DEFECT REPORT FORM

1. Defect Report Number: 9594/280

Title: IDP extension: CA/AA split in CRLs

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: Separation of CA & AA certs in IDP and crlScope extensions

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

8. Qualifier: Clarification

9. References in Document:

4th edition, 2000 clauses 8.6.2.2

10. Nature of Defect:

In the 3rd edition, the IDP extension contained a "onlyContainsCACerts" component. This was changed to "onlyContainsAuthorityCerts" in the 4th ed. Similarly, in the new extension "crlScope", there is a BIT STRING to indicate that the CRL covers specific certificate types (user, authority, attribute).

The problem is that there is no longer any way, in either extension, to indicate that a CRL covers only CA certificates (this was an error introduced when CA was changed to authority). In addition, the text erroneously implies that delta CRLs that contain this extension would not be stored separately in the Directory. The problems that need to be fixed are:

a) Allow the same functionality that the 3rd edition provided (i.e. allow a CRL to be restricted to covering only CA certificates);
b) Allow the restrictions that were intended for handling the different types of certificates related to PMI (end-entity attribute certificates, AA attribute certificates and SOA public-key certificates to be partitioned);
c) c) Clarify which component restrictions apply to public-key certificates and which apply to attribute certificates.
d) d) Clarify that dCRLs containing this extension would be stored in the deltaRevocationList directory attribute.
a)

11. Solution Proposed by the Source:

Replace the existing subclause 8.6.2.2 with the following and make associated changes to the ASN.1 in Appendix A:

8.6.2.2 Issuing distribution point extension

This CRL extension field identifies the CRL distribution point for this particular CRL, and indicates if the CRL is indirect, or if it is limited to covering only a subset of the revocation information. The limitation may be based on a subset of the certificate population or on a subset of revocation reasons. The CRL is signed by the CRL issuer's key — CRL distribution points do not have their own key pairs. However, for a CRL distributed via the Directory, the CRL is stored in the entry of the CRL distribution point, which may not be the directory entry of the CRL issuer. If this field and the CRL scope field are both absent, the CRL shall contain entries for all revoked unexpired certificates issued by the CRL issuer.

This field is defined as follows:

```
issuingDistributionPoint EXTENSION ::= {
  SYNTAX            IssuingDistPointSyntax
  IDENTIFIED BY     id-ce-issuingDistributionPoint }

IssuingDistPointSyntax ::= SEQUENCE {

  distributionPoint                  [0] DistributionPointName OPTIONAL,
  onlyContainsUserPublicKeyCerts     [1] BOOLEAN DEFAULT FALSE,
  onlyContainsCACerts                [2] BOOLEAN DEFAULT FALSE,
  onlySomeReasons                    [3] ReasonFlags OPTIONAL,
  indirectCRL                        [4] BOOLEAN DEFAULT FALSE,
  onlyContainsUserAttributeCerts     [5] BOOLEAN DEFAULT FALSE,
  onlyContainsAACerts                [6] BOOLEAN DEFAULT FALSE,
  onlyContainsSOAPublicKeyCerts      [7] BOOLEAN DEFAULT FALSE }
```

The **distributionPoint** component contains the name of the distribution point in one or more name forms. After a certificate appears on a CRL, it may be deleted from a subsequent CRL after the certificate's expiry.

If **onlyContainsUserPublicKeyCerts** is true, the CRL only contains revocations for end-entity public-key certificates. If **onlyContainsCACerts** is true, the CRL only contains revocations for CA certificates.

If **onlySomeReasons** is present, the CRL only contains revocations for the identified reason or reasons, otherwise the CRL contains revocations for all reasons.

If **indirectCRL** is true, then the CRL may contain revocation notifications from authorities other than the issuer of the CRL. The particular authority responsible for each entry is as indicated by the certificate issuer CRL entry extension in that entry or in accordance with the defaulting rules described in 8.6.2.3. In such a CRL, it is the responsibility of the CRL issuer to ensure that the CRL is complete in that it contains all revocation entries, consistent with **onlyContainsUserPublicKeyCerts**, **onlyContainsCACerts**, **onlyContainsUserAttributeCerts** , **onlyContainsAACerts, onlyContainsSOAPublicKeyCerts** and **onlySomeReasons** indicators, from all authorities that identify this CRL issuer in their certificates.

If **onlyContainsUserAttributeCerts** is true, the CRL only contains revocations for attribute certificates issued to end-entities that are not themselves AAs. If **onlyContainsAACerts** is true, the CRL only contains revocations for attribute certificates issued to subjects that are themselves AAs.

If **onlyContainsSOAPublicKeyCerts** is true, the CRL only contains revocations for public-key certificates issued to an entity that is an SOA for purposes of privilege management (i.e. certificates that contain the SOAIdentifier extension)..

For CRLs distributed via the Directory, the following rules regarding use of attributes apply. Unless the CRL is a dCRL, a CRL which has **onlyContainsCACerts**,**onlyContainsAACerts** or **onlyContainsSOAPublicKeyCerts** set shall be distributed via the **authorityRevocationList** attribute of the associated distribution point or, if no distribution point is identified, via the **authorityRevocationList** attribute of the CRL issuer entry. Otherwise the CRL shall be distributed via the **certificateRevocationList** attribute of the associated distribution point or, if no distribution point is identified, via the **certificateRevocationList** attribute of the authority entry. If the CRL is a dCRL it shall be distributed via

the **deltaRevocationList** attribute of the associated distribution point or, if no distribution point is identified, via the **deltaRevocationList** attribute of the CRL issuer entry.

This extension is always critical. A certificate user which does not understand this extension cannot assume that the CRL contains a complete list of revoked certificates of the identified authority. CRLs not containing critical extensions shall contain all current CRL entries for the issuing authority, including entries for all revoked user certificates and authority certificates.

> NOTE 1 — The means by which revocation information is communicated by authorities to CRL issuers is beyond the scope of this Recommendation | International Standard.
> NOTE 2 — If a authority publishes, in its own directory entry (i.e. not from a separately-named CRL distribution point), a CRL with **onlyContainsUserPublicKeyCerts** or **onlyContainsCACerts** set, then the authority should ensure that all certificates covered by this CRL contain the **basicConstraints** extension.
> NOTE 3 — If a authority publishes, in its own directory entry (i.e. not from a separately-named CRL distribution point), a CRL with **onlyContainsUserAttributeCerts**, **onlyContainsAACerts** or **onlyContainsSOAPublicKeyCerts** set, then the authority should ensure that all certificates covered by this CRL contain the **basicAttConstraints** extension.

In clause 8.5.2.5, and in Appendix A, replace the OnlyCertificateTypes ASN.1 construct with the following:

```
OnlyCertificateTypes        ::= BIT STRING {
  userPublicKey      (0),
  CA                 (1),
  userAttribute      (2),
  AA                 (3),
  SOAPublicKey       (4) }
```

12. Editor's Response:

Accepted solution proposed by source.