific TLVs | Present |
| 1 | May not be present | Present && ID\_TYPE != 2 | Security TLV | Not Present |
| 1 | Present | Present && ID\_TYPE = 2 | Security TLV | Present |