DEFECT REPORT FORM

1. Defect Report Number: 9594/277

Title: Requires explicit policy skip certificates value

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: Requires explicit policy skip certificates value

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

8. Qualifier: Clarification

9. References in Document:

4th edition, 2000 clauses 8.4.2.3 and 10

10. Nature of Defect:

The text of 8.4.2.3 indicates that a nominated CA is the CA that issued the certificate containing the policy constraints extension, (if **requireExplicitPolicy SkipCerts** value is zero) or a CA that is the subject of a subsequent certificate (if the **SkipCerts** value is non-zero). This indicates that if the **SkipCerts** value is "one" and there is only one subsequent certificate in the path, then no policy is explicitly required in the certification path.

However the processing steps in clause 10 would have the opposite effect. In the steps for processing intermediate certificates, in step f) the *inhibit-any-policy-pending* indicator would be set to 1 (for the example cited above). After that is completed, the next set of processing steps is applied "for all certificates". For the example above, the first step (that begins with: "if the *explicit-policy-pending* indicator is set …) would decrement the counter to zero and cause the *explicit-policy-indicator* to be set. When the next certificate (i.e. the last certificate in the example cited above) is processed, since the *explicit-policy-indicator* is set, explicit policies would be required for the certification path. This is contrary to what is stated in 8.4.2.3.

11. Solution Proposed by the Source:

In clause 8.4.2.3, in the last sentence of the first paragraph, replace "which is the subject of a subsequent certificate" with "which is the issuer of a subsequent certificate".

12. Editor's Response: