|  |  |
| --- | --- |
| Project | **IEEE 802.21m Media Independent Services**  **<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **Proposed remedy for Cmt #18 of LB10** |
| DCN | **21-16-0077-01-REVP** |
| Date Submitted | **May 19, 2016** |
| Source(s) | Yoshikazu Hanatani (Toshiba) |
| Re: | Session #74, Big Island, HI, USA |
| Abstract | MIS\_Push\_Certificate response message contains Certificate Serial Number Info TLV. But, MIS\_Push\_Certificate.response primitive does not contain CertificateSerialNumber parameter. So, generating method of Certificate Serial Number Info TLV from MIS\_Push\_Certificate.response primitive is unclear.  This contribution proposes deleting Certificate Serial Number Info TLV from MIS\_Push\_Certificate response message, and fixing editorial errors related to Certificate Serial Number Info TLV. |
| Purpose | Suggested remedy for Cmt #18 in LB10. |
| 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> |

Comment:

CertificateSerialNumbers parameter is contained in MIS\_Push\_Certificate response message, however the parameter is not contained in the corresponding MIS primitive that is defined in 7.4.23.3.

Problem:

MIS\_Push\_Certificate response message contains Certificate Serial Number Info TLV. But, MIS\_Push\_Certificate.response primitive does not contain CertificateSerialNumber parameter. So, generating method of Certificate Serial Number Info TLV from MIS\_Push\_Certificate.response primitive is unclear.

In some use case, CertificateSerialNumber parameter in Certificate Serial Number Info TLV is useful for managing certificates in an MIS user, but MIS\_Push\_Certificate.confirm does not include CertificateSerialNumber parameter.

# Ex. When a PoS issues two MIS\_Push\_Certificate request messages simaltanusly, CertificateSerialNumber parameter is required to indistingush MIS\_Push\_Certificate.confirm primitive.

There are Certificate Serial Number TLV which is undefined TLV. It should be Certificate Serial Number Info TLV.

Suggested remedy:

Delete Certificate Serial Number Info TLV from MIS\_Push\_Certificate response message.

Change Certificate Serial Number TLV to Certificate Serial Number Info TLV.

--------------------------------------



1. * + 1. MIS\_Push\_Certificate.response
          1. Function

This primitive is generated by an MIS User to acknowledge receipt of a credential from a PoS.

* + - * 1. Semantics of service primitive

MIS\_Push\_Certificate.response (

DestinationIdentifier,

CertificateSerialNumbers,

CertificateStatus)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| DestinationIdentifier | MISF\_ID | Specifies the sender of the credential. |
| CertificateSerialNumbers | CERT\_SERIAL\_NUMBER | X.509 certificate subfield -- serial number |
| CertificateStatus | CERT\_STATUS | Indicates whether a credential has been verified and is now in use by the recipient.  One of the following values is used:  1: Certificate Valid  2: Certificate Revoked  3: Certificate Expired  4: Verification Failed |

* + - * 1. When generated

An MIS User generates this primitive after receiving and processing of credential.

* + - * 1. Effect on receipt

An MIS\_Push\_Certificate response message is sent back to the sender of the credential to indicate a serial number in the credential and a status of the credential by providing the CertificateStatus. When CertificateStatus is “Certificate Valid,” the validated credential public keys can be utilized for multicast message exchange within their expiration period.

* + - 1. MIS\_Push\_Certificate.confirm
         1. Function

This primitive is generated by an MISF that receives an MIS\_Push\_Certificate response message to indicate the status of the credential inspection.

* + - * 1. Semantics of service primitive

MIS\_Push\_Certificate.confirm (

SourceIdentifier,

CertificateSerialNumbers,

CertificateStatus

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| SourceIdentifier | MISF\_ID | Identifies the remote MISF that invoked MIS\_Revoke\_Certificate.response. |
| CertificateSerialNumbers | CERT\_SERIAL\_NUMBER | X.509 certificate subfield -- serial number |
| CertificateStatus | CERT\_STATUS | Indicates whether a credential has been verified and is now in use by the recipient. |

* + - * 1. When generated

The MISF that receives an MIS\_Push\_Certificate response message generates this primitive to indicate the serial number in the credential and the status of the credential inspection.

* + - * 1. Effect on receipt

If CertificateStatus is “Certificate Valid”, then it indicates to the MIS User that a receiver of the MIS\_Push\_Certificate request message is capable of receiving signed multicast messages.

--------------------------------------

8.6.1.33 MIS\_Revoke\_Certificate indication

The corresponding MIS primitive of this message is defined in 7.4.24.1.

This message is used by the MISF to revoke a credential.

|  |
| --- |
| MIS Header Fields (SID=1, Opcode=3, AID=15) |
| **Source Identifier =** sending MISF ID (Source MISF ID TLV) |
| **Destination Identifier =** receiving MISF ID (Destination MISF ID TLV) |
| (Optional) CertificateSerialNumber  (Certificate Serial Number Info TLV) |
| CertificateRevocation  (Certificate Revocation Signature TLV) |
| (Optional) IssuerName  (Issuer Name TLV) |

8.6.1.34 MIS\_Revoke\_Certificate request

The corresponding MIS primitive of this message is defined in 7.4.24.1.

This message is used by the MISF to revoke a credential.

|  |
| --- |
| MIS Header Fields (SID=1, Opcode=1, AID=15) |
| **Source Identifier =** sending MISF ID (Source MISF ID TLV) |
| **Destination Identifier =** receiving MISF ID (Destination MISF ID TLV) |
| (Optional) CertificateSerialNumber  (Certificate Serial Number Info TLV) |
| CertificateRevocation  (Certificate Revocation Signature TLV) |
| (Optional) IssuerName  (Issuer Name TLV) |