|  |  |
| --- | --- |
| Project | **IEEE 802.21.1 Media Independent Services**  **<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **Suggested remedy for Cmt #132, #133, #134, and #135 of LB8** |
| DCN | **21-16-0011-02-REVP** |
| Date Submitted | **January 30, 2016** |
| Source(s) | Yoshikazu Hanatani (Toshiba) |
| Re: | Session #71, Atlanta |
| Abstract | This contribution suggest a remedy on the MIS\_Revoke\_Certificate primitives. |
| Purpose | Suggested remedy for Cmt #132, #133, #134, and #135 in LB8. |
| 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> |

Problem: The description of the CertificateSerialNumberList is not correct.

.

Suggested remedy:

Change as follows.

1. * 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,

CertificateSerialNumberList,

CertificateRevocation,

IssuerName

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **Name** | **Data Type** | **Description** |
| DestinationIdentifier | MISF\_ID | Specifies an MISF or a group of MISF peers to revoke the credential. |
| CertificateSerialNumberList | CERT\_SERIAL\_NUMBER\_INFO | List of revoked X.509 certificate subfield – serial number or 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. |

* + - * 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 sends the corresponding MIS\_Revoke\_Certificate request message to the destination MISF(s).

* + - 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,

CertificateSerialNumberList,

CertificateRevocation,

IssuerName

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **Name** | **Data Type** | **Description** |
| SourceIdentifier | MISF\_ID | Specifies the remote MISF that invoked MIS\_Revoke\_Certificate.request primitive. |
| CertificateSerialNumberList | CERT\_SERIAL\_NUMBER\_INFO | List of revoked X.509 certificate subfield – serial number or 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. |

* + - * 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 a MN or a PoS verifies a signature in the CertificateRevocation, else the MIS user verifies a signature contained in a 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".

* + - 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.