|  |  |
| --- | --- |
| Project | **IEEE 802.21.1 Media Independent Services**  **<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | Alternatives of key delivery mechanism described in 5.14 of Draft IEEE 802.21.1. |
| DCN | **21-15-00-0036-03-SAUC** |
| Date Submitted | **February 26, 2016** |
| Source(s) | Yoshikazu Hanatani (Toshiba) |
| Re: | IEEE 802.21.1 teleconference |
| Abstract | Suggested change in DCN 21-16-39-00 is reflected.  This contribution proposes alternatives of key delivery mechanism described in 5.14 of Draft IEEE 802.21.1. |
| Purpose | To provide a remedy for Cmt #106-109 of LB9. |
| 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> |

**Suggested remedy:**

Assumption: A SPoS and an MN have a SA generated by 21a.

The SPoS and a TPoS have another SA generated by 21a.  
 The SPoS is not compromised.

Questions:

1. Is MIS user generates a session key from a KeyDerivationKey K by using the key hierarchy described in 9.2.2 of 21m?  
    If the answer is Yes, Nonce-T and Nonce-N shall be added to some primitive.   
    If the answer is No, we should correct a text in “Effect on recept”.   
    Which is the correct answer?.

Answer: The session key is generated by MISF.

1. Nonce-N is selected by SPoS. Noce-N is used for establishing a session key between MN and TPoS. So, I think Nonce-N should be selected by TPoS.  
    Should we change it?

Answer: We make a changed draft, and then we will discuss it using the draft.

1. I am not sure .21a can be used between SPoS and TPoS. Please confirm it.  
   Answer: The interface between SPoS and TPoS can be protected through an out-of-the-scope mechanism (see the first paragraph of 5.14).
   * Nonce-N is generated by SPoS and Nonce-T is generated by MN. I think it is confusing. In this contribution, the names are chenged as follws.
     1. Nonce-N is generated by MN
     2. Nonce-T is generated by TPoS

*Change following clauses in Draft IEEE P802.21.1/D01.*

*Change 5.11.12 in Draft IEEE P802.21.1/D01 as follows.*

1. * + 1. **MIS\_Prereg\_Xfer.request**
          1. **Function**

This primitive is used to transport parameters and link layer frames from the MN’s MIS user to the MISF running on the MN’s serving the PoS (i.e., the SPoS) for preregistration signaling, including the establishment of a secure tunnel, between the MN and a target PoS (TPoS) in an appropriate target network.

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

MIS\_Prereg\_Xfer.request (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

TPoSIdentifier,

CandidateLinkList,

CiphersuiteCode

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **Name** | **Data type** | **Description** |
| DestinationIdentifier | MISF\_ID | Identifies an MISF as the destination of this request. |
| 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: included if the target link is known) Carries link layer frames. |
| TPoSIdentifier | MISF\_ID | (Optional) This identifies the target PoS (TPoS) that will be the destination of the link-layer frames. |
| CandidateLinkList | LIST (LINK\_PoA\_LIST) | (Optional) A list of PoAs, identifying candidate networks to which handover should be initiated. The list is sorted from most preferred first to least preferred last. The link information can include values and IEs from Table E.10, Table E.11, Table E.14, and Table F.1 of IEEE Std 802.21-XXXX, and Table F.1. |
| CiphersuiteCode | Octet(1) | (Optional) CiphersuiteCode (see Table 25 in 9.2.3 of IEEE Std 802.21-XXXX) is included when MN wishes to request use of a particular algorithm during the establishment of a security association with TPoS for the purposes of preregistration in the target network. |
| a Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN, and the PoA. | | |

* + - * 1. **When generated**

This primitive is generated by an MIS user on MN to preregister with a target PoS. The MN can send this primitive to instruct its serving PoS (i.e., the SPoS) to generate a Security Association with an appropriate TPoS when the SPoS and the TPoS reside on different nodes.

* + - * 1. **Effect on receipt**

If the TargetLinkIdentifier is not included, the SPoS shall use the CandidateLinkList (if included) to identify the appropriate TPoS that can initiate preregistration activities with an appropriate TPoA. In the absence of other information, the SPoS can use available link-type information and location information for the MN to identify an appropriate TPoS. After reception of this primitive, the SPoS’s MISF must generate an MIS\_Prereg\_Xfer.indication primitive destinated to the SPoS’s MIS user.

* + - 1. **MIS\_Prereg\_Xfer.indication**
         1. **Function**

This primitive is used by the SPoS’s MISF to notify the SPoS’s MIS user about the reception of an MIS\_Prereg\_Xfer request message.

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

MIS\_Prereg\_Xfer.indication (

SourceIdentifier,

TargetLinkIdentifier,

LLInformation,

TPoSIdentifier,

CandidateLinkList,

CiphersuiteCode

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **Name** | **Data type** | **Description** |
| SourceIdentifier | MISF\_ID | Identifies the invoker, an MN in the same network as the SPoS. |
| 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) This carries link layer frames. This attribute may be included if the target link is known. |
| TPoSIdentifier | MISF\_ID | (Optional) This identifies the target PoS |
| CandidateLinkList | LIST(LINK\_PoA\_LIST) | (Optional) A list of PoAs, identifying candidate networks to which handover should be initiated. The list is sorted from most preferred first to least preferred last. The link information can include values and IEs from Table E.10, Table E.11, Table E.14, and Table F.1 of IEEE Std 802.21-XXXX, and Table F.1. |
| CiphersuiteCode | Octet(1) | (Optional) CiphersuiteCode (see Table 25 in 9.2.3 of IEEE Std 802.21-XXXX) is included when the MN wishes to request use of a particular algorithm during the establishment of a security association with the TPoS for the purposes of preregistration in the target network. |
| a Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN, and the PoA. | | |

* + - * 1. **When generated**

This primitive is generated by an MISF after receiving an MIS\_Prereg\_Xfer request message.

* + - * 1. **Effect on receipt**

If TPoSIdentifier is not provided, the MIS user on the SPoS uses the information provided by the MN to identify an appropriate target PoS (TPoS). If the TPoS is hosted remotely (e.g., in a separate target network), the MIS user on the SPoS must generate a MIS\_N2N\_Prereg\_Xfer.request primitive for the TPoS. Otherwise, the MIS application must generate a MIS\_Prereg\_Xfer.response primitive and transmit that response to the MISF specified by the SourceIdentifier.

* + - 1. **MIS\_Prereg\_Xfer.response**
         1. **Function**

The SPoS’s MIS application uses this primitive to relay preregistration frames to the MN via the SPoS’s local MISF.

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

MIS\_Prereg\_Xfer.response (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

MN\_NAI,

TPoSIdentifier,

SALifeTime,

Status

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **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 |
| 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. | | |

* + - * 1. **When generated**

This primitive is generated by the MIS user on SPoS either: a) after receiving an MIS\_Prereg\_Xfer.indication primitive if the MIS user that received the corresponding MIS\_Prereg\_Xfer.request primitive did not invoke an MIS\_N2N\_Prereg\_Xfer.request primitive, or b) after receiving a MIS\_N2N\_Prereg\_Xfer.confirm primitive. If the SPoS has received a positive confirmation that the TPoS has accepted the Security Association, this will enable the MN to complete the establishment of the secure tunnel.

* + - * 1. **Effect on receipt**

The local MISF generates an MIS\_Prereg\_Xfer response message in order to provide the MN with the information previously requested in MIS\_N2N\_Prereg\_Xfer request.

* + - 1. **MIS\_Prereg\_Xfer.confirm**
         1. **Function**

This primitive is used to notify the MN’s MIS application about the reception of an MIS\_Prereg\_Xfer response message.

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

MIS\_Prereg\_Xfer.confirm (

SourceIdentifier,

TargetLinkIdentifier,

LLInformation,

MN\_NAI,

TPoSIdentifier,

KeyDerivationKey,

SALifeTime,

Status

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **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~~ | ~~OCTET(16)~~ | ~~(Optional) A key derivation key~~ ~~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.~~ | | |

* + - * 1. **When generated**

The MN’s MISF generates this primitive after receiving an MIS\_Prereg\_Xfer response message. If the MN included CiphersuiteCode with the MIS\_Prereg\_Xfer request message, the optional KeyDerivationKey will be included in the MIS\_Prereg\_Xfer response message so that the MN’s MISF can compute the keys necessary for communication with the TPoS and the TPoA according to 9.2.2 of IEEE Std 802.21-XXXX.

* + - * 1. **Effect on receipt**

The MIS user on the MN may generate another MIS\_Prereg\_Xfer.request primitive—for example, if preregistration procedures are not completed.

*Change 5.12.1 in Draft IEEE P802.21.1/D01 as follows.*

* 1. 1. **MIS\_N2N\_Prereg\_Xfer**

The primitives defined in this clause are used by MIS functions running on the SPoS and the TPoS to enable preregistration for MN on a target Point of Attachment. See Annex I for examples. The primitives provide the ability to transport link-layer frames for the target link over the MIS protocol between the source network PoS and the target PoS. Preregistration is conducted between the MN and the target PoA. As part of preregistration, media-specific authentication may be conducted with an authenticator deployed in the target PoA.

* + - 1. **MIS\_N2N\_Prereg\_Xfer.request** 
         1. **Function**

The SPoS generates this primitive to deliver link layer frames to the target PoS.

* + - * 1. **Semantics of Service Primitive**

MIS\_N2N\_Prereg\_Xfer.request (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

MNID,

CandidateLinkList,

CiphersuiteCode

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **Name** | **Data type** | **Description** |
| DestinationIdentifier | MISF\_ID | This identifies a remote MISF that will be the destination of this request. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | (Optional) Identifies the remote PoA as the corresponding peer of the L2 exchange;a shall be included if the target link is known. |
| LLInformation | LL\_FRAMES | (Optional) Carries link layer frames; shall be included if the target link is known. |
| MNID | MISF\_ID | (Optional) MISF\_ID of the MN to identify the MN’s Media Independent Root Key to be transferred to the target PoS. |
| CandidateLinkList | LIST (LINK\_PoA\_LIST) | (Optional) A list of PoAs, identifying candidate networks to which handover should be initiated. The list is sorted from most preferred first to least preferred last. This attribute shall not be included if the target link is known. |
| CiphersuiteCode | Octet(1) | (Optional) CiphersuiteCode (see Table 25 in 9.2.3 of IEEE Std 802.21-XXXX) is included when the MN wishes to request use of a particular algorithm during the establishment of a security association with the TPoS for the purposes of preregistration in the target network. |
| a Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN, and the PoA. | | |

* + - * 1. **When generated**

The MIS user on SPoS generates this primitive after receiving an MIS\_Prereg\_Xfer.indication primitive, to relay preregistration signaling to the target PoS. The SPoS may do this to relay link-layer frames or to establish a security association derived from KeyDerivationKey. In order to establish a SA between the TPoS and the MN the MISF of the SPoS produces KeyDerivationKey. Then SPoS’s MISF encrypts the service specific TLVs including Nonce-T using the mechanism specified in 9 of IEEE Std 802.21-XXXX, and transmits the result to the TPoS, where Nonce-T is the value received from the MN in the MIS\_Prereg\_Xfer message.

* + - * 1. **Effect on receipt**

The local MISF shall generate a MIS\_N2N\_Prereg\_Xfer request message to the remote MISF.

* + - 1. **MIS\_N2N\_Prereg\_Xfer.indication**
         1. **Function**

This primitive is used by the MISF of the TPoS to notify its MIS user of the reception of an MIS\_N2N\_Prereg\_Xfer request message.

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

MIS\_N2N\_Prereg\_Xfer.indication (

SourceIdentifier,

TargetLinkIdentifier,

,

MNID,

KeyDerivationKey

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **Name** | **Data type** | **Description** |
| SourceIdentifier | MISF\_ID | This identifies the invoker, which is a remote MISF. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | (Optional)This identifies the remote PoA that is the corresponding peer of the L2 exchange.a This attribute shall be included if the target link is known. |
| LLInformation | LL\_FRAMES | (Optional) carries link layer frames. This attribute shall be included only if the target link is known. |
| MNID | MISF\_ID | ID of the MN, used to index and compute the MN’s Media Independent Root Key to be established by the target PoS |
| KeyDerivationKey | OCTET(16) | A key derivation key |
| a Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. | | |

* + - * 1. **When generated**

TPoS’s MISF generates this primitive upon receiving a MIS\_N2N\_Prereg\_Xfer request message. If the MIS\_N2N\_Prereg\_Xfer request message include KeyDerivationKey *K* and Nonce-N, the MISF generates Nonce-T and it derives the key hierarchy from KeyDerivationKey *K*, Nonce-N, and Nonce-T as described in 9.2.2 of IEEE Std 802.21-XXXX, installing keys as necessary in the AAA used by the target network.

* + - * 1. **Effect on receipt**

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 KeyDerivationKey *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.

The MIS user must generate an MN\_NAI associated with the MNID provided; the two IDs are allowed to be the same.

The MIS application must subsequently generate an MIS\_N2N\_Prereg\_Xfer.response primitive and include MN\_NAI.

* + - 1. **MIS\_N2N\_Prereg\_Xfer.response**
         1. **Function**

This primitive is used by the TPoS’s MIS application to supply preregistration frames to the TPoS’s MISF.

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

MIS\_N2N\_Prereg\_Xfer.response (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

MN\_NAI,

SALifeTime,

Status

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **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. | | |

* + - * 1. **When generated**

This primitive is generated after receiving an MIS\_N2N\_Prereg\_Xfer.indication primitive.

* + - * 1. **Effect on receipt**

The MISF at the TPoS shall generate an MIS\_N2N\_Prereg\_Xfer response message in order to provide the required information until the authentication is finished.

* + - 1. **MIS\_N2N\_Prereg\_Xfer.confirm**
         1. **Function**

This primitive is used to notify the SPoS’s MIS user about the reception of an MIS\_N2N\_Prereg\_Xfer response message.

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

MIS\_N2N\_Prereg\_Xfer.confirm (

SourceIdentifier,

TargetLinkIdentifier,

LLInformation,

MN\_NAI,

SALifeTime,

Status

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **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.

* + - * 1. **When generated**

This primitive is generated by the remote MIS application after receiving a MIS\_N2N\_Prereg\_Xfer response message.

* + - * 1. **Effect on receipt**

The SPoS MIS application generates an MIS\_Prereg\_Xfer.response primitive with the information obtained from this primitive. The SPoS MISF retrieves its stored value for KeyDerivationKey which had previously been sent to the TPoS MISF, encrypting service specific TLVs including it using the SA between SPoS and MN as described in 9 of IEEE Std 802.21-XXXXfor use in the MIS\_Prereg\_Xfer response message.

*Change 5.13.3.19 in Draft IEEE P802.21.1/D01 as follows.*

1. * + 1. MIS\_Prereg\_Xfer Request

The MN’s MISF sends this message so that the SPoS transmits link layer frames to expedite preregistration with an appropriate TPoS, particularly to initiate proactive authentication for the establishment of a security association. The corresponding primitive is defined in 5.11.12.1. Nonce-N is included if the MN is requesting the SPoS to establish a security association with the TPoS. CandidateLinkList is included if the MN has information available about the desired target link. Nonce-N is generated by MN’s MISF.

|  |
| --- |
| MIS Header Fields (SID=3, Opcode=1, AID=13) |
| **Source Identifier** = sending MISF ID  (Source MISF ID TLV) |
| **Destination Identifier** = receiving MISF ID  (Destination MISF ID TLV) |
| TargetLinkIdentifier (optional)  (Link Identifier TLV) |
| LLInformation (optional)  (Link Layer Information TLV) |
| TPoSIdentifier (optional)  (TPoS Identifier TLV) |
| CandidateLinkList (optional)  (Link identifier list TLV) |
| CiphersuiteCode (optional) (Ciphersuite Code TLV) |
| Nonce-N (optional) (Nonce TLV) |

* + - 1. *Change 5.13.3.20 in Draft IEEE P802.21.1/D01 as follows.*MIS\_Prereg\_Xfer Response

This message is used by the MISF running on the SPoS to complete the establishment of a security association between an MN and an appropriate TPoS. The corresponding primitive is defined in 5.11.12.3. SALifetime, KeyDerivationKey, and Nonce-T are not sent unless the MN sent Nonce-N in the MIS\_Prereg\_Xfer request and the SPoS and the MN have a security association. When SALifetime and KeyDerivationKey are sent, the service specific TLVs shall be encrypted by the security association between the SPoS and the MN described in9 of IEEE Std 802.21-XXXX.

|  |
| --- |
| MIS Header Fields (SID=3, Opcode=2, AID=13) |
| **Source Identifier** = sending MISF ID  (Source MISF ID TLV) |
| **Destination Identifier** = receiving MISF ID  (Destination MISF ID TLV) |
| TargetLinkIdentifier (optional) (Link Identifier TLV) |
| LLInformation (optional) (Link Layer Information TLV) |
| MN\_NAI (optional) (Network Access Identifier TLV) |
| TPoSIdentifier (optional) (TPoS Identifier TLV) |
| KeyDerivationKey (optional) (Key TLV) |
| Nonce-T (optional) (Nonce TLV) |
| SALifeTime (optional) (KeyLifeTime TLV) |
| Status (Status TLV) |

*Change 5.13.3.21 in Draft IEEE P802.21.1/D01 as follows.*

* + - 1. MIS\_N2N\_Prereg\_Xfer Request

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 KeyDerivationKey must all be absent when the MISF and a remote MISF do not have a security association. When Nonce-T, Nonce-N, and the KeyDerivationKey are present, the service specific TLVs shall be encrypted by the security association between the MISF and the remote MISF as described in 9 of IEEE Std 802.21-XXXX.The MISF generates Nonce-N and the KeyDerivationKey.

|  |
| --- |
| MIS Header Fields (SID=3, Opcode=1, AID=14) |
| **Source Identifier** = sending MISF ID (Source MISF ID TLV) |
| **Destination Identifier** = receiving MISF ID (Destination MISF ID TLV) |
| TargetLinkIdentifier (optional) (Link Identifier TLV) |
| LLInformation (optional) (Link Layer Information TLV) |
| MNID (optional) (Mobile node MISF ID TLV) |
| CiphersuiteCode (optional) (Ciphersuite Code TLV) |
| KeyDerivationKey (optional) (Key TLV) |
| Nonce-N (optional) (Nonce TLV) |
| SALifeTime (optional) (KeyLifeTime TLV) |

* + - 1. MIS\_N2N\_Prereg\_Xfer Response

An MISF sends this message to complete the establishment of a security association between itself and the preregistering MN or to accomplish other layer-2 signaling. The corresponding primitive is defined in 5.12.1.3. The SALifeTime may be included if specified by the TPoS for the requested security association. The TPoS may also include the MN\_NAI parameter if the MNID parameter of the MIS\_N2N\_Prereg\_Xfer request message is not appropriate for use in the target network.

|  |
| --- |
| MIS Header Fields (SID=3, Opcode=2, AID=14) |
| **Source Identifier** = sending MISF ID (Source MISF ID TLV) |
| **Destination Identifier** = receiving MISF ID (Destination MISF ID TLV) |
| TargetLinkIdentifier (Link Identifier TLV) |
| LLInformation (optional) (Link Layer Information TLV) |
| MN\_NAI (optional) (Network Access Identifier TLV) |
| Nonce-T (optional) (Nonce TLV) |
| SALifeTime (optional) (KeyLifeTime TLV) |
| Status (Status TLV) |

*Change 5.14 in Draft IEEE P802.21.1/D01 as follows.*

* 1. PoS facilitated proactive authentication for single radio handover service
     1. Establishing MIS Security Association between roaming partners

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).

Other mechanisms for providing message integrity and confidentiality, such as IPSec and TLS over TCP, can also be used for protecting the communications between SPoS and TPoS.

Except for the initial network attachment, 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 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. In Clause 9 of Draft IEEE Std 802.21-XXX, an MIS SA can be established through (D) TLS or EAP. The methods specified there shall be used to establish an MIS SA between an MN and a TPoS so that TPoS can provide security service, in particular, can facilitate proactive authentication for an MN in a handover event. For single radio handover, an optimized MIS SA establishment mechanism is introduced to speed up when the home networks of SPoS and TPoS have an existing trust relationship through partnership agreement.

* + 1. Optimized MIS SA establishment for single radio handover service



This clause specifies one optimized MIS SA establishment for single radio handover service. It allows a TPoS to obtain a key derivation key *K* from a SPoS or from a higher level entity. The key derivation key K is used to derive other keys such as the media independent session key (MISK) as described in 9.2.1 of IEEE Std 802.21-XXXX between the MN and the TPoS, enabling further secure preregistration activities.

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. As discussed in 5.14.1, the protection mechanisms applied between SPoS and TPoS are out of the scope of this specification. If the key K is distributed by SPoS to MN and to TPoS, the key distribution is protected by MIH SA between MN and SPoS and by out of scope mechanisms between SPoS and TPoS.

In order to establish an SA between the MN and the TPoS, they need to exchange Nonce-N and Nonce-T through messages MIS\_Prereg\_Xfer Request, MIS\_Prereg\_Xfer Response, MIS\_N2N\_Prereg\_Xfer Request, and MIS\_N2N\_Prereg\_Xfer Response. They also need to agree on a cipher suite coded as c. With the information, MN and TPoS can derive the media independent session key (MISK) as specified in 9.2.2 of IEEE Std 802.21-XXXX.

Note:

1. The optimized MIH SA establishment is allowed only when a trust relationship has established between the network domains of SPoS and TPoS. It shall fall back to an SA establishment mechanism as specified in IEEE Std 802.21-XXXX whenever it is possible, or if any of the MN or TPoS requests so.

2. If protocol of establishing SAs between an MN and a TPoS is EAP, the optimized MIH SA etsblishment applies. In this case, the MN and the TPoS use key derivation key K as it is obtained through an EAP or ERP execution.

3. If protocol of establishing SAs between an MN and a TPoS is TLS, then the optimized SA establishment method does not apply, because the MN and the TPoS cannot use key derivation key K in TLS.

4. If any SPoS is compromised, the generated key K is compromised and so is the remaining of the PoS chains assuming that a TPoS will become a SPoS. To prevent such domino effect, the chain shall be limited. That is, after certain number of executions of the optimized SA establishment, it shall force an SA establishment through the methods specified in IEEE Std 802.21-XXXX.

* + 1. 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.