|  |  |
| --- | --- |
| Project | **IEEE 802.21.1 Media Independent Services** **<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **Suggested remedy for Cmt#149 of LB8** |
| DCN | **21-16-00-0010-01-REVP** |
| Date Submitted | **January 20, 2016** |
| Source(s) | Yoshikazu Hanatani (Toshiba) |
| Re: | Session #71, Atlanta |
| Abstract | The handover specific commands, MIS\_Prereg\_Xfer and MIS\_N2N\_Prereg\_Xfer, deliver a handover specific key derivation key. 9.2.2 in Draft IEEE 802.21m/D01 includes a key derivation method only used by the handover specific key derivation key. This contribution suggests as follows:1. Remove the key derivation method for the handover specific key derivation key from Draft IEEE 802.21m/D01.
2. Add new subclause on the the key derivation method for the handover specific key derivation key to Draft IEEE 802.21.1/D01.
 |
| Purpose | Suggested remedy for Cmt #149 in LB8. |
| 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> |

Problem: Texts in 9.2.2 includes a handover specific key derivation procedure.

The handover specific key derivation procedure should be a part of 21.1.

Suggested remedy:

Change 9.2.2 in Draft IEEE 802.21m/D01 as follows.

* + 1. **Key derivation and key hierarchy**

Upon a successful MIS service access authentication, the authenticator (i.e., the PoS) obtains a master session key (MSK) or a re-authentication master session key (rMSK) via EAP to generate a KeyDerivationKey shared between the MN and the PoS.

The keys derived from KeyDerivationKey include a 128 bit authentication key (MIAK) used to generate a value AUTH, the session keys determined by the ciphersuite code *c* agreed upon between the MN and the serving PoS. If no ciphersuite code is specified by the MN, the default ciphersuite code is used as specified in Table 25 in 9.2.3. The session keys used for MIS 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.

For the key derivation, the following notations and parameters are used.

*K* - key derivation key. It is truncated from a master session key (MSK) or re-authentication MSK (rMSK). 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 the key derivation key *K*. If CMAC-AES is used as a PRF, then the first 128 bits of MSK or rMSK are used as the key derivation key *K*.

*L* - The binary length of derived keying material MISK. *L* is determined by the selected ciphersuite, which is specified in 9.2.3.

*h* - The output binary length of PRF used in the key derivation. That is, *h* is the length of the block of the keying material derived by one PRF execution. Specifically, for HMAC-SHA-1, *h* = 160 bits; for HMAC-256, *h* =256 bits; for CMAC-AES, *h* = 128 bits.

*n* - The number of iterations of PRF in order to generate *L*-bits keying material.

*Nonce-T* and *Nonce-N* - The nonces exchanged during the execution of service access authentication.

*c* - The ciphersuite code is a one octet string specified for each ciphersuite. The code is defined in 9.2.3.

*v* - The length of the binary representation of the counter and the length of keying material *L*. The default value for *v* is 32.

 “MISK” - 0x4D49534B, ASCII code in hex for string “MISK.”

 *[a]2* - Binary representation of integer *a* with a given length.

For a given PRF, the key derivation for MISK can be described in the following procedures:

**Fixed input values:** *h* and *v*.

**Input:** *K*, *Nonce-T*, *Nonce-N*, *L*, and ciphersuite code.

**Process:**

1. *n*:=[L/h];
2. If *n* >2*v* *-1*, then indicate an error and stop.
3. Result (0) :=empty string.
4. For *i* =*1* to *n*, do
	* 1. *K(i) := PRF(K, “MISK” || [i]2 || Nonce-T || Nonce-N || c || [L]2)*.
		2. *Result(i) = Result (i-1) || K(i)*.
5. Return *Result* *(n)* and *MISK* is the leftmost *L* bits of Result *(n)*.

The *MISK* is parsed in such a way that

*MISK = MIAK || MIIK || MIEK*.

With the above procedure, a key hierarchy is derived as shown in Figure 46.



1. **Figure 46—MIS Key Hierarchy**

Add following new subclause as 5.15 of .21.1.

**5.15　 Key derivation and key hierarchy for media independent handover service**

The KeyDerivationKey may be securely exchanged with the serving PoS from another trusted PoS (e.g., SPoS) using the transfer mechanism specified in 5.14.2. In the case, the MISF identifier of the MN, Nonce-T generated by the MN, and Nonce-N generated by the SPoS are also transferred together with a KeyDerivationKey.

The media independent session key (MISK) is derived from the KeyDerivationKey as described in 9.2.3 in Draft IEEE 802.21.1/D01. A SALifeTime for the MISK may be overridden by passing a preferred value as the SALifeTime parameter in relevant MIS primitives.

Change text in 5.11.12.4.4 of .21.1 as follows.

5.11.12.4.4 Effect on receipt

The MIS application on the MN may generate another MIS\_Prereg\_Xfer.request primitive—for example, if preregistration procedures are not completed. If KeyDerivationKey is present, the MN derives the key hierarchy according to 5.15.

Change text in 5.11.12.4.4 of .21.1 as follows.

5.11.12.4.4 Effect on receipt

The TPoS MISF recovers KeyDerivationKey *K* according to the formula in 5.14.2. The MISF then passes *K* to the MIS application, which then derives the key hierarchy, installing keys as necessary in the AAA used by the target network. The TPoS also must generate appropriate messages to the TPoA to install a media-specific pair-wise master key (MSPMK, defined in 10.2.1.2 of IEEE Std 802.21-XXXX) also derived from *K*, which will be used by the MN as necessary when the MN connects to the target network. The MSPMK will be distributed to the target PoA using media-specific key distribution described in10.2.2 of IEEE Std 802.21-XXXX.

Change text in 5.12.1.2.4 of .21.1 as follows.

The TPoS MISF recovers KeyDerivationKey *K* according to the formula in 5.14.2. The MISF then passes *K* to the MIS application, which then derives the key hierarchy, installing keys as necessary in the AAA used by the target network. The TPoS also must generate appropriate messages to the TPoA to install a media-specific pair-wise master key (MSPMK, defined in 10.2.1.2 of IEEE Std 802.21-XXXX) also derived from *K*, which will be used by the MN as necessary when the MN connects to the target network. The MSPMK will be distributed to the target PoA using media-specific key distribution described in10.2.2 of IEEE Std 802.21-XXXX.

Change text in 5.13.2.21 of .21.1 as follows.

An MISF sends this message to relay link layer frames during preregistration. The corresponding primitive is defined in 5.12.1.1. Nonce-T, Nonce-N, and the encrypted KeyDerivationKey must all be present, or must all be absent; MISF generates Nonce-N and the encrypted KeyDerivationKey. The method for encrypting KeyDerivationKey is specified in 5.14.2.