DEFECT REPORT FORM

1. Defect Report Number: 9594/219
   Title: CA Certificate and Basic Constraints

2. Source: IETF

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

5. Date circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning:
ITU-T X.509 (1997) | ISO/IEC 9594-8:1997

8. Qualifier:
Error

9. References in Document:
Clause 12.4.2.1

10. Nature of Defect:

If there is no basicConstraints extension in a certificate, there is no way to know (from the certificate itself) whether the subject of the certificate is a CA or an end-entity. Making the presence of the extension mandatory in a PKIX (or other) profile doesn t solve the problem because there is no way to know (from the certificate itself) whether it is a certificate issued according to that profile or not. Therefore the fix needs to be made in X.509 and not the profiles.

11. Solution Proposed by the Source:

Since X.509 allows, even slightly recommends, that an end-entity certificate contain this extension, it cleaner to express this in terms of requiring a CA certificate to have the extension, if it is a v3 certificate, rather than to state what absence of the extension means.

12. Editor s Response:

Accepted as a defect. However, rather than mandate inclusion of basicConstraints in all v3 certificates, the correction will be to state that absence of this extension in a v3 certificate means that the certificate is to be considered an end-entity certificate. The solution proposed by source would have required that this extension be present in certificates issued in environments where it is not necessary as a differentiator (e.g. environments where a CA is only ever issuing end-entity certificates). Profiles may, depending on the environment they are operated within, require this to be included, however X.509 needs to remain as flexible as possible to accommodate all environments as efficiently as possible without overloading certificates with unnecessary data.

Also, In clause 8, replace the final sentence of text that describes the contents of the CA certificate and cross certificate pair attributes (new text added to resolve DR 185) In the case of v3 certificates, none of the above CA certificates shall include a basicConstraints extension with the cA value set to FALSE with the following: In the case of v3 certificates, all of the above CA certificates shall include a basicConstraints extension with the cA value set to TRUE .

(Orlando meeting Apr 99)