|  |  |  |
| --- | --- | --- |
| Project | **IEEE 802.21 MIHS**  **<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** | |
| Title | **Suggested remedy for IEEE 802.21m draft related to IEEE 802.21d** | |
| DCN | 21-15-0050-01-REVP | |
| Date Submitted | **May 11th, 2015** | |
| Source(s) | Yoshikazu Hanatani (Toshiba) |  |
| Re: | Comments to IEEE 802.21m draft from IEEE 802 editor. | |
| Abstract | This document describes suggested remedy for comments to IEEE 802.21m draft from IEEE 802 editor. | |
| Purpose | To create IEEE 802.21m draft | |
| 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 [MT1]:** This has not been added yet, Amendment D, will be added post edit of the amendment.

We will check edited version.

**Comment [MT2]:** Verify this is the correct figure.

This comment is related to IEEE 802.21c.

**Comment [MT3]:** These may not be the correct clause numbers, inconsistencies with numbering in Amendment D, please check.

Problem: Clause numbers in 21d D8 are already used in another annex (21c?).

Suggested remedy:

Add “7.4.30 **MIH\_Configuration\_Update** of D8” to D9.1 as 7.4.34.

Add “7.4.31 **MIH\_MN\_Group\_Manipulate** of D8” to D9.1 as 7.4.35.

Add “7.4.32 **MIH\_Net\_Group\_Manipulate.request** of D8” to D9.1 as 7.4.36.

Add “7.4.33 **MIH\_Pull\_Certificate** of D8” to D9.1 as 7.4.37.

Add “7.4.34 **MIH\_Push\_Certificate** of D8” to D9.1 as 7.4.38.

Add “7.4.35 **MIH\_Revoke\_Certificate** of D8” to D9.1 as7.4.39.

Change Table 3 as follows.

7.4.30 to 7.4.34.

7.4.31 to 7.4.35.

7.4.32 to 7.4.36.

7.4.33 to 7.4.37.

7.4.34 to 7.4.38.

7.4.35 to 7.4.39.

**Comment [MT4]:** Inconsistencies with numbering Annex D, please fix.

Problem: Clause numbers in 21d D8 are already used in another annex (21c?).

Suggested remedy:

Change Table 17 as follows.

7.4.30 to 7.4.34.

7.4.31 to 7.4.35.

7.4.32 to 7.4.36.

7.4.33 to 7.4.37.

7.4.34 to 7.4.38.

7.4.35 to 7.4.39.

**[MT5]:** Change as modified by 21d was not made here, this was confusing. The text did not match what was in the base nor modifications made by the previous amendments. Therefore I left text as is.

Problem: Base texts in 7.4.16.1.4 of 21d D8 are from 7.4.15.2.4 of 21 base specification.

Suggested remedy:

If the destination of the request is the local MIHF itself, the local MIHF issues a Link\_Action.request(s) to the specified ~~lower layer~~ link layer(s).

If the destination of the request is a remote MIHF, based on the ResponseFlag parameter, the local MIHF generates and sends an MIH \_Link \_Actions request message or an MI\_Link\_Actions indication message to the remote MIHF. Upon the receipt of the message, the remote MIHF then issues Link\_Action.request(s) to the specified ~~lower layer~~ link layer(s). If Response Flag parameter is set, the remote MIHF also generates a response message for the sending MIHF.

Memo

“indication.message” in 7.4.15.2.4 should be “indication message”

**Comment [MT6]:** By default the numbering was changed based on modification in 802.21a, however I didn’t make any changes to Clause 8 (as modified by 21d (editorial intructions, are very unclear).

Problem: Some instructions are unclear.

Related problem: There is a reference mistake in 9.6.2 of D8.

Suggested remedy:

**Change numbering of Clause 8.4.1a of IEEE 802.21a to 8.4.2.**

***Change second paragraph of Clause 8.4.2 as described in D8.***

**Insert Table 4 of D8 to the end of 8.4.2 in D9.1.**

**Change Figure 36 of D9.1 to Figure 29 of D8.**

**Change numbering of Clause 8.4.1a.1 of IEEE 802.21a to 8.4.2.1.**

**Add the following text at the end of Clause 8.4.2.1:**

A Signature TLV shall not be carried when MIH PDU is protected by (D)TLS (RFC 6347). Note that an MIH PDU protected by (D)TLS should only be used for unicast communication.

**Change numbering of Clause 8.4.1a.2 of IEEE 802.21a to 8.4.2.2.**

***Add the following text at the end of Clause 8.4.2.2:***

A Signature TLV shall not be carried when MIH PDU is protected through EAP-generated MIH SA.

**Change numbering of Clause 8.4.1a.3 of IEEE 802.21a to 8.4.2.3.**

**Add following clause at the end of 8.4.2.3**

8.4.2.4 MIH PDU protected through Group key generated MIH SA

When a GKB is used to distribute a MGK, the keys derived from MGK shall be used for a group MIH SA that is created for a group of MIHFs to encrypt Service Specific TLVs of an MIH PDU. The group MIH SA is identified by a security association identifier assigned by the PoS and carried in a SAID TLV. For integrity protection, a Signature TLV is carried in the MIH PDU. Figure 30 shows a protected MIH PDU for GKB-generated MIH SA. The protection procedure is specified in 9.6.2.

***Insert figure 30 of D8 at the end of Clause 8.4.2.3:***

***Add following clause at the end of 8.4.2.4:***

8.4.2.5 MIH PDU protected by digital signature only

When an MIH PDU with the S bit set sent by a PoS is not encrypted, it is integrity protected by a digital signature. Figure 31 shows an MIH PDU protected by a digital signature only. The protection procedure is specified in 9.6.

***Insert figure 31 of D8 at the end of Clause 8.4.2.4:***

**Memo:**

**Following text described in 9.6.2 of D8 should be modified.**

Problem: Protection method using AES-CCM should be referred. But, 8.4.2 describes Protected MIH protocol frame format.

1) The MIH Service Specific TLVs or fragment 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~~9.3.3.

**Comment [MT7]:** I have to figure out how to get this 2 closer to the parens.

?

**Comment [MT8]:** Check these last three rows, the modification in Amendment A, was unclear on where the insertions should go.

This comment is related to IEEE 802.21a.

**Comment [MT9]:** Check for proper placement, based on Amendment B, it is unclear where the insertion should be.

This comment is related to IEEE 802.21b.

**Comment [MT10]:** Check, for proper placement, Amendment C added this as item 5, however, the table already had the preceding information for 5.

This comment is related to IEEE 802.21c.

**Comment [MT11]:** Review, this modification was added in Amended C, Bit 5: had already been added by a previous amendment.

This comment is related to IEEE 802.21c.

**Comment [MT12]:** Check these three highlighted rows, the placement was not clear in Amendment A.

This comment is related to IEEE 802.21a.

**Comment [MT13]:** Did not make changes as modified by Amendment A and Amemendment C (the instructions and information was conflicting in Amendment A and unclear, so left as is.

This comment is related to IEEE 802.21a and IEEE 802.21c.

**Comment [MT14]:** Review these modification, the previous row was added in a previous amendment, and according to Annex C, this information should be added, M.8.4.43 already existed. Fix discrepancy.

This comment is related to IEEE 802.21c.