|  |  |  |
| --- | --- | --- |
| Project | **IEEE 802.21 MIHS**  **<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** | |
| Title | **Proposed remedy for Comments 29, 30, 46 to 50** | |
| DCN | **21-14-0xxx-00-MuGM** | |
| Date Submitted | **May 13, 2014** | |
| Source(s) | Yoshihiro Ohba (Toshiba) |  |
| Re: | IEEE 802.21 Session #62 in Waikoloa | |
| Abstract | This document describes a proposed remedy for LB7c Comments #29, #30, #46 through #50 about MIH\_Pull\_Certificate. | |
| Purpose | For LB7c Comment Resolution | |
| 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> | |

# Comments

Comments on 7.4.33.3 (MIH\_Pull\_Certificate primitive):

* Cmt #29: What do we mean by "An MIH User generates this primitive using a leaf key corresponding with the certificate requester." This primitive is sent by a PoS, you mean that the PoS cyphers the certificate with the leaf key corresponding to the node? Is this explained somewhere?
* Cmt #30: Here "leaf key" is used in the sentence "An MIH User generates this primitive using a leaf key corresponding with the certificate requester." In fact, a leaf key is one of the device keys for a leaf node. For example, in a depth-3 tree, node 000 will have device keys k<>, k<0>, k<00>, and k<000>, where k<000> is called a leaf key. In the whole document, the device keys are only used to encapsulate a group key in the GKB. The usage of the device key for this purpose has never been clear or discussed. Furthermore, the title of the subclause is "when generated" not "how generated". The sentence does not seem right in any case. If this is only for sending a certificate, why a leaf key is needed? what is "a leaf key corresponding with the certificate request. A leaf key is a symmetric key. How could the responder know the key for the requestor?

Comments on 8.6.1.27 (MIH\_Pull\_Certificate request message) and 8.6.1.28 (MIH\_Pull\_Certificate response message):

* Cmt #46: In the sentences "This message is used by the MIHF to deliver a credential from a PoS used for creating an EAP-generated MIH SA", is the credential used for creating an EAP-generated SA?
* Cmt #47: Need to define somewhere how the decryption using the leaf key is done
* Cmt #48: In the sentence "Certificate is decrypted by the leaf key of the MN", it is not clear why a certificate needs to be encrypted. If a leaf key is a symmetric key, how does the PoS know the key? [Also see comment on definition of leaf key"].
* In the sentence "This message is used by the MIHF to deliver a credential encrypted by the leaf key that the MIH node identified by the Destination Identifier holds to the MIH node," what is the credential? Is it a certificate? If it is a certificate, why does it need to be encrypted? In fact, the sentence is not readable. In particular, the phrase "the leaf key that the MIH node identified by the Destination Identifier holds to the MIH node" is very unclear. What is "holds to the MIH node"?

# Discussion

The use of a leaf key in MIH\_Pull\_Certificate is a leftover of LB7b comment resolution, and should not be used for MIH\_Pull\_Certificate

# Suggested Remedy:

[1] Change 7.4.33.3.3 as follows:

**7.4.33.3.3 When generated**

An MIH User generates this primitive ~~using a leaf key corresponding with the certificate requester~~ in response to MIH\_Pull\_Certificate.indication primitive.

[2] Change 8.6.1.26 as follows:

**8.6.1.26 MIH\_Pull\_Certificate request**

The corresponding MIH primitive of this message is defined in 7.4.33.1.

This message is used by the MIHF to request a PoS certificate from ~~credential to~~ the PoS identified by the Destination Identifier.

[3] Change 8.6.1.27 as follows:

**8.6.1.27 MIH\_Pull\_Certificate response**

The corresponding MIH primitive of this message is defined in 7.4.33.3. This message is used by the MIHF to deliver a PoS certificate ~~credential~~ from a PoS to the sender of an MIH\_Pull\_Certificate request message ~~used for creating an EAP-generated MIH SA. Certificate is decrypted by the leaf key of the MN~~.