DEFECT REPORT FORM

1. Defect Report Number: 9594/240
   Title: CA Certificate and Basic Constraints

2. Source: IETF / ISO Rapporteur

3. Addressed to:

4. (a)
   (b)

5. Date circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning:

ITU-T X.09 (1997) | ISO/IEC 9594-8:1997

8. Qualifier:

Clarification

9. References in Document:

Annex A

10. Nature of Defect:

The folowing corrections fix errors in the ASN.1 in Annex A.

11. Solution Proposed by the Source:

1 Add “id-mr” to the list of objects imported from UsefulDefinitions module in the authenticationFramework module

2 Add “AttributeType”, “Attribute”, and “MATCHING-RULE” to the set of objects imported into the authenticationFramework module from the InformationFramework module.

3 Add “GeneralNames” to the set of objects imported into the authenticationFramework module from the CertificateExtensions module.

4 Consider adding the following definition to the authenticationFramework module because this is imported into other modules in the X.500 Series of Recommendations, but had never been included in the 97 text of X.509:

```
HASH {ToBeHashed}     ::=     SEQUENCE {
     algorithmIdentifier          AlgorithmIdentifier,
     hashValue                    BIT STRING ( CONSTRAINED BY {
        -- must be the result of applying a hashing procedure to the DER-encoded octets --

      -- of a value of --ToBeHashed } ) }
```

5 Add the following OID assignments in the authenticationFramework module:

```
id-at-attributeCertificateRevocationList  OBJECT IDENTIFIER ::=      {id-at 59}

id-mr-attributeCertificateMatch         OBJECT IDENTIFIER                 ::=        {id-mr
42}
```

6 Add “Time” to the set of objects imported into the certificateExtensions module from the authenticationFramework module.

7 In the certificateExtensions module, and in the main text of X.509 clause 12.7.2, replace

CertPolicySet ::= SEQUENCE (1..MAX) OF CertPolicyId

with

CertPolicySet ::= SEQUENCE SIZE (1..MAX) OF CertPolicyId

12. Editor’s Response:

Accepted solution as proposed by source.