|  |  |
| --- | --- |
| Project | **IEEE 802.21 MIHS****<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **Proposed remedy for Comments 112** |
| DCN | **21-14-0095-00-MuGM** |
| Date Submitted | **May 14, 2014** |
| Source(s) | Yoshikazu Hanatani (Toshiba) |  |
| Re: | IEEE 802.21 Session #62 in Waikoloa |
| Abstract | This document describes a proposed remedy for LB7c Comments #112 about group manipulation commands and group addressed commands protection. |
| Purpose | For LB7c Comment Resolution |
| 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> |

# Comments

* Cmt #112: In step h) recipient verifies the Signature TLV, but there is no step for command center to genenate a Signature TLV.

# Suggested Remedy:

[1] Change 9.5.3.1.2 as follows:

**9.5.3.1.2 MIHF of a GMCS**

~~k) If a security association ID with respect to the DestinationIdentifier is stored in its own~~ *~~Recipient~~**~~Information Base~~*~~, it encrypts Service Specific TLVs of this group manipulation command as shownin 9.6.4.~~

~~l) Generate a Signature TLV as shown in 9.6.4 using the signing key of the MIHF.~~

~~m~~k) If ResponseFlag=0, generate an MIH\_Net\_Group\_Manipulate indication using the preceding TLVs, else generate an MIH\_Net\_Group\_Manipulate request using the preceding TLVs.

l) Protect the MIH\_Net\_Group\_Manipulate indication message or the MIH\_Net\_Group\_Manipulate request message as shown in 9.6.2.

[2] Change Figure 40 as follows:



Change to “Generate MIH\_Group\_Manipulate indication”

Change to “Generate MIH\_Group\_Manipulate request”

Protect the message

Send the message

[3] Change 9.6.2 as follows:

**9.6.2 Multicast message ~~encrypton~~ protection**

In order to send a multicast MIH request or MIH indication message, the MIH User of the command center generates a request primitive and delivers it to the local MIHF. Upon receiving the request, the MIHF of the command center behaves as follows:

 a) The MIHF generates a Source MIHF ID TLV based on its own MIHF ID.

 b) The MIHF generates a Destination MIHF ID TLV based on the DestinationIdentifier in the received request.

 c) The MIHF generates service specific TLVs based on the received request primitive.

 d) Consulting with the Multicast Address Information Base, the MIHF finds the multicast address associated with the DestinationIdentifer in the received request.

 e) The MIHF generates an MIH request or indication message~~, and it sends the message to the multicast address found in Step d)~~.

 1) The service specific TLVs may be encrypted with an MIGSK associated to the DestinationIdentifier to make a Security TLV if necessary in the scheme described in 8.4.2.

 2) A signature TLV is generated as shown in 9.6.4 using the signing key of the MIHF.

f) The MIHF sends the message to the multicast address found in Step d).

When an MIHF of a recipient receives the message, it issues an indication primitive to its local MIH User, following the next steps:

 ~~f~~a) The Destination Identifier is retrieved from the Destination MIHF ID TLV. The MIHF checks if the Destination Identifier is registered in the Group Information Base or not. If it is not, the message is not for the recipient. Thus, it cancels the following steps and stops processing.

 ~~g~~b) The Source Identifier is retrieved from the Source MIHF ID TLV.

 ~~h~~c) The MIHF verifies the Signature TLV using the verification key corresponding with the preceding Source Identifier. If the verification fails, it cancels the following steps and abort.

 ~~i~~d) The service specific parameters are retrieved from the service specific TLVs. If the service specific TLVs are encrypted in a Security TLV, the MIHF decrypts the Security TLV with the ~~group key~~MIGSK associated with the Destination Identifier that is available in the Group Information Base.