|  |  |
| --- | --- |
| Project | **IEEE 802.21 MIHS****<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **Proposed remedy for SB Comment i-12** |
| DCN | **21-14-0151-04-MuGM** |
| Date Submitted | **November 2, 2014** |
| Source(s) | Yoshihiro Ohba and Yusuke Doi (Toshiba) |  |
| Re: | IEEE 802.21d Sponsor Ballot comment resolution |
| Abstract | This document describes a proposed remedy for SB comment i-12 about MIH\_Configuration\_Update. |
| Purpose | For Sponsor Ballot 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> |

# Comment i-12 (p28, 7.4.35.1.2)

When multiple certificates are revoked, it should be able to revoke them using a single message. In that case, the size of the message should be reduced as much as possible.

1. Proposed resolution

[1] Apply the following changes to MIH\_Revoke\_Certificate.indication and .request primitives:

* Change CertificateSerialNumber to CertificateSerialNumberList
* Change CERT\_SERIAL\_NUMBER to CERT\_SERIAL\_NUMBER\_INFO
* Change Description for CertificateRevocation to: "(Optional) Digital signature for a revoked X.509 certificate serial numbers generated by CA. This parameter shall be contained only if List or Bloom Filter of X.509 certificate subfield serial numbers is contained in CertificateSerialNumberList.

[2] Define the following new data types:

|  |  |  |
| --- | --- | --- |
| **Data type name** | **Derived from** | **Definition** |
| CERT\_SERIAL\_NUMBER\_INFO | CHOICE(LIST(CERT\_SERIAL\_NUMBER), CERT\_BLOOM\_FILTER, X509CRL) | List or Bloom Filter of X.509 certificate subfield serial numbers or X.509 Certificate Revocation List. |
| CERT\_BLOOM\_FILTER | SEQUENCE(OCTET\_STRING, UNSIGNED\_INT(1)) | The OCTET\_STRING part contains a Bloom Filter value computed against a set of serial numbers of revoked certificates. The UNSIGNED\_INT(1) part contains Bloom Filter parameter k. See Annex V for detailed operations. |
| X509CRL | OCTET\_STRING | CertificateList defined in RFC 5280 [RFC5280]. |

[3] In 8.6.1.30, change "CertificateSerialNumber (Certificate Serial Number TLV)" to "CertificateSerialNumbers (Certificate Serial Number Info TLV)".

[4] In Table L.2 change "Certificate Serial Number" TLV of type "CERT\_SERIAL\_NUMBER" to "Certificate Serial Number Info" TLV of type "CERT\_CERIAL\_NUMBER\_INFO".

[5] Add the following Annex.

**Annex V**

(normative)

**Use of Bloom Filter for Certificate Revocation**

A Bloom Filter (BF) [Bloom] is characterized by the following parameters.

* *m*: length of BF output value in bits
* *k*: number of elements in a set of hash functions {H*i*}

In this specification, hash function H*i* is defined as follows.

H*i*(*x*) = SHA-256 ([*i*]2 || *x*) mod *m*, where [*i*]2 is 32-bit binary representation of integer *i*, 0<=*i*<=*k*-1, and “||” is an operator for concatenation of octet strings.

**V.1 Calculating Bloom Filter output for revoked certificates**

Let S be a set of serial numbers for revoked certificates, BS be a BF output value computed against S.

BS is calculated as follows.

Step 1: Set each bit of BS to zero.

Step 2: For each e in S and for each i in [0,k-1], set Hi(e)-th bit of BS to 1.

**Figure V.1 Bloom Filter example (k=3, m=32)**

**V.2 Certificate revocation check**

For a BF output, a certificate of serial number e is considered to be revoked if Hi(e)-th bit of the BF output is set to 1 for all i in [0, k-1].

**V.3 False positive case**

Since BF is computed using hash functions, there can be a false positive case in which a non-revoked certificate is considered to be revoked. When a false positive case occurs, a valid certificate suffering from the false positive case may be replaced with a new BF-negative certificate using MIH\_Push\_Ceritifcate.

[6] Add the following reference:

[Bloom] Berton H. Bloom, “Space/Time Trade-offs in Hash Coding with Allowable Errors”, Communications of the ACM, Vol. 13, No. 7, July 1970.

[RFC5280] D. Cooper, et al., “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC 5280, May 2008.