DEFECT REPORT FORM

1. Defect Report Number: 310

Title: Unrecognized CRL and CRL entry extensions

2. Source: IETF PKIX RFC 3280bis design team

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

5. Date circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning: Processing of CRLs with an unrecognized CRL or CRL entry extension

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

8. Qualifier: Error

9. References in Document: 4th edition clause 7.3 Note 4

10. Nature of Defect:

Note 4 mandates that, if a critical CRL extension or critical CRL entry extension is not recognized, and the serial number of interest appears on the CRL, that certificate as a minimum, is considered revoked. However, this may not in fact be the case and certificates that are not actually revoked (e.g. in the case of the certificateIssuer extension) will be considered revoked. There could be other extensions defined by other groups that may also cause certificates to incorrectly be considered revoked. As a result of this, the relying party would not try other potential sources of revocation status information that it could properly process, such as a full CRL for that CA or an OCSP service.

There is also a potential denial of service attack if a CRL with this extension is issued and includes a whole set of serial numbers that are known to be used by other CAs (recognizing that such a CRL would need to be issued by a recognized CRL issuer).

11. Solution Proposed by the Source:

Rather than considering such certificates revoked, the outcome for these cases should be that the CRL that contains the unrecognized critical extensions cannot be used to check revocation status for that certificate. This enables the relying party to seek revocation status from other known sources if they exist and it also enables local policy to determine whether or not to trust the certificate in the absence of reliable status information.

Replace Note 4 of 7.3 with the following:

> NOTE 4 – When an implementation processing a certificate revocation list does not recognize a critical extension in the **crlEntryExtensions** field, that CRL cannot be used to determine the status of the certificate. When an implementation does not recognize a critical extension in the **crlExtensions** field, that CRL cannot be used to determine the status of the certificate. In these cases local policy may dictate actions in addition to and/or stronger

than those stated in this Specification, such as seeking revocation status information from other sources. Certificates for which revocation status cannot be determined should not be considered valid certificates.

12. Editor's Response: