DEFECT REPORT FORM

1. Defect Report Number: 305

Title: IDP extension

2. Source: S. Boeyen (Entrust)

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

5. Date circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning: Revisions to IDP resulting in backward compatibility and migration problems

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

8. Qualifier: Error

9. References in Document: 4th edition clause 8.6.2.2

10. Nature of Defect:

In the 4th edition of X.509, the Issuing Distribution Point extension was extended to address revocation notices for attribute certificates as well as public key certificates. However DR 280 identified a number of problems with the enhanced version of this extension. A resolution for DR 280 was approved and is contained in TC 3. However, since that time serious problems have been identified with the resulting specification for that extension. These problems are related to migration of systems that implement only the original unenhanced edition of that extension (defined in the 3rd edition of X.509) and the revised definition. The OID was never changed, but the elements of the extension have changed both in syntax as well as semantics, resulting in an extremely problematic situation for interoperability and migration and breaking backward compatibility with 3rd edition systems (upon which most, if not all, existing profiles are based.

11. Solution Proposed by the Source:

Rather than trying to combine everything into a single extension, there should be two separate extensions. The Issuing Distribution Point extension should be rolled back and stay as originally defined in the 3rd edtion text. A separate extension should be defined that is used solely for attribute certificates. If a CRL covers both public key and attribute certificates it would contain both extensions.

In 8.6.2 add a new list item c) as follows and renumber the existing list items c) through f) to d) through g) accordingly:

c) AAissuingDistributionPoint

In 8.6.2, replace the second sentence of the last paragraph with the following:

Issuing distribution point, AA issuing distribution point, delta CRL indicator and base update shall be used only as CRL extensions.

In 8.6.2 add the following paragraph to the end of the section, immediately before 8.6.2.1:

While the issuing distribution point extension and the AA issuing distribution point extension serve similar purposes, they apply to different certificates. The issuing distribution point extension applies only to public key certificates issued to users and/or CAs. The AA issuing distribution point extension applies only to attribute certificates issued to users and AAs as well as public-key certificates issued to SOAs. If a single CRL covers certificate types that span these, then that CRL would need to include both extensions. Note that the CRL scope extension defined in 8.5.2.5 is also similar to these two extensions. However that extension is known to be flawed and its usage is deprecated. The issuing distribution point extension and/or AA issuing distribution point extension should be used instead of the CRL scope extension.

In section 8.5.2.5 (CRL scope extension), replace the following paragraph

> Note that the **issuingDistributionPoint** extension and **crlScope** extension can conflict with each other and are not intended to be used together. However, if the CRL contains both an **issuingDistributionPoint** extension and a **crlScope** extension, then a certificate falls within the scope of the CRL if and only if it meets the criteria of both extensions. If the CRL contains neither an **issuingDistributionPoint** nor **crlScope** extension, then the scope is the entire scope of the authority, and the CRL may be used for any certificate from that authority.

with

> Note that the **issuingDistributionPoint** extension and **crlScope** extension can conflict with each other and are not intended to be used together. However, if the CRL contains both an **issuingDistributionPoint** extension and a **crlScope** extension, then a public-key certificate falls within the scope of the CRL if and only if it meets the criteria of both extensions. If the CRL contains an **AAissuingDistributionPoint** extension, but does not contain an **issuingDistributionPoint** or **crlScope** extension, then the scope does not include public-key certificates. If the CRL does not contain an **issuingDistributionPoint**, **AAissuingDistributionPoint**, or **crlScope** extension, then the scope is the entire scope of the authority, and the CRL may be used for any certificate from that authority.
>
> Similarly, the **iAAssuingDistributionPoint** extension and **crlScope** extension can conflict with each other and are not intended to be used together. However, if the CRL contains both an **AAissuingDistributionPoint** extension and a **crlScope** extension, then an attribute certificate falls within the scope of the CRL if and only if it meets the criteria of both extensions. If the CRL contains an **issuingDistributionPoint** extension, but does not contain an AA**issuingDistributionPoint** or **crlScope** extension, then the scope does not include attribute certificates. If the CRL does not contain an **issuingDistributionPoint**, **AAissuingDistributionPoint**, or **crlScope** extension, then the scope is the entire scope of the authority, and the CRL may be used for any certificate from that authority.

Replace section 8.6.2.2 with the following:

8.6.2.2 IssuingDistributionPoint extension

This CRL extension field identifies the CRL distribution point for public-key certificates 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 private 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 the issuing distribution point field, the AA issuing distribution point field, and the CRL scope field are all absent, the CRL shall contain entries for all revoked unexpired public-key certificates issued by the CRL issuer. If the issuing distribution point field and the CRL scope field are both absent, but the AA issuing distribution point field is present, the scope of the CRL does not include public-key certificates.

Editor's Note: *When compiling the next edition of X.509 note that there is an additional sentence that needs to be added to the above paragraph as a result of TC 3 and the resolution of DR 298).*

After a certificate appears on a CRL, it may be deleted from a subsequent CRL after the certificate's expiry.

This field is defined as follows:

```
issuingDistributionPoint      EXTENSION   ::=   {
   SYNTAX     IssuingDistPointSyntax
   IDENTIFIED BY  id-ce-issuingDistributionPoint }
IssuingDistPointSyntax ::= SEQUENCE {
--If onlyContainsUserPublicKeyCerts and onlyContainsCACerts are both FALSE, the CRL covers both
certificate types--
    distributionPoint       [0] DistributionPointName OPTIONAL,
    onlyContainsUserPublicKeyCerts [1] BOOLEAN DEFAULT FALSE,
    onlyContainsCACerts     [2] BOOLEAN DEFAULT FALSE,
    onlySomeReasons         [3] ReasonFlags OPTIONAL,
    indirectCRL             [4] BOOLEAN DEFAULT FALSE }
```

The **distributionPoint** component contains the name of the distribution point in one or more name forms.

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

If **onlySomeReasons** is present, the CRL only contains revocations of public-key certificates 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 for public-key certificates 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**, and **onlySomeReasons** indicators, from all authorities that identify this CRL issuer in their public-key certificates.

For CRLs distributed via the Directory the following rules apply. 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, regardless of the settings for certificate types covered by the CRL. Unless the CRL is a dCRL:

- A CRL which has **onlyContainsCACerts** set and does not contain an **AAissuingDistributionPoint** extension 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.
- A CRL which has **onlyContainsCACerts** set and contains an **AAissuingDistributionPoint** extension with **containsUserAttributeCerts** set to false 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.
- A CRL which has only **onlyContainsCACerts** set to false 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 CRL issuer entry.
- A CRL which contains both an **issuingDistributionPoint** extension and an **AAissuingDistributionPoint** extension with **containsUserAttributeCerts** set 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 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 an authority publishes a CRL with **onlyContainsUserPublicKeyCerts** or **onlyContainsCACerts** set to true, then the authority shall ensure that all CA certificates covered by this CRL contain the **basicConstraints** extension.

Add the following new section:

8.6.X.X AAIssuingDistributionPoint extension

This CRL extension field identifies the CRL distribution point for attribute certificates 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 private 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 the issuing distribution point extension, the AA issuing distribution point extension, and the CRL scope field are all absent, the CRL shall contain entries for all revoked unexpired attribute certificates issued by the CRL issuer. If the AA issuing distribution point field and the CRL scope field are both absent, but the issuing distribution point field is present, the scope of the CRL does not include attribute certificates.

After a certificate appears on a CRL, it may be deleted from a subsequent CRL after the certificate's expiry.

This field is defined as follows:

```
AAissuingDistributionPoint EXTENSION  ::=  {
   SYNTAX     AAIssuingDistPointSyntax
   IDENTIFIED BY  id-ce-AAissuingDistributionPoint }
AAIssuingDistPointSyntax ::= SEQUENCE {
   distributionPoint                [0] DistributionPointName OPTIONAL,
   onlySomeReasons                  [1] ReasonFlags OPTIONAL,
   indirectCRL                  [2] BOOLEAN DEFAULT FALSE,
   containsUserAttributeCerts   [3] BOOLEAN DEFAULT TRUE,
   containsAACerts              [4] BOOLEAN DEFAULT TRUE,
   containsSOAPublicKeyCerts    [5] BOOLEAN DEFAULT TRUE }
```

The **distributionPoint** component contains the name of the distribution point in one or more name forms.

If **onlySomeReasons** is present, the CRL only contains revocations for attribute certificates 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 for attribute certificates 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 **containsUserAttributeCerts**, **containsAACerts, containsSOAPublicKeyCerts** and **onlySomeReasons** indicators, from all authorities that identify this CRL issuer in their attribute certificates.

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

If **containsSOAPublicKeyCerts** is true, the CRL 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 apply. 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, regardless of the settings for certificate types covered by the CRL. Unless the CRL is a dCRL:

- A CRL that does not contain an **issuingDistributionPoint** extension which has only **containsAACerts** and/or **containsSOAPublicKeyCerts** set shall be distributed via the **attributeAuthorityRevocationList** attribute of the associated distribution point or, if no distribution point is identified, via the **attributeAuthorityRevocationList** attribute of the CRL issuer entry.
- A CRL that does not contain an **issuingDistributionPoint** extension which has **containsUserAttributeCerts** set (with or without **containsAACerts** and/or **containsSOAPublicKeyCerts** also set) shall be distributed via the **attributeCertificateRevocationList** attribute of the associated distribution point or, if no distribution point is identified, via the **attributeCertificateRevocationList** attribute of the CRL issuer entry.
- A CRL which contains an **issuingDistributionPoint** extension shall be distributed as specified in section 8.6.2.2.

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 an authority publishes a CRL with **containsAACerts** set to true and **containsUserAttributeCerts** not set to true, then the authority shall ensure that all AA certificates covered by this CRL contain the **basicAttConstraints** extension.

NOTE 3 --- If an authority publishes a CRL with **containsSOAPublicKeyCerts** set to true, then the authority shall ensure that all SOA certificates covered by this CRL contain the **SOAIdentifier** extension.

12. Editor's Response: