DEFECT REPORT FORM

1. Defect Report Number: 314

Title: Name constraints extension alignment with RFC 3280

2. Source: Collaborative - RFC 3280bis design team
3. Addressed to:
4. (a)

   (b)
5. Date circulated by WG Secretariat:
6. Deadline for Response from Editor:
7. Defect Report Concerning: Definition of the Name Constraints extension format

ITU-T X.509 (08/2005) | ISO/IEC 9594-8: 2005

8. Qualifier: Error
9. References in Document: Clause 8.4.2.2 Name constraints extension
10. Nature of Defect:

    Corrigendum 1 (10/2001) changed the syntax of the name constraints extension by adding the **requiredNameForms** parameter and changing the extension OID from {id-ce 30} to {id-ce 30 1}. The old version of the extension was removed and is therefore no longer supported by X.509.

    Despite the considerable time that has passed after this change, adoption of this new extension has neither propagated within the industry nor to the IETF RFC 3280 profile.

    The current update work of RFC 3280 (RFC 3280bis) has currently no intention of changing to the new {id-ce 30 1} version of name constraints as it would make current compliant implementations non-conformant.

    This has lead to the situation where this extension, which is a core component in path validation, is incompatible between these standards.

    In addition, RFC 3280 requires this extension to be critical while X.509 recommends it to be critical, which makes interoperability an even bigger issue. If a CA's would issue certificate with the new X.509 extension being critical, the path would fail in implementations purely based on RFC 3280. Trying to solve this by Including multiple extensions of both versions as a migration solution would be confusing and would force the different versions of extensions to have different criticality settings to succeed creating functional differences in the level of enforcement and forcing clients to process the old critical version of the extension or reject the path. Such a migration strategy is not realistic.

11. Solution Proposed by the Source:
    a. Revert back to the X.509 (03/2000) ASN.1 syntax of the name constraints extension as well as reverting back to the original extension OID {id-ce 30}.
    b. Update the text of the name constraints extension to remove text related to **requiredNameForms**.
    c. Do one of the following additional changes.
        i. Preserve the current logic of the path validation algorithm but clarify that the **requiredNameForms** parameter must be provided as

initialization input to the path validation algorithm. This would also make it possible to tie this into a future extension.

ii. Create a new “name type constraints” extension which includes this **requiredNameForms** parameter (possibly with an eye toward adding other useful parameters for expressing requirements on required and excluded name types).

12. Editor's Response: