DEFECT REPORT FORM

1. Defect Report Number: 289

Title: Certification path processing

2. Source: United States Federal Public Key Infrastructure Technical Working Group

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

5. Date circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning: Final path processing steps

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

8. Qualifier: Clarification

9. References in Document:

4th edition, 2000 clause 10.5.4

10. Nature of Defect:

Clause 10.5.4 is unclear as to whether a failure indication must be returned when the explicit-policy-indicator is set and the user-constrained-policy-set is empty. Clause 8.1.4 and the final sentence in clause 10.5.4 imply that the path is invalid, yet there is no explicit check for this condition in clause 10.5.4.

11. Solution Proposed by the Source:

Section 10.1, item c, revise as follows

an *initial-policy-set* comprising one or more certificate policy identifiers, indicating that any one of these policies would be acceptable to the certificate user for the purposes of certification path processing; this input can also take the special value *any-policy*, but it can not be null;
Replace paragraphs in clause 10.5.4 with the following:

10.5.4 Final processing

Once all certificates in the path have been processed, the following actions are then performed:

a) Determine the *authorities-constrained-policy-set* from the *authorities-constrained-policy-set* table. If the table is empty, then the *authorities-constrained-policy-set* is the empty or null set. If the *authorities-constrained-policy-set[0, path-depth]* is *any-policy*, then the *authorities-constrained-policy-set* is *any-policy*. Otherwise, the *authorities-constrained-policy-set* is, for each row in the table, the value in the left-most cell which does not contain the identifier *any-policy*.

b) Calculate the *user-constrained-policy-set* by forming the intersection of the *authorities-constrained-policy-set* and the *initial-policy-set*.

c) If the *explicit-policy-indicator* is set, check that neither the *authorities-constrained-policy-set* nor the *user-constrained-policy-set* is empty.

If any of the above checks were to fail, then the procedure shall terminate, returning a failure indication, an appropriate reason code, the *explicit-policy-indicator*, the *authorities-constrained-policy-*

set and the *user-constrained-policy-set*. If the failure is due to an empty *user-constrained-policy-set*, then the path is valid under the authority-constrained policy(s), but none is acceptable to the user.

If none of the above checks were to fail on the end certificate, then the procedure shall terminate, returning a success indication together with the *explicit-policy-indicator*, the *authorities-constrained-policy-set* and the *user-constrained-policy-set*.

12. Editor's Response: