1. Defect Report Number:
   Title: Certificate Policy Mapping

2. Source: Santosh Chokhani, US

3. Addressed to:

4. (a)
   (b)

5. Date circulated to 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 and Omission

9. References in Document:

Clause 12.2.2.6 (omission); 12.4.3 (error)

10. Nature of Defect:

In order to ensure that each domain controls whether trust transits through another domain it certifies, it must not assert the policy of its (issuer) domain, but that of the subject CA domain. However, the current policy mapping processing logic is flawed. It will not work since policy mapping is picked up after policy checking. The current policy processing logic will work if the issuer CA asserted the policy of its (issuer) domain. However, asserting the issuer domain policy means losing control of inhibit policy mapping feature.

See attached briefing if further details are desired.

11. Solution recommended by the Source:

1. Add the following sentence in certificate policies extension section (Section 12.2.2.6) of the X.509 Amendment : “If the subject of the certificate is a CA in another domain, the policy(s) asserted shall be those of the subject CA’s domain.

2. Delete the following from item e (“If policy-mapping-inhibit-indicator is not set:”) in path validation section, 12.4.3.

“— process any policy mapping extension with respect to policies in the user-constrained-policy-set and add appropriate policy identifiers to the user-constrained-policy-set.
— process any policy mapping extension with respect to policies in the authority-constrained-policy-set and add appropriate policy identifiers to the authority-constrained-policy-set.”

3. Add the following to the list of check just prior to item “c” check in path validation section, 12.4.3.

“If policy-mapping-inhibit-indicator is not set:.

— process any policy mapping extension with respect to policies in the user-constrained-policy-set and add appropriate policy identifiers to the user-constrained-policy-set.
— process any policy mapping extension with respect to policies in the authority-constrained-policy-set and add appropriate policy identifiers to the authority-constrained-policy-set.”