|  |  |
| --- | --- |
| Project | **IEEE 802.21m Revision Project**  **<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **Method for adding indication messages to MIS\_Push\_Certificate command and MIS\_Revoke\_Certificate command** |
| DCN | **21-16-0051-00-REVP** |
| Date Submitted | **March 16, 2016** |
| Source(s) | Yoshikazu Hanatani (Toshiba) |
| Re: | Session #73, Macau |
| Abstract | The MIS\_Push\_Certificate command and the MIS\_Revoke\_Certificate in Draft IEEE P802.21m/D01 do not support indication messages. The indication messages are useful for reducing a traffic of response messages when the number of recipients of MIS command is huge. This contribution provides a method to support the indication messages by using ResponseFlag parameter. |
| Purpose | Updating Draft IEEE P802.21m/D01. |
| 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> |

Change 7.4.23 as follows

1. * 1. MIS\_Push\_Certificate
        1. MIS\_Push\_Certificate.request
           1. Function

This primitive is generated by an MIS User at the PoS to send a Certificate to a destination PoS(es) or MN(s).

* + - * 1. Semantics of service primitive

MIS\_Push\_Certificate.request (

DestinationIdentifier,

ResponseFlag,

Certificate

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| DestinationIdentifier | MISF\_ID | Specifies the recipient(s) of the credential. |
| ResponseFlaga | RESPONSE\_FLAG | (Optional) Flag that represents whether or not a response is needed. |
| Certificate | CERTIFICATE | A PoS’s X.509 certificate. |
| a If the ResponseFlag parameter is not present, the MISF shall generate a request message, otherwise the MISF generates either a request or an indication message, based on the ResponseFlag parameter. | | |

* + - * 1. When generated

A PoS generates this primitive for initial provisioning of credentials or for credential updates.

* + - * 1. Effect on receipt

Upon receipt of this primitive, the MISF on the PoS sends the corresponding MIS\_Push\_Certificate request message or MIS\_Push\_Certificate indication message to the destination MN(s) or PoS(es), based on the ResponseFlag parameter.

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

This primitive is generated by an MISF to notify a local MIS User that an MIS\_Push\_Certificate request message has been received.

* + - * 1. Semantics of service primitive

MIS\_Push\_Certificate.indication (

SourceIdentifier,

ResponseFlag.

Certificate

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| SourceIdentifier | MISF\_ID | Identifies the sender of the credential. |
| ResponseFlaga | RESPONSE\_FLAG | (Optional) Flag that represents whether or not a response is needed. |
| Certificate | CERTIFICATE | A PoS’s X.509 certificate. |
| a If the ResponseFlag parameter is not present, the MISF shall generate a response message, otherwise the MISF may generate either a response message or no response message, based on the ResponseFlag parameter. | | |

* + - * 1. When generated

This primitive is generated by an MISF when an MIS\_Push\_Certificate request message is received.

* + - * 1. Effect on receipt

Upon receipt of this primitive, an MIS user on an MN or a PoS verifies a X.509 certificate in the Certificate. The result of verification is provided back to push requester via CertificateStatus parameter in MIS\_Push\_Certificate.response primitive. The CertificateStatus parameter value is set as follows. If the X.509 certificate is revoked by a certificate revocation list then CertificateStatus is set to “Certificate Revoked,” else if the X.509 is expired then CertificateStatus is “Certificate Expired,” else if a signature in X.509 is not valid then CertificateStatus is set to “Verification Failed”, else CertificateStatus is set to “Certificate Valid.”

If the ResponseFlag parameter is not present, or ResponseFlag parameter is present and its value is TRUE, the MIS User shall generate an MIS\_Configuration\_Update.response primitive.

* + - 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,

CertificateStatus

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| DestinationIdentifier | MISF\_ID | Specifies the sender of the credential. |
| 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 status of a 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,

CertificateStatus

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| SourceIdentifier | MISF\_ID | Identifies the remote MISF that invoked MIS\_Revoke\_Certificate.response. |
| 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 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.

Change 7.4.24 as follows

* + 1. MIS\_Revoke\_Certificate
       1. MIS\_Revoke\_Certificate.request
          1. Function

This primitive is generated by a PoS used to revoke a credential.

* + - * 1. Semantics of service primitive

MIS\_Revoke\_Certificate.request (

DestinationIdentifier,

ResponseFlag,

CertificateSerialNumberList,

CertificateRevocation,

IssuerName

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| DestinationIdentifier | MISF\_ID | Specifies an MISF or a group of MISF peers to revoke the credential. |
| ResponseFlaga | RESPONSE\_FLAG | (Optional) Flag that represents whether or not a response is needed. |
| CertificateSerialNumberList | CERT\_SERIAL\_NUMBER\_INFO | List of revoked X.509 certificate subfield – serial number, Bloom Filter of revoked X.509 certificate subfield – serial number, or X.509 Certificate Revocation List. |
| CertificateRevocation | SIGNATURE | (Optional) Digital signature for a revoked X.509 certificate serial numbers generated by CA. This parameter shall be contained if and only if List or Bloom Filter of revoked X.509 certificate subfield serial numbers is contained in CertificateSerialNumberList. |
| IssuerName | OCTET\_STRING | (Optional) Distinguished name of the issuer of the revoked certificates. |
| aIf the ResponseFlag parameter is not present, the MISF shall generate a request message, otherwise the MISF generates either a request or an indication message, based on the ResponseFlag parameter. | | |

* + - * 1. When generated

The MIS user generates this primitive to revoke credentials.

* + - * 1. Effect on receipt

Upon receipt of this primitive, the MISF on the PoS generates and sends the corresponding MIS\_Revoke\_Certificate request message or MIS\_Revoke\_Certificate indication message to the destination MISF(s) based on the ResponseFlag parameter.

* + - 1. MIS\_Revoke\_Certificate.indication
         1. Function

This primitive is generated by an MISF to revoke a credential stored in MN(s) and PoS(es).

* + - * 1. Semantics of service primitive

MIS\_Revoke\_Certificate.indication (

SourceIdentifier,

ResponseFlag,

CertificateSerialNumberList,

CertificateRevocation,

IssuerName

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| SourceIdentifier | MISF\_ID | Specifies the remote MISF that invoked MIS\_Revoke\_Certificate.request primitive. |
| ResponseFlaga | RESPONSE\_FLAG | (Optional) Flag that represents whether or not a response is needed. |
| CertificateSerialNumberList | CERT\_SERIAL\_NUMBER\_INFO | List of revoked X.509 certificate subfield – serial number, Bloom Filter of revoked X.509 certificate subfield – serial number, or X.509 Certificate Revocation List. |
| CertificateRevocation | SIGNATURE | (Optional) Digital signature for a revoked X.509 certificate serial numbers generated by CA. This parameter shall be contained if and only if List or Bloom Filter of X.509 certificate subfield serial numbers is contained in CertificateSerialNumberList. |
| IssuerName | OCTET\_STRING | (Optional) Distinguished name of the issuer of the revoked certificates. |
| a If the ResponseFlag parameter is not present, the MISF shall generate a response message, otherwise the MISF may generate either a response message or no response message, based on the ResponseFlag parameter. | | |

* + - * 1. When generated

This primitive is generated by an MISF on an MN or a PoS when receiving an MIS\_Revoke\_Certificate request message from a remote MISF.

* + - * 1. Effect on receipt

Upon receipt of this primitive, if a CertificateRevocation is presented, an MIS user on an MN or a PoS verifies a signature in the CertificateRevocation, else the MIS user verifies a signature contained in X.509 Certificate Revocation List in the CertificateSerialNumberList. If the signature is valid and certificate serial numbers indicated by the CertificateSerialNumberList are present, then it deprecates the certificate specified by the CertificateSerialNumber and invokes an MIS\_Revoke\_Certificate.response primitive with CERT\_STATUS "Certificate Revoked", else if the certificate serial numbers indicated by the CertificateSerialNumberList are not present, it invokes an MIS\_Revoke\_Certificate.response primitive with CERT\_STATUS “Not Present”. If the signature is not valid, it invokes an MIS\_Revoke\_Certificate.response primitive with CERT\_STATUS "Verification Failed".

If the ResponseFlag parameter is not present, or ResponseFlag parameter is present and its value is TRUE, the MIS User shall generate an MIS\_Push\_Group\_Manipulate.response primitive.

* + - 1. MIS\_Revoke\_Certificate.response
         1. Function

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

* + - * 1. Semantics of service primitive

MIS\_Revoke\_Certificate.response (

DestinationIdentifier,

CertificateStatus

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| SourceIdentifier | MISF\_ID | Specifies the remote MISF that invoked MIS\_Revoke\_Certificate.request primitive. |
| 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:  0: Not Present  2: Certificate Revoked  4: Verification Failed |

* + - * 1. When generated

This primitive is generated by an MIS user on an MN or a PoS when receiving an MIS\_Revoke\_Certificate.indication primitive.

* + - * 1. Effect on receipt

Upon receipt of this primitive, an MIS user on an MN or a PoS deprecate the credential specified by the CertificateSerialNumber and invokes an MIS\_Revoke\_Certificate.confirm primitive.

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

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

* + - * 1. Semantics of service primitive

MIS\_Revoke\_Certificate.confirm (

SourceIdentifier,

CertificateStatus

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| SourceIdentifier | MISF\_ID | Identifies the remote MISF that invoked MIS\_Revoke\_Certificate.response. |
| CertificateStatus | CERT\_STATUS | Indicates whether a credential has been revoked. |

* + - * 1. When generated

The MISF that receives an MIS\_Revoke\_Certificate response message generates this primitive to indicate the status of the credential revocation.

* + - * 1. Effect on receipt

If CertificateStatus indicates success for all the MISF peers to which credential revocation request was sent, the PoS can change status of the credential to revoked.

Change 8.6.1.3o to 8.6.1.33 as follows

1. * + 1. MIS\_Push\_Certificate indication

The corresponding MIS primitive of this message is defined in 7.4.23.1.

This message is used by the MISF to deliver a credential encrypted by the leaf key that the MIS node identified by the Destination Identifier holds to the MIS node.

|  |
| --- |
| MIS Header Fields (SID=1, Opcode=3, AID=14) |
| **Source Identifier =** sending MISF ID (Source MISF ID TLV) |
| **Destination Identifier =** receiving MISF ID (Destination MISF ID TLV) |
| Certificate  (Certificate TLV) |

* + - 1. MIS\_Push\_Certificate request

The corresponding MIS primitive of this message is defined in 7.4.23.1.

This message is used by the MISF to deliver a credential encrypted by the leaf key that the MIS node identified by the Destination Identifier holds to the MIS node.

|  |
| --- |
| MIS Header Fields (SID=1, Opcode=1, AID=14) |
| **Source Identifier =** sending MISF ID (Source MISF ID TLV) |
| **Destination Identifier =** receiving MISF ID (Destination MISF ID TLV) |
| Certificate  (Certificate TLV) |

* + - 1. MIS\_Push\_Certificate response

The corresponding MIS primitive of this message is defined in 7.4.23.3.

This message is used by the MISF to acknowledge receipt of a credential from a PoS.

|  |
| --- |
| MIS Header Fields (SID=1, Opcode=2, AID=14) |
| **Source Identifier =** sending MISF ID (Source MISF ID TLV) |
| **Destination Identifier =** receiving MISF ID (Destination MISF ID TLV) |
| CertificateSerialNumbers  (Certificate Serial Number Info TLV) |
| CertificateStatus  (Certificate Status TLV) |

* + - 1. 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 TLV) |
| CertificateRevocation  (Certificate Revocation Signature TLV) |
| (Optional) IssuerName  (Issuer Name TLV) |

* + - 1. 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 TLV) |
| CertificateRevocation  (Certificate Revocation Signature TLV) |
| (Optional) IssuerName  (Issuer Name TLV) |

* + - 1. MIS\_Revoke\_Certificate response

The corresponding MIS primitive of this message is defined in 7.4.24.3.

This message is used by the MISF to acknowledge receipt of a credential revocation request from a PoS.

|  |
| --- |
| MIS Header Fields (SID=1, Opcode=2, AID=15) |
| **Source Identifier =** sending MISF ID (Source MISF ID TLV) |
| **Destination Identifier =** receiving MISF ID (Destination MISF ID TLV) |
| CertificateStatus  (Certificate Status TLV) |

Change Annex L.8.4 PDUs as follows

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| L.8.4.46 | MIS\_Push\_Certificate indication? | 8.6.1.30 | MC12.M | Yes [ ] No [ ] | PDU46 |
| L.8.4.47 | MIS\_Push\_Certificate request? | 8.6.1.31 | MC12.M | Yes [ ] No [ ] | PDU47 |
| L.8.4.48 | MIS\_Push\_Certificate response? | 8.6.1.32 | MC12.M | Yes [ ] No [ ] | PDU48 |
| L.8.4.49 | MIS\_Revoke\_Certificate indication? | 8.6.1.33 | MC12.M | Yes [ ] No [ ] | PDU49 |
| L.8.4.50 | MIS\_Revoke\_Certificate request? | 8.6.1.34 | MC12.M | Yes [ ] No [ ] | PDU50 |
| L.8.4.51 | MIS\_Revoke Certificate response? | 8.6.1.35 | MC12.M | Yes [ ] No [ ] | PDU51 |