|  |  |
| --- | --- |
| Project | **IEEE 802.21 MIHS****<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **Proposed update [revised] to Section 9.2.2** |
| DCN | **21-13-0062-00-0000** |
| Date Submitted | **April 5, 2013** |
| Source(s) | Charles Perkins and Yoshihiro Ohba |  |
| Re: | IEEE 802.21 Session #55 in Orlando |
| Abstract | This document proposes an update for Section 9.2.2 of 802.21c/D02 |
| Purpose | Comment resolution of 802.21 LB#6a |
| 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> |

**[1] *Replace the first paragraph of subclause 9.2.2 in 802.21a with the following:***

Upon a successful MIH service access authentication, the authenticator, (i.e., the serving PoS) obtains a master session key (MSK), a re-authentication master session key (rMSK) via EAP to generate a root key *K* shared between the MN and the serving PoS. Alternatively, the root key *K* may be securely exchanged with the serving PoS from another trusted PoS (e.g., OPoS) using the transfer mechanism specified in 10.3.1. In the latter case, the MIHF identifier of the MN, Nonce-T, generated by the MN and Nonce-N, generated by the OPoS are also transferred together with *K*. Nonce-T is generated as follows: Nonce-T = PRF(Nonce-T’ || MN\_MIHF\_ID), where Nonce-T’ is provided by the MN and MN\_MIHF\_ID is the MN’s MIFH identity. Similarly, PoS generates Nonce-N by first generating a random number Nonce-N’. Then Nonce-N = PRF(Nonce-N’ || POS\_MIHF\_ID), where POS\_MIHF\_ID is the PoS’s MIHF identity.

The keys derived from *K* include a 128 bit authentication key (MIAK) used to generate a value AUTH, the session keys determined by the ciphersuite *c* agreed upon between the MN and the serving PoS. The session keys used for MIH message protection consist of an encryption key (MIEK) only, an integrity key (MIIK) only, or both an encryption key (MIEK) and an integrity key (MIIK). The concatenation of MIAK, MIEK and MIIK is called the media independent session key (MISK). The length, *L*, of the MISK is specified in 9.2.3.

 **[2] *Replace the third paragraph of subclause 9.2.2 in 802.21a with the following:***

* K - key derivation key. It is truncated from a master session key (MSK) or re-authentication MSK (rMSK), or obtained by key exchange with another trusted PoS. The length of K is determined by the pseudorandom function (PRF) used for key derivation. If HMAC-SHA-1 or HMAC-SHA-256 is used as a PRF, then the full MSK or rMSK is used as key derivation key, *K*. If CMAC-AES is used as a PRF, then the first 128 bits of MSK or rMSK are used as key derivation key, *K*.

In the following figure, change K’ to K, and delete the lower-right rectangle (the one with the legend “K’ (transmitted to other PoS)”.

**Figure 36 MIH Key Hierarchy**