|  |  |  |
| --- | --- | --- |
| Project | **IEEE 802.21 MIHS**  **<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** | |
| Title | **Proposed remedy for Comment #47** | |
| DCN | **21-14-0058-00-MuGM** | |
| Date Submitted | **March 20, 2014** | |
| Source(s) | Yoshihiro Ohba (Toshiba) |  |
| Re: | IEEE 802.21 Session #61 in Beijing | |
| Abstract | This document describes a proposed remedy for LB7b Comment #47 about MIH\_Pull\_Credential primitives. | |
| Purpose | To addresses LB7b Comment #47. | |
| 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> | |

[1] *Change 7.4.33 as follows.*

**7.4.33 MIH\_Pull\_Certificate~~Credential~~**

**7.4.33.1 MIH\_Pull\_Certificate~~Credential~~.request**

**7.4.33.1.1 Function**

This primitive is generated by an MN or a PoS and it is used to request sending of a PoS certificate from the destination PoS to the requestor.

**7.4.33.1.2 Semantics of service primitive**

MIH\_Pull\_Certificate~~Credential~~.request (

DestinationIdentifier,

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **Name** | **Data Type** | **Description** |
| DestinationIdentifier | MIHF\_ID | This identifies a remote MIHF that will be the destination  of this request.~~Specifies the sender of the credential.~~ |

**7.4.33.1.3 When generated**

An MN generates this primitive for requesting a PoS credential ~~or for credential updates~~.

**7.4.33.1.4 Effect on receipt**

Upon receipt of this primitive, the MIHF on the MN sends the corresponding MIH\_Pull\_Certificate~~Credential~~ request message to the ~~destination MN or~~ PoS.

**7.4.33.2 MIH\_Pull\_Certificate~~Credential~~.indication**

**7.4.33.2.1 Function**

This primitive is generated by an MIHF that receives an MIH\_Pull\_Certificate~~Credential~~ request message in order to inform the MIH User.

**7.4.33.2.2 Semantics of service primitive**

MIH\_Pull\_Certificate~~Credential~~.indication (

SourceIdentifier,

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **Name** | **Data Type** | **Description** |
| SourceIdentifier | MIHF\_ID | This identifies the invoker of this primitive, which is  a remote MIHF.  ~~Identifies the requester of the~~  ~~credential.~~ |

**7.4.33.2.3 When generated**

This primitive is generated by an MIHF when an MIH\_Pull\_Certificate~~Credential~~ request message is received.

**7.4.33.2.4 Effect on receipt**

Upon reception of this primitive, the MIH user generates an MIH\_Pull\_Certificate~~Credential~~.response to deliver a PoS certificate~~credential~~ to the requester.

**7.4.33.3 MIH\_Pull\_Certificate~~Credential~~.response**

**7.4.33.3.1 Function**

This primitive is generated by an MIH User in order to deliver a PoS certificate~~credential~~ to an MN or other PoS ~~for MIH protocol protection as described in IEEE Std 802.21a-2012 Section 9~~.

**7.4.33.3.2 Semantics of service primitive**

MIH\_Pull\_Certificate~~Credential~~.response (

DestinationIdentifier,

Certificate~~EncryptedCredential~~

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **Name** | **Data Type** | **Description** |
| DestinationIdentifier | MIHF\_ID | This identifies a remote MIHF that will be the destination  of this response.~~Specifies the sender of the credential.~~ |
| Certificate~~EncryptedCredential~~ | CERTIFICATE~~ENCRYPTED\_KEY~~ | A PoS's X.509 certificate for  signature-based MIH protection as described in 8.4.2.~~Encrypted credential used for~~  ~~creating an EAP-generated MIH SA.~~ |

**7.4.33.4 MIH\_Pull\_Certificate~~Credential~~.confirm**

**7.4.33.4.1 Function**

This primitive is generated by an MIHF that receives an MIH\_Pull\_Certificate~~Credential~~ response, in order to inform of the PoS certificate~~credential~~ received by the MIHF ~~User~~.

**7.4.33.4.2 Semantics of service primitive**

MIH\_Pull\_Certificate~~Credential~~.confirm (

SourceIdentifier,

Certificate~~Credential~~

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **Name** | **Data Type** | **Description** |
| SourceIdentifier | MIHF\_ID | This identifies the invoker of this primitive, which is  a remote MIHF. ~~Identifies the remote MIHF that~~  ~~invoked MIH\_Pull\_Credential~~  ~~response.~~ |
| Certificate~~Credential~~ | CERTIFICATE~~KEY~~ | A PoS's X.509 certificate for  signature-based MIH protection as described in 8.4.2. ~~A credential for MIH protection as~~  ~~described in Section 9 of IEEE Std 802.21a-2012~~ |

**7.4.33.4.3 When generated**

The MIHF that receives an MIH\_Pull\_Certificate~~Credential~~ response message generates this primitive to indicate the PoS ceritificate~~credential~~.

**7.4.33.4.4 Effect on receipt**

Upon reception of this primitive, the MIH User installs the PoS certificate for signature verification of MIH PDUs sent by the remote MIHF.

~~After verification, validated credential keys within their expiration period can be utilized for IEEE 802.21a.~~

[2] In 8.6.1.26 and 8.6.1.27:

- Change MIH\_Pull\_Credential to MIH\_Pull\_Certificate

- Change parameter name “EncryptedCredential” to “Certificate”

- Change Encrypted Credential TLV to Certificate TLV

[3] In 7.4.34, 8.6.1.28 and 8.6.1.29:

- Change MIH\_Push\_Credential to MIH\_Push\_Certificate

- Change parameter name “Credential” to “Certificate”.

- Change parameter name “CredentialStatus” to “CertificateStatus”

- Change parameter name “CredentialSerialNumber” to “CertificateSerialNumber”

- Change Credential TLV to Certificate TLV

- Change Credential Status TLV to Certificate Status TLV

- Change Credential Serial Number TLV to Certificate Serial Number TLV

[4] In 7.4.35, 8.6.1.30, 8.6.1.31:

- Change MIH\_Revoke\_Credential to MIH\_Revoke\_Certificate

- Change parameter name “CredentialStatus” to “CertificateStatus”

- Change parameter name “CredentialSerialNumber” to “CertificateSerialNumber”

- Change parameter name “CredentialRevocation” to “CertificateRevocation”

- Change Credential Status TLV to Certificate Status TLV

- Change Credential Serial Number TLV to Certificate Serial Number TLV

- Change Credential Revocation Signature TLV to Certificate Revocation Signature TLV

[5] In Table L.2,

Change “Credential Revocation Signature” to “Certificate Revocation Signature”

Change “Credential” to “Certificate”

Change “Credential Serial Number” to “Certificate Serial Number”

Change “Credential Status” to “Certificate Status”