DEFECT REPORT FORM

1. Defect Report Number: 9594/275

Title: Extended key usage

2. Source: X.509 editor

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

5. Date circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning: extended key usage

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

8. Qualifier: Clarification

9. References in Document:

4th edition, 2000 (clause 8.4.2.1 and clause 15.5.2.1)

10. Nature of Defect:

As a result of the resolution to DR 244, it is no longer possible to include an extended key usage extension that allows applications that require a specific value to be present to make use of a certificate that contains the extension with the appropriate OID, but does not restrict the certificate to be used ONLY for the identified usages.

11. Solution Proposed by the Source:

In clause 8.2.2.4, add the following as a new second paragraph following the ASN.1 for the **extendedKeyUsage** extension.

A CA may assert any-extended-key-usage by using the **anyExtendedKeyUsage** identifier. This enables a CA to issue a certificate that contains OIDs for extended key usages that may be required by certificate-using applications, without restricting the certificate to only those key usages. If extended key usage would restrict key usage, then the inclusion of this OID removes that restriction.

extendedKeyUsage OBJECT IDENTIFIER ::= { 2 5 29 37 0 }

12. Editor's Response:

Accepted solution proposed by source