DEFECT REPORT FORM

1. Defect Report Number : 9594/185

Title: Use of cACertificate and crossCertificatePair attributes

2. Source: : ISO/IEC Rapporteur

3. Addressed to: ISO/IEC JTC1/SC6 and ITU-T Study Group 7 Editor Group on the Directory

4 . (a) WG Secretariat : US (ANSI)
(b) IUT-T WP : SG 7/WP 4

5. Date Circulated by WG Secretariat

6. Deadline for Response from Editor

7. Defect Report Concerning :

X.509 (1993) and ISO/IEC 9594-8 (1994)
The Directory: Authentication Framework

8. Qualifier: (e.g. error, omission, clarification required)

omission/clarification

9. References in Document:

8

10.Nature of Defect :

Clarification is required regarding the use of these two attributes.

11.Solution Proposed by the Source:

Text to be added explaining that the cACertificate attribute type is used to store the self signed certificate of the CA which anchors the trust for this CA. The crossCertificatePair attribute type is used to store certificates for cross-certification agreeements this CA is involved in. In some cases both forward and reverse certificates will be stored, while in others only one may be present. The example in the text needs to be expanded or replaced to reflect the current practice.

12. Editor' s Response:

Certificates issued from one CA to another CA are to be stored in forward element of the crossCertificatePairs attribute in the subject CA’s directory entry. Optionally, a subset, determined through local means, of these may also be stored in the cACertificate attribute of the subject CA’s directory entry.

Certificates issued from one CA to another CA may also optionally be stored in the reverse element of the crossCertificatePairs attribute in the issuing CA’s directory entry.

Self-issued certificates are stored in the cACertificate attribute of that CA’s directory entry.

In addition to revising the text, Figure 4 needs to be modified so that the directory entry for CA W contains the certificate “X<W>” and the directory entry for CA V contains the certificate “W<V>”.