DEFECT REPORT FORM

1. Defect Report Number: 9594/281

Title: FreshestCRL extension

2. Source: Editor

3. Addressed to:
4. (a)
(b)

5. Date circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning: Underspecification of the semantics of the FreshestCRL extension

ITU-T X.509 (2000) | ISO/IEC 9594-8: 2000

8. Qualifier: Clarification

9. References in Document:

4th edition, 2000 clauses 8.6.2.6 and B.5.1.4

10. Nature of Defect:

Section 8.6.2.6 of the 4th edition provides a high-level description of the FreshestCRL extension, but does not specify the semantics of the fields in the extension. Annex B describes the rules for processing CRLs. Section B.5.1.4 explains how to determine whether the scope of a CRL includes a particular certificate if the certificate references the CRL using the cRLDistributionPoints extension, but not if the certificate references the CRL using the FreshestCRL extension.

11. Solution Proposed by the Source:

In section 8.6.2.6, add the following paragraph after the ASN.1:

The value of type **CRLDistPointsSyntax** is as defined in the CRL distribution points extension in subclause 8.6.2.1 of this Specification.

Replace the existing subclause B.5.1.4 with the following:

In order to determine that a CRL is one of the CRLs indicated by a distribution point in the CRL distribution point extension or freshest CRL extension in a certificate, all of the following conditions shall be true:

- Either the distribution point field in the CRL's issuing distribution point extension shall be absent (only when not looking for a critical CRL DP), or one of the names in the distribution point field of the CRL DP or freshest CRL extension of the certificate shall match one of the names in the distribution point field in the issuing distribution point extension of the CRL. Alternatively, one of the names in the **cRLIssuer** field of the certificate's CRLDP or freshest CRL extensioncan match one of the names in DP of the IDP; and
- If the certificate is an end entity certificate, the CRL shall not contain **onlyContainsAuthorityCerts** field set to **TRUE** in the issuing distribution point extension of the CRL; and

- If **onlyContainsAuthorityCerts** is set to **TRUE** in the issuing distribution point extension of the CRL, then the certificate being checked shall contain the **basicConstraints** extension with the **cA** component set to **TRUE**; and
- If the **reasons** field is present in the certificate's CRL DP or freshest CRL extension, the **onlySomeReasons** field shall be either absent from the issuing distribution point extension of the CRL or contain at least one of the reason codes asserted in the CRL DP or freshest CRL extension of the certificate; and
- If the **cRLIssuer** field is absent from the relevant extension in the certificate (either CRL DP or freshest CRL) , the CRL shall be signed by the same CA that signed the certificate; and
- If the **cRLIssuer** field is present in the relevant extension in the certificate (CRL DP or freshest CRL) , the CRL shall be signed by the CRL issuer identified in the **cRLIssuer** field and the CRL shall contain the issuing distribution point extension with the **indirectCRL** field set to **TRUE**.

  Note: When testing the **reasons** and **cRLIssuer** field for presence, the test succeeds only if the field is present in the same **DistributionPoint** of the CRL DP or freshest CRL extension in the certificate for which there is a name match in the corresponding distribution point field of the IDP extension in the CRL.

12. Editor's Response:

Accepted solution proposed by source.