DEFECT REPORT FORM

1. Defect Report Number: 9594/276

Title: Use of anyPolicy in self issued certificates

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: use of anyPolicy in self issued certificates

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

8. Qualifier: Clarification

9. References in Document:

4th edition, 2000 clauses 8.1.5, 8.4.2.4 and 10.5

10. Nature of Defect:

One use of self-issued certificates is for a CA to roll over its certificate and/or CRL signing keys without disruption to certification paths that were previously established. In such cases it is convenient for the CA to include the special value **anyPolicy** in the certificate policies extension of the self-issued certificate. This allows the self-issued certificate to provide a link in certification paths for any policy that would be valid if the self-issued certificate did not exist. However, there is a problem if *the inhibit-any-policy-indicator* is set in the certification path processing procedure prior to a self-issued certificate. The current text would result in failure of the path because of the existence of **anyPolicy** in the self-issued certificate. However, if the self-issued certificate did not exist (i.e. the CA had not yet rolled over its key), paths for which specific policies are present in all subsequent certificates may have passed, but will always fail due to **anyPolicy** in the self-issued certificate.

11. Solution Proposed by the Source:

The presence of the special value **anyPolicy** in a self-issued certificate should not cause a certification path to fail, that would otherwise pass if the self-issued certificate was not in the path.

In clause 8.1.5, in the last sentence, replace “and *explicit-policy-pending indicators*” with “*explicit-policy-pending* and *inhibit-any-policy indicators*”.

In clause 8.4.2.4, in the first sentence, replace “for all certificates in the certification path” with “for all non-self-issued certificates in the certification path”.

In clause 10.5, in the first bullet list, step e), replace “or if the *inhibit-any-policy-indicator* is set, then delete” with “or if the *inhibit-any-policy-indicator* is set and the certificate is not a self-issued intermediate certificate, then delete”.

12. Editor's Response:

Accepted solution proposed by source