|  |  |
| --- | --- |
| Project | **IEEE 802.21.1 Media Independent Services** **<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **Proposed remedy for Cmt #1 of LB10** |
| DCN | **21-16-00-0011-00-REVP** |
| Date Submitted | **May 16, 2016** |
| Source(s) | Yoshikazu Hanatani (Toshiba) |
| Re: | Session #74, Big Island, HI, USA |
| Abstract | The definition of MIS security association (SA) mentions to EPA-generated SA and GKB-generated SA. But, it does not mention to GKB-generated SA. To solve the issue, this contribution proposes an update of the definition of MIS SA. |
| Purpose | Suggested remedy for Cmt #1 in LB10. |
| 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> |

Cmt #1:

Clause Number: 3

Starting Page Number: 9

Starting Line Number: 37

 Comment Details: mention MIS SA established via GKB method

 Suggested Remedy: Add an explanation such as "The group MIS SA is created with GKB generation."

Proposed remedy:

 Update the definition of MIS security association (SA) in clause 3 as follows

 **Original definition**

MIS security association (SA): An MIS security association is a set of cryptographic attributes established between the peer MIS entities for protecting MIS messages at the MIS protocol layer. An MIS SA is established via TLS handshake or EAP execution, where both the TLS handshake and EAP execution take place over the MIS protocol. When an MIS SA is established via TLS handshake, the TLS master key and its child keys, TLS random values and the TLS cipher suite negotiated in the TLS handshake are a part of the MIS SA. When an MIS SA is established via EAP execution, an MSK or rMSK and its child keys, MIS random values and the MIS cipher suite negotiated between the peer MIS entities are associated with the MIS SA.

 **Updated definition**

MIS security association (SA): An MIS security association is a set of cryptographic attributes established between the peer MIS entities for protecting MIS messages at the MIS protocol layer. An MIS SA is established via TLS handshake, ~~or~~ EAP execution, or via a group key distribution mechanism using GKB where ~~both~~ all of the TLS handshake, ~~and~~ EAP execution, and group key distribution take place over the MIS protocol. When an MIS SA is established via TLS handshake, the TLS master key and its child keys, TLS random values and the TLS cipher suite negotiated in the TLS handshake are a part of the MIS SA. When an MIS SA is established via EAP execution, a~~n~~ master session key (MSK) or re-authentication master session key (rMSK) and its child keys, MIS random values and the MIS cipher suite negotiated between the peer MIS entities are associated with the MIS SA. When an MIS SA is established via group key distribution mechanism using GKB, the master group key and its child keys, and the MIS group cipher suite indicated to the peer MIS entities are associated with the MIS SA.