|  |  |
| --- | --- |
| Project | **IEEE 802.21a** **<https://mentor.ieee.org/802.21>** |
| Title | **Suggested Remedies on Clause 9 of 802.21a/D03** |
| DCN | 21-10-0068-00-0sec |
| Date Submitted |  |
| Source(s) | Yoshihiro Ohba (Toshiba) |
| Re: |  |
| Abstract | This document contains remedies to 802.21a/D03 associated with the author’s LB5b comment on Clause 9. |
| Purpose | Proposes changes in the current 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#_blank) <[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#_blank)> and in *Understanding Patent Issues During IEEE Standards Development* [http://standards.ieee.org/board/pat/faq.pdf](http://standards.ieee.org/board/pat/faq.pdf#_blank) |

# Proposal

Change Clause 9 as follows:

9. MIH protocol protections

*(Insert the following new Clause)*

**9.1 Common procedures**

In the following, the procedures for sending and receiving any protected MIH PDU are described.

**9.1.1 Sending**

For sending a remote MIH message in a protected manner, an MIH PDU is created in the following steps.

a)At the sender, which can be an MN or a PoS, the MIH user generates an MIH primitive and passes it to the MIHF.

b)The MIHF at the sender constructs an MIH PDU. If an MIH security association (SA) exists, then the MIHF at the sender applies protection algorithms specified by the negotiated ciphersuite to the MIH PDU and then encapsulates the protected MIH PDU in a security TLV. If no MIH SA exists, then the MIH PDU is passed to a lower layer which is the transport protocol of the MIH message.

c) The security TLV is encapsulated in an MIH PDU with the S bit in the MIH header setting to one.

d) The MIH PDU is passed to a lower layer protocol which is the transport protocol of the MIH message.

**9.1.2 Receiving**

For receiving a protected MIH message from a remote entity, the protected MIH PDU is processed in the following steps.

a) At the receiver, which can be an MN or a PoS, the MIHF receives a protected MIH PDU from a lower layer, which is the transport protocol of the MIH message.

b) If the S bit is set to one in the header, the MIHF processes security TLV and extract the plaintext MIH PDU. Otherwise, it obtains MIH PDU.

c) The MIHF creates an MIH primitive from MIH PDU and passes it to the MIH user at the receiver.

The processing steps at the sender and receiver are described in Figure 32.

(Insert Figure 32 of D03 here)

**Figure 32 – Protect MIH PDU**

**The transport protocol entities to be associated with an MIH SA are MIHF peers and are identified by MIHF identifiers. Therefore, the transport address of an MIHF can change over the lifetime of an MIH SA as long as the mapping between the transport address and the MIHF identifier of an MIHF is maintained.**

**9.~~1~~2 Protection ~~established through MIH (D)TLS~~ with (D)TLS-generated MIH SA**

**In this option, a mobile node, the client, and a PoS, the server, execute a TLS, specified in IETF RFC 5246, or DTLS, specified in IETF RFC 4347, to establish MIH protections. When the MIH protocol transport is reliable, TLS is used. Otherwise, DTLS is used. In the rest of this clause, (D)TLS is used to denote TLS or DTLS. In a (D)TLS handshake, the mutual authentication is executed through either pre-shared key or a public key certified by a trusted third party such as a certificate authority. In this option, the authentication may or may not be related to access control. It can be an access authentication for MIH service if a PoS holds service credentials for the mobile nodes. A (D)TLS handshake record is carried in a Authentication TLV of an MIH\_Auth indication message.**

**After the handshake, a (D)TLS session is established. In this case, the TLS master key and the keys derived from the master key, all the TLS parameters, and TLS ciphersuite negotiated in the TLS handshake form an MIH SA. The (D)TLS security association identifier is carried in each message in the SA ID TLV.**

**In a (D)TLS session, an MIH message is first protected as application data. Then the (D)TLS record is trans­ported by MIH protocol by security TLV. ~~In the following, the procedures for sending and receiving are introduced.~~**

**For a (D)TLS-generated MIH SA, it can be terminated through (D)TLS session termination using an MIH\_Auth indication message.**

**~~9.1.1 Sending~~**

**~~9.1.2 Receiving~~**

*(Insert the following new Clause)*

9.3 MIH message protection mechanisms for EAP-generated MIH SAs

**9.~~2~~3.1 Key establishment ~~through an MIH access authentication~~**

**9.~~2~~3.1.1 MIH service access authentication**

**9.~~2~~3.1.2 Key derivation and key hierarchy**

**9.~~2~~3.1.3 EAP-generated MIH security association**

**9.~~2~~3.1.4 Termination**

**9.3.2 MIH message protection mechanisms for EAP-generated SAs**

**9.3.2.1 General MIH PDU protection procedure**

**9.3.2.2 MIH PDU protection by AES CCM**

**9.3.2.2.1 AES CCM Parameters**

**9.3.2.2.2 Construct AES CCM Nonce**

**9.3.2.2.3 Operational procedures in AES CCM**

**9.3.2.2.3.1 Encapsulation**

**9.3.2.2.3.2 Decapsulation**

**9.3.2.2.4 Format of security TLV**

**9.3.2.3 MIH PDU protection by AES in CBC mode and HMAC-SHA1-96**

**9.3.2.3.1 Initiate vector for AES in CBC mode**

**9.3.2.3.2 Operational procedures in applying AES CBC and HMAC-SHA1-96**

**9.3.2.3.2.1 Encapsulation**

**9.3.2.3.2.2 Decapsulation**

**9.3.2.3.3 Format of security TLV**

**9.3.2.4 MIH PDU protection by HMAC-SHA1-96**

**9.3.2.4.1 MIC generation and verification**

**9.3.2.4.1.1 MIC generation**

**9.3.2.4.1.2 MIC verification**

**9.3.2.4.2 Format of security TLV**

**9.3.2.5 MIH PDU protection by AES-CMAC**

**9.3.2.5.1 MIC generation and verification**

**9.3.2.5.1.1 MIC generation**

**9.3.2.5.1.2 MIC verification**

**9.3.2.5.2 Format of security TLV**