|  |  |
| --- | --- |
| Project | **IEEE 802.21 MIHS****<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **Additional remedies on Comment 102** |
| DCN | **21-14-0104-00-MuGM** |
| Date Submitted | **May 22, 2014** |
| Source(s) | Yoshihiro Ohba (Toshiba) |  |
| Re: | IEEE 802.21 Session #62 in Waikoloa |
| Abstract | This document describes a proposed remedy for LB7c Comment #102 |
| 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> |

# Comment #102 (about 9.5.3.1.2, page 64, line 8)

Comment: It has never been clear that the MIHF in GMCS is also a recipient of group manipulate command. However, it "stores the pairs of a Node Index and a corresponding Node Key (i.e., device keys) to retrieve a group key from a GKB," This is very confusing! What device keys the MIHF of GMCS should have? Its own device keys or device keys for all the potential recipients? If these are its own device keys as a recipient of group manipulation command, then the purpose of "retrieve a group key from a GKB" does not sound right, because "MGK" is also an item in this Recipient Information Base. It does not need to retrieve it from GKB. If these are device keys for all the potential recipients, then they have already stored in the MIH User of GMCS (see 9.5.3.1.1).

Suggested Remey: Discuss, clarify and correct.

Status: Deffered

Remark: Detailed remedy will be described in a revision of DCN 097

# Discussion

Additional issues related to this comment were found after May 2014 meeting.

Issue 1: It is better to rename CC (Command Center) to GM (Group Manager) since a group addressed command/message may be sent by a PoS that does not have a group manipulation functionality such as issuing a group manipulation command.

Issue 2: It is better to remove the terms GMCS and GMCR since (1) the roles of GMCS and GMCR can change per message basis and (2) the terms are used in 9.5.3.1 and 9.5.3.2 only. It is better to describe those sections without introducing new terms.

Issue 3: It is better to replace the term “group addressed command” with “group addressed message” since there are a number of MIH messages that can be multicast but do not belong to command service.

Issues 1 and 2 are relatively easier to resolve than Issue 3.

With regard to Issue 3, it has been identified that there is one exceptional case where a MIH\_Capability\_Discover request message sent to MIHF Broadcast ID can be sent by an MN, while all other group addressed messages are sent by a PoS. Since there may be other MN-originated group addressed messages defined in a future, it is suggested to revise Section 9 such that not only PoS-originated group addressed messages but also MN-originated group addressed messages are also covered. From security point of view, digital signature usage for group addressed message may need to be reconsidered. There are three options:

**Option 1: Make digital signature mandatory for all group addressed messages**

**Option 2: Make digital signature mandatory for PoS-originated group addressed messages and optional for MN-originated group addressed messages**

**Option 3: Make digital signature optional for all group addressed messages**

# Suggested Remedies

The following remedies are proposed in addition to those described in DCN 097.

<Section 3>

**group manager (GM):** An MIH User that manages the group by adding, deleting, and updating the group membership information. It may also generate the group key when needed. It is also the entity that issues group manipulation commands.

**group addressed message:** An MIH message sent to nodes that belong to a group identified by an MIHF Group ID. A group addressed message is sent using a multicast transport mechanism, which is out of the scope of this specification.

<Section 4>

~~CC Command Center~~

GM Group Manager

<Section 5>

* In Figure 24, change one of “PoS with Command Center” box to “PoS with Group Manager”, and change other “PoS with Command Center” box to “PoS”.
* Change the 1st and 2nd paragraphs to (superseding Cmt #7) :

There are scenarios where a set of nodes moves like a group between network points of attachment. Examples of these scenarios are: networks of sensors/actuators that move between production and management networks, a set of nodes in a mesh network that moves as a group from one gateway node to another, a group of nodes that travels together in a transportation medium while changing the network point of attachment. To manage the handover operation of these nodes in a bandwidth efficient manner when the network is performing failover, failback, configuration and other management operations, multicast-based group communication is required.

This standard allows network nodes to communicate handover commands to a group of MNs and PoSes via a multicast transport in a secure way. The standard defines primitives and corresponding messages for managing the multicast group membership (e.g., join, leave and update the group membership) and provide mechanisms for managing the multicast group keys. Figure 24 shows the logical view of the functional entities that are involved in a multicast-based group communication. The group manager is responsible for issuing the group manipulation commands in addition to generating the keys and managing the group. PoSes communicate with MNs via a multicast transport that is made available by the underlying network.

<Section 7>

* Change the following entry in Table 17:

|  |  |  |  |
| --- | --- | --- | --- |
| MIH\_Net\_Group\_Manipulate | Service Management | Used by a GM to manipulate the group membership of a node. | 7.4.32 |

<Section 8>

* Change the following paragraph in 8.3.1:

In particular, the following MIH messages can use an MIHF Group ID except for MIHF Broadcast ID. In the next list, when a message can be sent by a PoS and an MN, the only allowed multicast transmission is when the message is sent by the PoS:

<Section 9>

* Change the following paragraphs as specified below (superseding Cmt #53, #55, #58) :

9.5 Group manipulation for group addressed messages

A group addressed message is sent to a group of recipients. A recipient of a group addressed message can be a mobile node (MN) or a point of service (PoS). Each group is identified by an MIHF group ID. A group is dynamic in the sense that some of the group members may leave, while the new member may join. The group is managed through group manipulation commands.

A series of group addressed messages may follow a group manipulation command that defines a target group of recipients. A group addressed message is sent, for instance, by a PoS to instruct the group that the members should handover to a PoA or that they should update their configuration parameters. A payload of a group addressed message can be protected (encrypted) using the SA derived from the MGK. The following describes group manipulation commands and group addressed messages.

* Step 1: A group manipulation command is issued by a group manager to instruct recipients to join or leave a group. A group manipulation command may also be used to update a group key stored at a recipient. Group manipulation commands are carried in an MIH\_Net\_Group\_Manipulate request or indication message or an MIH\_MN\_Group\_Manipulate response message. An MIH\_Net\_Group\_Manipulate request or indication message is either unicast or multicast. An MIH\_MN\_Group\_Manipulate response message is unicast. Those messages are digitally signed by the originating MIHF. A group is indentified by an MIHF Group ID and associated with a multicast transport. The address used by this multicast transport can be provided by the group manipulation command itself. Note that a recipient over the multicast transport may not be in the group.
* Step 2: A group addressed message is sent to instruct the recipients to take an action. The MIHF Group ID of the target group is set to the Desitnation MIHF ID field in the group addressed message. A group addressed message is sent using a multicast transport associated with the MIHF Group ID. A group addressed message may alternatively take two types of payload: protected and non-protected. If a payload is protected, it uses AES CCM mode with a key derived from the current group key. (*Author’s Note: Adopt one of the following sentences*) *(Option 1)* Whether it is protected or not, the payload of a group addressed message is authenticated by a digital signature of the sender. *(Option 2)* Whether it is protected or not, the payload of a group addressed message sent by a PoS shall be authenticated by a digital signature of the PoS, and the payload of a group addressed message sent by an MN may be authenticated by a digital signature of the MN. *(Option 3)* Whether it is protected or not, the payload of a group addressed message may be authenticated by a digital signature of the sender.
* Change the following paragraph in 9.5.1.1 as specified below:

The device key assignment mechanism specified in this standard is based on a binary key structure, called a key tree. A key tree is a binary tree in depth d, where d is a system constant. A group manager, at its initialization period, shall generate a group management tree whose depth is less than 256. The root of the key tree is called a level 0 node. A node is a logical entity in a binary tree for which each leaf node represents a potential recipient of group addressed messages sent to a group created by the group manager of the key tree. Each recipient is a device, which can be an MN or a PoS. At level k, there are 2k nodes, 0≤ k≤d. Each level k node can be represented as a k-bit string. The string is called the index of the node. For example, when d > 1, the level 2 nodes are represented by the indices 00, 01, 11, 10. Each node is assigned to a key, called a node key and identified by the Node Index. For example, the node keys assigned to level 2 nodes are denoted as k<00>, k<01>, k<10>, k<11>.

* Change the last paragraph of 9.5.2 as specified below:

A group manager has a component called GKB Generator. A GKB Generator receives all the device keys assigned to all the recipients associated to a group and a MGK. The MGK is a master group key for that group. Recipients and the group manager can generate a Media Independent Group Session Key (MIGSK) from MGK (see 9.6). The mechanism to provide all device keys to the GKB generator is out of the scope of this specification. This mechanism can just encompass the explicit provision of the device keys to the GKB Generator or the random seed used to derive them. On receiving those data, a GKB Generator outputs a GKB, or several GKBs.

* Change the following paragraphs in 9.5.3 as specified below:

(*Author’s Note: Adopt one of the following paragraphs*)

*(Option 1)* In case the MIH PDU is protected through GKB-generated MIH SA as specified in Clause 8.4.2.3, the originating MIHF generates a Signature TLV consisting of a SIGNATURE\_DATA and a CERT\_SERIAL\_NUMBER. The SIGNATURE\_DATA is created by signing the MIH PDU using a signing key corresponding with a verification key specified by CERT\_SERIAL\_NUMBER.

*(Options 2 and 3)* In case the MIH PDU is protected through GKB-generated MIH SA as specified in Clause 8.4.2.3, the originating MIHF may generate a Signature TLV consisting of a SIGNATURE\_DATA and a CERT\_SERIAL\_NUMBER. The SIGNATURE\_DATA is created by signing the MIH PDU using a signing key corresponding with a verification key specified by CERT\_SERIAL\_NUMBER.

* Change the last paragraph of 9.5.3 as specified below:

Figure 37 illustrates group manipulation command distribution initiated by a PoS with group manager via a multicast transport. The MIH User of the PoS with group manager generates an MIH\_Net\_Group\_Manipulate.request, described in 7.4.32, and then it passes the request to the MIHF of the group manager. Upon receiving the request, the MIHF generates MIH\_Net\_Group\_Manipulate indication (Note that the decision on sending an indication message or a request message depends on the ResponseFlag parameter of the MIH\_Net\_Group\_Manipulate.request primitive), described in 8.6.1.23, and sends it to the recipients via multicast mechanisms. When a recipient receives the MIH\_Net\_Group\_Manipulate indication message, the MIHF of the recipient processes the message. After processing the message, the MIHF sends MIH\_Group\_Manipulate.indication to the MIH User of the recipient.

* In Figure 37, Change “Command Center PoS“ to “PoS with Command Center”
* Change section title of 9.5.3.1 to:

9.5.3.1 Sending procedures for group manipulation commands

* Change section title of 9.5.3.1.1 to:

**9.5.3.1.1 MIH user of a PoS with Group Manager**

* Change section title of 9.5.3.1.2 to:

**9.5.3.1.2 MIHF of a PoS with Group Manager**

* Change title of 9.5.3.2 to:

**9.5.3.2 Receiving procedures for group manipulation commands**

* **In 9.5.3.1 and 9.5.3.2, replace “command center” with “PoS with group manager”**