DEFECT REPORT FORM

1. Defect Report Number: 302

Title: Skip Certs in policy constraints

2. Source: Sharon Boeyen

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

5. Date circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning: policy constraints and requires explicit policy

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

8. Qualifier: Clarification

9. References in Document:

4th edition, 2000 clause 8.4.2.3

10. Nature of Defect:

The meaning of the SkipCerts value for requireExplicitPolicy in policyConstraints was changed as a result of DR 222 and DR 277, however there is still a sentence in 8.4.2.3 that is inconsistent with the modified meaning. The paragraph/sentence that begins with "A value of type SkipCerts indicates …" is still correct with respect to inhibitPolicyMapping, but incorrect with respect to requireExplicitPolicy.

Note also that although policyConstraints can only be included in CA certificates and not in EE certificates (see second paragraph of 8.4.2), the first sentence of 10.5.3 says "For all certificates …". Although this is somewhat inconsistent it is also harmless as the extension can never appear in EE certificates. This could be clarified by replacing "all" with "intermediate" but this is not really necessary. There should NOT be a change to allow policy constraints in EE certificates however. That would be contrary to the model, where issuing CAs can impose constraints through extensions in intermediate certificates but relying party constraints are imposed by the relying party's own local authority by initializing, in this case, the 'explicit-policy-indicator' to a value that suits the relying party domain's own security policy. Note that the inclusion of a critical certificate policy extension is an issuing CAs method of indicating that a certificate cannot be used for purposes other than the indicated policies.

11. Solution Proposed by the Source:

In 8.4.2.3, add text to the end of the paragraph that begins with "If the requireExplicitPolicy component is present …" as follows:

A value of type SkipCerts indicates the number of subsequent certificates in the certification path at which point the constraint becomes effective. For example, a value of '0' means the existence of this constraint in the present certificate requires all certificates in the path to include policy identifiers. A value of '4' indicates that if there are 4 subsequent certificates in the path then all certificates in the path are required to include policy identifiers.

12. Editor's Response: