|  |  |
| --- | --- |
| Project | **IEEE 802.21 MIHS****<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **Proposed remedy for SB Comment i-37 and i-15** |
| DCN | **21-14-0152-02-MuGM** |
| Date Submitted | **October 10, 2014** |
| Source(s) | Yoshihiro Ohba and Yoshikazu Hanatani (Toshiba) |  |
| Re: | IEEE 802.21d Sponsor Ballot comment resolution |
| Abstract | This document describes a proposed remedy for SB comment i-37, i-15 about signature. |
| Purpose | For Sponsor Ballot 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

# Comment i-37 (p81, Annex F)

SIGNATURE TLV should contain sequence number at least when AES-CCM protection via Security TLV is not used.

* Comment i-15 (p36, line 12)

Signature TLV should be optional when S-bit is 1 and Security TLV is used. One case is when a message is sent to a two-member group which is equivalent to pairwise SA, then Message Authentication is sufficient and digital signature is not needed.

# Proposed resolution

* Comment i-37

[1] Change SIGNATURE data type as SEQUENCE(CERT\_SERIAL\_NUMBER, CHOICE(SEQUENCE\_NUMBER, NULL), SIGNATURE\_DATA).

[2] Add the following sentence to Description: "SEQUENCE\_NUMBER" shall be contained when MIH PDU protected by digital signature only.

[3] Revise 9.6.3.1 and 9.6.3.2 so that sequence number in signature is taken into account of signature generation and verification (see below)

* Comment i-15 (revised remedy)

[1] In the last row, change "Present" to "May not be present" for Signature TLV.

[2] Add the following text to 8.4.2: “A Signature TLV should be used for multicast MIH messages in order to provide source origin authentication for multicast MIH messages. Otherwise, a message alternation attack by an insider who has a GKB SA is possible even if the multicast MIH message is integrity protected by the group key corresponding to the GKB SA. A Signature TLV is not needed for a message that is protected by a GKB SA for a two-member group.

[3] Change 9.6.2 to make Signature TLV optional (see below).

**9.6.2 Multicast message protection**

Line 24:

e) The MIHF generates an MIH request or indication message.

 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 may be generated as shown in 9.6.3.1 using the signing key of the MIHF.

Line 34:

c) If the Signature TLV is attached, the MIHF verifies SIGNATURE\_DATA in the Signature TLV using the verification key corresponding with the CERT\_SERIAL\_NUMBER in the Signature TLV as shown in 9.6.3.2.

 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 MIGSK associated with the preceding Destination Identifier and the SAID in the Security TLV that is available in the Group Information Base. If the decryption fails, it cancels the following steps and abort.

*New text for 9.6.3.1 and 9.6.3.2 addressing comments i-35 and i-37:*

**9.6.3.1 Multicast Message Signatures**

Multicast Messages are signed with the message source using a private key of the message source. Integrity and proof of origin of a multicast message is verified by verifying the message signature with the public key of a message source. The message content is signed using elliptical curve cryptography.

In case the MIH PDU is protected through GKB-generated MIH SA with a signature as specified in ~~Clause~~ 8.4.2.3, the MIHF of PoS generates a Signature TLV consisting of a CERT\_SERIAL\_NUMBER and a SIGNATURE\_DATA. The SIGNATURE\_DATA is created by signing an MIH\_Group\_Manipulate command or a group addressed command using a signing key corresponding with a verification key specified by CERT\_SERIAL\_NUMBER. Figure 44 illustrates the data protection procedure with confidentiality.



1. —Signing (with confidentiality)

The MIHF encrypts the Service Specific TLVs with MIGSK, and generates the Security TLV. The MIHF selects a certification serial number and generates CERT\_SERIAL\_NUMBER from the certification serial number. Then, the MIHF computes the SIGNATURE\_DATA of the Signature TLV from the MIH Header, the Source MIHF Identifier TLV, the Destination MIHF Identifier TLV, the SAID TLV, the Security TLV, and the Type, Length and Value fields of the Signature TLV excluding the SIGNATURE\_DATA.

Note: If the MIH PDU is protected through a GKB-generated MIH SA, the signature TLV shall not include the SEQUENCE\_NUMBER.

In case the MIH PDU is not protected through a GKB-generated MIH SA and protected with a signature only as specified in 8.4.2.4, the MIHF of PoS generates a Signature TLV consisting of a SIGNATURE\_DATA, a CERT\_SERIAL\_NUMBER and a SEQUENCE\_NUMBER. Figure 45 illustrates the data protection procedure without confidentiality.



1. —Signing (without confidentiality)

The MIHF computes the SIGNATURE\_DATA of the Signature TLV from the MIH Header, the Source MIHF Identifier TLV, the Destination MIHF Identifier TLV, the Service Specific TLVs, and the Type, Length and Value fields of the Signature TLV excluding the SIGNATURE\_DATA.

Note: If the MIH PDU is not protected through a GKB-generated MIH SA, the signature TLV shall include the SEQUENCE\_NUMBER.

On receipt of signed multicast message there is an optional response indicating the validity of signature.

Message source requests credentials for key updates. Message source provides updates of credentials to destination devices (with overlap period).

**9.6.3.2 Signature Verification**

The signature is verified using the message source signature verification key. The message source will identify which key is to be used for the multicast message so that verification will utilize the correct key for signature verification.

In case the MIH PDU received contains a Signature TLV and is protected through a GKB-generated MIH SA, then the MIHF of recipient retrieves a CERT\_SERIAL\_NUMBER and a SIGNATURE\_DATA from the Signature TLV. Then, the MIHF verifies the SIGNATURE\_DATA using a verification key specified by the CERT\_SERIAL\_NUMBER. If the Signature TLV includes a SEQUENCE\_NUMBER, the MIH PDU shall be dropped since it is a wrong form. Figure 46 illustrates the data protection procedure with confidentiality.



1. —Signature verification (with confidentiality)

In the case the MIH PDU contains a Signature TLV and is not protected through a GKB-generated MIH SA, then the MIHF of recipient retrieves CERT\_SERIAL\_NUMBER, SIGNATURE\_DATA and SEQUENCE\_NUMBER from the Signature TLV. Then, the MIHF verifies the SIGNATURE\_DATA using a verification key specified by the CERT\_SERIAL\_NUMBER, and the SEQUENCE\_NUMBER. The received SEQUENCE\_NUMBER is considered valid if and only if the SEQUENCE\_NUMBER is greater than the last valid incoming sequence number maintained for the sender. Figure 47 illustrates the data protection procedure without confidentiality.



1. —Signature verification (without confidentiality)

**9.6.4 Multicast Ciphersuites**

***Figure 44, 45, 46, 47 and the related texts are moved to 9.6.3.1 and 9.6.3.2.***