DEFECT REPORT FORM

1. Defect Report Number: 9594/**279**

Title: Certification path syntaxes

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: Simple syntax to represent certification path

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

8. Qualifier: Clarification

9. References in Document:

4th edition, 2000 clauses 7, 11.1.6, 11.2.10, 11.3.9

10. Nature of Defect:

The existing syntaxes in 7 and 11.2.10 for specifying a certification path are not sufficient as they all imply 'pairs' of certificates rather than a simple sequence. There is no simple way to specify an ordered path of certificates. The pkiPath attribute, while intended to hold ordered sequences of certificates, currently uses a 'paired' syntax, which is overly confusing and complex. A simple syntax is needed for generic communication of paths in application protocols. This same syntax should be reused as the syntax for storing paths in directory attributes. Also the **pkiPath** attribute should be able to be used as well to store **pkiPath** values in a user's entry, where the path includes that user's end-entity certificate.

11. Solution Proposed by the Source:

a) In clause 7, add the following immediately after the ASN.1 **CrossCertificates** production:
"

```
PkiPath ::=          SEQUENCE OF Certificate
```

PkiPath is used to represent a certification path. Within the sequence, the order of certificates is such that the subject of the first certificate is the issuer of the second certificate, etc.
"

b) In clause 11.1.6, replace "object class **pkiCA**" with "**pkiCA** or **pkiUser**".

c) In the last sentence of the last paragraph of clause 7, replace "component of **CertPath**" with "component of **CertPath** or a value of **Certificate** in **PkiPath**."

d) In clause 11.2.10, delete the **PkiPath** ASN.1 production. In the first sentence of 11.2.10, replace "cross-certificates" with "certificates". Replace the text following the ASN.1 with the following: "This attribute can be stored in a directory entry of object class **pkiCA** or **pkiUser**.

When stored in **pkiCA** entries, values of this attribute contain certification paths excluding end-entity certificates. As such, the attribute is used to store certification paths that are frequently used by relying parties associated with that CA. A value of this attribute can be used in conjunction with any end-entity certificate issued by the last certificate subject in the attribute value.

When stored in **pkiUser** entries, values of this attribute contain certification paths that include the end-entity certificate. In this case, the end-entity is the user whose entry holds this attribute. The values of the attribute represent complete certification paths for certificates issued to this user.

e) In clause 11.3.9, in the last sentence of the first paragraph, replace “issued to the CA that issued the end-entity certificate being validated.” with “issued to the specified subject”.

12. Editor's Response: