

DEFECT REPORT FORM

1. Defect Report Number: 9594/**274**

Title: Attribute Certificate version

2. Source: X.509 editor

3. Addressed to:

5. Date circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning:

ITU-T X.509 (1997 and 2000 editions) | ISO/IEC 9594-8:1997 and 2000 editions

8. Qualifier: Clarification

9. References in Document:

4th edition, 2000 (clause 12.1 and Annex A)

10. Nature of Defect:

There is an error in the asn.1 for **AttributeCertificateInfo** and the text below it that explains versioning. Specifically a v1 certificate cannot be formed correctly with this ASN.1 because the holder syntax is not backward compatible. There is no requirement to carry v1 through to this 4th edition text and as such it is recommended that the 4th edition require v2. The changes to the text in order to align with this are described below. The other option, which would also solve the problem, is to retain the option of v1 or v2 but this would require changing the syntax of holder to be a choice of v1 form or v2 form, similar to the way issuer is currently handled in the 4th edition text. However, discussion among the defect resolution group to date agreed that it was unnecessary to carry over v1 to this edition and that the simplest solution is to require v2. Implementations may still support the v1 attribute certificate syntax as defined in the 3rd edition text. Implementations wishing to support the v2 syntax would do so as defined in the 4th edition text.

11. Solution Proposed by the Source:

No changes are required to 3rd edition text. The following changes are applied to 4th edition text.

*a) In clause 12.1 in the **AttributeCertificateInfo** ASN.1 production, replace:*

version **AttCertVersion DEFAULT v1,**
with:

version **AttCertVersion --version is v2,**

*b) In clause 12.1 replace the **AttCertVersion** ASN.1 production with:*

AttCertVersion ::= **INTEGER {v2(1)}**

c) In clause 12.1 replace the **AttCertIssuer** ASN.1 production with:

```
AttCertIssuer ::= [0] SEQUENCE {  
  issuerName GeneralNames OPTIONAL,  
  baseCertificateID [0] IssuerSerial OPTIONAL,  
  objectDigestInfo [1] ObjectDigestInfo OPTIONAL }
```

d) In the ASN.1 Holder production, replace the comment under objectDigestInfo that reads “—if present, version must be v2” with the following asn.1 comment “—used to directly authenticate the holder, eg. an executable”

e) Replace the first paragraph that follows the ASN.1 with the following:

The **version** differentiates between different versions of the attribute certificate. For attribute certificates issued in accordance with the syntax in this specification, **version** must be **v2**.

f) The same changes listed in bullets a), b), c) and d) must also be made in Annex A in the **attributeCertificateDefinitions** module.

12. Editor's Response:

Accepted solution proposed by source