|  |  |
| --- | --- |
| 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 | **21-15-00-0036-00-SAUC** |
| Date Submitted | **February 18, 2016** |
| Source(s) | Yoshikazu Hanatani (Toshiba) |
| Re: |  |
| Abstract | This contribution propose alternatives of key delivery mechanism described in 5.14 of Draft IEEE 802.21.1. |
| Purpose | To discuss a remedy for Cmt #106-109 of LB9. This contribution propose two alternatives. We should select an alternative to solve Cmt #106-109 of LB9.1. Remove 5.14. (Proposed by DCN 21-16-0029-00)
2. Use 21a-generated SA to deriver new key derivation key. (Proposed in this contribution as Remedy 1.)
3. Use 21d to deriver new key derivation key. (Proposed in this contribution as Remedy 2)
4. Another solution.
 |
| 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> |

**Contributor’s opinion:**

 At a viewpoint of security, removing clause 5.14 is no problem. So, I will agree with the removing of 5.14, if all BRC members are agree with it.

 If we keep a simplified key distribution mechanism described in 5.14, I believe we should provide a specific secure key delivery method.

 If the users use an insecure PRF, the current method described in 5.14 is insecure. And, in fact, there are so many insecure PRFs. For users who are not so familiar with PRFs, we should specify a secure function, at least.

 I suggest to remove the key distribution mechanism using PRF and to use existing mechanism defined by 21a or 21d.

**Outline of the remedies:**

Lily proposed a remedy by removing clause 5.14.

I propose two remedies.

 **Remedy 1**: using 21a-generated SA to distribute new key.

Strong point:

* MIS\_Prereg\_Xfer and MIS\_N2N\_Xfer are simplified.
* New message or primitive is not required.

Weak point:

* The domino effect is still remained. Need warning texts.
* I am not sure .21a can be used between SPoS to TPoS. Please confirm it.
* The ID\_TYPE of security association is 0: TLS-generated, 1: EAP-generated, or 2: GKB-generated only. But, the session key delivered by MIS\_Prereg\_Xfer and MIS\_N2N\_Prereg\_Xfer is not TLS-generated SA, EAP-generated SA, or GKB-generated SA. We should assign new ID type for the session key.

 **Remedy 2:** using 21d to distribute new key derivation key.

Strong point:

* The domino effect can be removed.
* MIS\_Prereg\_Xfer and MIS\_N2N\_Xfer are simplified.

Weak point:

* A PoS with group manager is required, and MNs and PoSs using MIS\_Prereg\_Xfer and MIS\_N2N\_Prereg\_Xfer based key distribution shall have device keys.
* New message will be required to inform members who are require new group key.

If we agree with this mechanism, I can provide the detail. (Hana)

**Suggested remedy 1:**

Using existing SA based on .21a for the key delivery.

Removing the key delivery mechanism using a shared PRF.

Strong point:

 MIS\_Prereg\_Xfer and MIS\_N2N\_Xfer are simplified.

 New message or primitive is not required.

Weak point:

1. The domino effect is still remained. Need warning texts.
2. I am not sure .21a can be used between SPoS to TPoS. Please confirm it.
3. The ID\_TYPE of security association is 0: TLS-generated, 1: EAP-generated, or 2: GKB-generated only. But, the session key delivered by MIS\_Prereg\_Xfer and MIS\_N2N\_Prereg\_Xfer is not TLS-generated SA, EAP-generated SA, or GKB-generated SA. We should assign new ID type for the session key.

Detail of suggested remedy 1:

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

 The SPoS and a TPoS have another SA generated by .21a.

* + - 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. CiphersuiteCode 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-T 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) |
|  |

* + - 1. 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, and KeyDerivationKey are not sent unless the MN sent CiphersuiteCode 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 Draft IEEE P802.21m.

|  |
| --- |
| 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) |
|  |
| SALifeTime (optional) (KeyLifeTime TLV) |
| Status (Status TLV) |

* + - 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. The KeyDerivationKey must be absent when the MISF and a remote MISF do not have a security association. When the KeyDerivationKey is included, the service specific TLVs shall be encrypted by the security association between the MISF and the remote MISF as described in 9 of Draft IEEE P802.21m.

|  |
| --- |
| 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) |
|  |
|  |
| SALifeTime (optional) (KeyLifeTime TLV) |

* 1. Proactive authentication
		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).

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.

* + 1. Key generation and distribution by SPoS

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.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

This specifies one algorithm to allow 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.

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.

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.

The SPoS shall encrypt the entire contents by using the SAsthat 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 key derivation key; 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.

* + 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.

**Suggested remedy 2:**

Using 21d, GKB-generated SA, for the key delivery.

Removing the key delivery mechanism using a shared PRF.

Strong point:

1. The domino effect can be removed.
2. MIS\_Prereg\_Xfer and MIS\_N2N\_Xfer are simplified.

Weak point:

1. A PoS with group manager is required, and MNs and PoSs using MIS\_Prereg\_Xfer and MIS\_N2N\_Prereg\_Xfer based key distribution shall have device keys.
2. New message will be required.

If we agree with this mechanism, I can provide the detail. (Hana)

Assumption: A TPoS and an MN have a device key issued by a PoS with group manager.

Proposed call flow

　The SPoS does not generate the key derivation key for the TPoS and MN.

 The SPoS informs an information of TPoS and MN to the PoS with GM.

 The PoS with GM generates a group key as the key derivation key, and it sent the group key to SPoS and TPoS using MIS\_Push\_Group\_Manipulate message.

 The TPoS and MN generate a session key from the key derivation key.

****

MIS\_Push\_Group\_Manipulate

**New message**
(request to issue a group key for the MN and TPoS)

PoS with GM

To inform the information of TPoS and MN from the SPoS, we should define new message and primitive.