|  |  |
| --- | --- |
| Project | **IEEE 802.21m Revision Project** **<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **Suggested remedy for Cmt #149 of LB8** |
| DCN | **21-16-00-0010-02-REVP** |
| Date Submitted | **January 22, 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. Modify 5.14 of Draft IEEE 802.21.1/D01 to include the removed text.
 |
| 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**

*Change 5.14 of .21.1 as follows*.

1. 1. **Proactive authentication for single radio handover service**

An alternative to proactive authentication mechanism specified in clause 10 in Draft IEEE 802.21m/D01 is described below.

**5.14.1 Establishing MIS Security Association between roaming partners**

The PoS is a convenient and natural place to locate security services, and roaming partners have in place agreements that can be used to beneficially establish the needed security agreements between different PoS modules in partner networks. It is expected that the PoS functions in partner networks must often communicate by data paths that traverse the external Internet; in such cases, a secure communication channel must exist or must be established between the partners. It is out of scope for this document to specify exactly how the secure communication channel should be established, but this can be done by configuration when the partners enter into their roaming agreement. It can also be done on demand by using IKEv2 (RFC 7296) [B36]. The following overview describes in more detail the circumstances enabling dynamic establishment of security association between the SPoS and the TPoS.



1. **—MN handover signaling for preregistration using SPoS.**

MIS\_Prereg\_Xfer and MIS\_N2N\_Prereg\_Xfer messages exchanged between the SPoS and the TPoS may require security protection. Furthermore, the TPoS may reject these messages from an unauthorized source network PoS. To protect the link between the SPoS and the TPoS, several approaches are possible.

An MIS SA (Security Association) (see 8.4.2 of IEEE Std 802.21-XXXX) can be used for protecting the communications between an SPoS and a TPoS. In this case, the SPoS acts as the initiating end-point of an MIS SA and a TPoS as the other end-point of the MIS SA. The MIS SA can be established using (D)TLS over MIS or EAP over MIS (see 9.2 of IEEE Std 802.21-XXXX).

Except for the initial network attach, by the time an MN enters a network, it can also have a security relationship with the PoS in that network by using MIS\_Prereg\_Xfer commands. For each newly visited network, this security relationship can be created on demand, enabled by signaling from another PoS. The PoS creating the visited security relationship can either be the MN's home PoS (HPoS, a PoS in MN's home network) or the PoS in the network previously visited by the MN. When the MN first attaches to one of the partner networks of the roaming partners, it is either the MN's home network or a visited network. If the first attachment is to the MN's home network, the MN is expected to already have a security association with HPoS; otherwise, the MN can bootstrap this security association with the assistance of the HPoS, IKEv2, standard AAA mechanisms, or other proprietary means.

After initial attachment, there is signaling defined so that at all times the MN has a security association with the PoS in the network at its current point of attachment, i.e., the SPoS. As the MN moves from one partner network to the next target network, the MN establishes or renews a security association with the PoS in the target network, the TPoS. When handover is completed, the TPoS naturally begins to play the role of the MN’s serving PoS, and subsequently when a handover is required the TPoS plays the role of the SPoS.

In order to enable a wider application of handovers and in particular preregistration signaling, security must be guaranteed for the control traffic. As described above, this signaling traffic is mediated by the PoS in each target network, which may be unknown to the MN until the need for handover has been determined. In such cases, for secure signaling, the MN needs to establish a security association with the TPoS. The process of establishing such a security association can be quite time consuming and often expensive in processor cycles as well. This clause specifies a fast, straightforward method for providing security associations as needed between the MN and the TPoS in any target network within the networks covered by the roaming partners.

**5.14.2 Key generation and distribution by SPoS**

This clause specifies one alternative algorithm to key derivation mechanism specified in 9.2.2 in Draft IEEE 802.21m/D01 allows the SPoS to distribute a key derivation key *K* to the MN and to its desired TPoS. The key derivation key is then used to derive other keys that are used as the basis for a secure communications channel between the MN and the TPoS, enabling further secure preregistration activities. The notation used in this clause for PoS-based handover keys is listed in Table 11.

1. **—Notation for SPoS-based exchange of key derivation key *K***

|  |  |
| --- | --- |
| 1. *K*
 | 1. Key derivation key
 |
| 1. *K*SPoS
 | 1. Encryption key (i.e., MIAK (MN, SPoS)) between the MN and the SPoS
 |
| 1. *K*stpos
 | 1. Encryption key between the SPoS and the TPoS
 |
| 1. PRFSPoS
 | 1. pseudo-random function between the MN and the SPoS
 |
| 1. PRFstpos
 | 1. pseudo-random function between the SPoS and the TPoS
 |

Because of previous protocol operations (e.g., derivation of MIAK upon arrival in the source network), the MN has a current security association with the SPoS. This security association is bidirectional and based on a shared key *K*SPoS.

Suppose the MN determines to move to a new network, the target network; for preregistration, the MN needs to use the PoS in the target network, i.e., the TPoS. Before it can do this, it needs to discover the address of the TPoS and establish a security association with the TPoS by exchanging MISK as described in 9.2.1 of IEEE Std 802.21-XXXX.

For this purpose, the MN can make use of its existing security association with the SPoS, because the SPoS either already has, or can readily establish, a security association with the TPoS, for example, using IKEv2[B36]. Suppose the SPoS already has the required security association with the TPoS. Then, when the MN begins forwarding preregistration traffic to the TPoS via the SPoS, the SPoS will provide the MN and the TPoS with a key derivation key, *K*, for use to derive MIAK, which can be used to protect the remainder of the the MN’s signaling traffic with the TPoS. The SPoS thus forwards the initial traffic to the TPoS on behalf of the MN; the SPoS uses its own security relationship with the TPoS to protect this initial preregistration signaling, and it also supplies the value of *K* to the TPoS by adding a new extension to the preregistration traffic.

To send *K* to the TPoS, the SPoS provides the following payload within the TLVs of the MIS\_N2N\_Prereg\_Xfer request (see 5.12.1.1):

Payload = MNID, Nonce-T, Nonce-N, [*K* ⊕ PRFstpos (MNID, Nonce-T, Nonce-N)]

Upon receiving this payload, the TPoS calculates PRFstpos (MNID, Nonce-T, Nonce-N) and XORs the result to the third parameter of the payload to recover *K*.

Similarly, to send *K* to the MN, the SPoS provides the following payload as a parameter to MIS\_Prereg\_Xfer response (see 5.11.12.3):

Payload = TPoSIdentifier, Nonce-N, [*K* ⊕ PRFSPoS (TPoSIdentifier, Nonce-N)]

Upon receiving the payload, the MN calculates PRFSPoS (TPoSIdentifier, Nonce-T, Nonce-N) and XORs the result to the third parameter of the payload to recover *K*.

Alternatively, for either of these messages, the SPoS could encrypt the entire contents by using *K*stpos or *K*SPoS, the keys the SPoS has available with the TPoS and the MN respectively. The MN is allowed to send more signaling information to the TPoS via the SPoS even after the SPoS distributes the keys; the SPoS continues to forward traffic back and forth between the MN and the TPoS as needed until both endpoints have used *K* to derive the required security associations. For best performance and least likelihood of congestion at the SPoS, the MN and the TPoS should begin to use direct signaling as soon as possible thus bypassing the SPoS. Other structures for the message payloads are also possible, depending on requirements.

Once the handover is completed, the TPoS “becomes” the SPoS and the handover cycle can begin anew whenever the MN determines the need for the next handover.

**5.14.3 TPoS selection by the SPoS**

It is possible for the SPoS to take a more active role to promote smooth handover. When the MN determines the need for handover, but does not already know the address of the TPoS for the intended target network, the MN can start the preregistration sequence by sending all the known information to the SPoS. If the SPoS has access to information about each surrounding network and information about the MIS PoS in each such surrounding network, the SPoS can make a determination about which target network may best be able to provide connectivity and service to the MN. This also depends on the SPoS having access to location and configuration information about the MN—for example which radio access technologies (RATs) are configured for operation on the MN. When the candidate TPoS is in another operator’s network, it may be also important that the SPoS should have a security relationship with a candidate TPoS in order to avoid interference from malicious nodes. This would typically mean that the operators are also roaming partners.

Subsequently, the SPoS will provide the address of the TPoS to the MN along with *K*, as described above. The exact nature of the information about TPoS provided by the MN is dependent on the radio access technology type (RAT) of the target network and is outside the scope of this document.

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.

Change 5.11.12.3.2 in .21.1 as follows.

* + - * 1. **Semantics of service primitive**

MIS\_Prereg\_Xfer.response (

 DestinationIdentifier,

 TargetLinkIdentifier,

 LLInformation,

 MN\_NAI,

 TPoSIdentifier,

 SALifeTime,

 Status

)

|  |  |  |
| --- | --- | --- |
| **Name** | **Data type** | **Description** |
| DestinationIdentifier | MISF\_ID | This identifies an MISF that will be the destination of this response. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | (Optional: may be included if the target link is known) Identifies the remote PoA as the corresponding peer of the L2 exchange.a |
| LLInformation | LL\_FRAMES | (Optional) Carries link layer frames; included if and only if the corresponding MIS\_Prereg\_Xfer.indication contained LLInformation. |
| MN\_NAI | MISF\_ID | (Optional) Carries the MN’s Network Access Identifier in the case optimized pull key distribution is used. |
| TPoSIdentifier | MISF\_ID | (Optional) This identifies the target PoS. |
| SALifeTime  | LIFETIME | (Optional) Lifetime of the Security Association. b |
| Status | STATUS | Status of the preregistration transfer with TPoS. Code 3 (Authorization Failure) is not applicable. (See Table E.2 of IEEE Std 802.21-XXXX) |
| a Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN, and the PoA.b When (D)TLS is not used to establish the MIS security association between the MN and the TPoS, the default SALifeTime for MISK and derived keys is 65,536 seconds (slightly over 18 hours). This value may be overridden by passing a preferred value as the SALifeTime parameter in relevant MIS primitives. |

Change text in 5.11.12.4.2 of .21.1 as follows.

* + - * 1. **Semantics of service primitive**

MIS\_Prereg\_Xfer.confirm (

 SourceIdentifier,

 TargetLinkIdentifier,

 LLInformation,

 MN\_NAI,

 TPoSIdentifier,

 KeyDerivationKey,

 SALifeTime,

 Status

)

|  |  |  |
| --- | --- | --- |
| **Name** | **Data type** | **Description** |
| SourceIdentifier | MISF\_ID | This identifies the invoker, which is an MISF. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | This identifies the remote PoA that is the corresponding peer of the L2 exchange.a |
| LLInformation | LL\_FRAMES | (Optional) Carries link layer frames. |
| MN\_NAI | MISF\_ID | (Optional) Carries the Network Access Identifier assigned for use by the MN after movement to the target network. |
| TPoSIdentifier | MISF\_ID | (Optional) Identifies the target PoS. |
| KeyDerivationKey | ENCR\_BLOCK | (Optional) A key derivation key encrypted in a way recoverable by the TPoS. b |
| SALifeTime  | LIFETIME | (Optional) Lifetime of the Security Association |
| Status | STATUS | Status of the preregistration transfer with the TPoS. Code 3 (Authorization Failure) is not applicable. (See Table E.2 of IEEE Std 802.21-XXXX) |
| a Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN, and the PoA.b When (D)TLS is not used to establish the MIS security association between the MN and the TPoS, the default SALifeTime for MISK and derived keys is 65,536 seconds (slightly over 18 hours). This value may be overridden by passing a preferred value as the SALifeTime parameter in relevant MIS primitives. |

Change text in 5.12.1.3.2 of .21.1 as follows.

* + - * 1. **Semantics of service primitive**

MIS\_N2N\_Prereg\_Xfer.response (

 DestinationIdentifier,

 TargetLinkIdentifier,

 LLInformation,

 MN\_NAI,

 SALifeTime,

 Status

)

|  |  |  |
| --- | --- | --- |
| **Name** | **Data type** | **Description** |
| DestinationIdentifier | MISF\_ID | This identifies a remote MISF that will be the destination of this response. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | This identifies the remote PoA that is the corresponding peer of the L2 exchange. a |
| LLInformation | LL\_FRAMES | (Optional) Carries link layer frames. |
| MN\_NAI | MISF\_ID | (Optional) Carries the MN’s temporary Network Access Identifier assigned by the target network. |
| SALifeTime  | Lifetime TLV | (Optional) Lifetime of the Security Association b |
| Status | STATUS | Status of the preregistration transfer with the TPoS. Code 3 (Authorization Failure) is not applicable. (See Table E.2 of IEEE Std 802.21-XXXX) |
| a Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN, and the PoA.b When (D)TLS is not used to establish the MIS security association between the MN and the TPoS, the default SALifeTime for MISK and derived keys is 65,536 seconds (slightly over 18 hours). This value may be overridden by passing a preferred value as the SALifeTime parameter in relevant MIS primitives. |

Change text in 5.12.1.4.2 of .21.1 as follows.

* + - * 1. **Semantics of service primitive**

MIS\_N2N\_Prereg\_Xfer.confirm (

 SourceIdentifier,

 TargetLinkIdentifier,

 LLInformation,

 MN\_NAI,

 SALifeTime,

 Status

)

|  |  |  |
| --- | --- | --- |
| **Name** | **Data type** | **Description** |
| SourceIdentifier | MISF\_ID | This identifies the invoker, which is a remote MISF. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | This identifies the remote PoA that is the corresponding peer of the L2 exchange.a |
| LLInformation | LL\_FRAMES | (Optional) This carries link layer frames. |
| MN\_NAI | MISF\_ID | (Optional) This carries the MN’s Network Access Identifier. |
| SALifeTime  | Lifetime TLV | (Optional) Lifetime of the Security Association. b |
| Status | STATUS | Status of the preregistration transfer with the TPoS. Code 3 (Authorization Failure) is not applicable. Code 6 (the TPoS is identical to the SPoS), is not applicable. (SeeTable E.2 of IEEE Std 802.21-XXXX) |
| a Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN, and the PoA.b When (D)TLS is not used to establish the MIS security association between the MN and the TPoS, the default SALifeTime for MISK and derived keys is 65,536 seconds (slightly over 18 hours). This value may be overridden by passing a preferred value as the SALifeTime parameter in relevant MIS primitives. |