DEFECT REPORT FORM

1. Defect Report Number: **231**

   Title: Simple Credential ASN.1 Error in X.511

2. Source: CEN/ISSS/WS-DIR (ISSS-x511-1 R2

3. Addressed to: ISO/IEC JTC1/SC6 and ITU-T SG 7
   Editor Group on the Directory

4. (a) WG Secretariat: UK (BSI)
   (b) ITU-T WP: WP 4

5. Date Circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning: ITU-T Rec. X.511 (1997) | ISO/IEC 9594-3:1998

8. Qualifier: Error

9. References in Document: (e.g.: page, clause/section, figure, and/or table numbers)

"7.10 Security parameters", "8.1.1 Directory Bind Syntax ", and Annex A

10. Nature of Defect: (complete, concise explanation of the perceived problem)

Technical corrigendum 4 to edition 2 and technical corrigendum 2 to edition 3 update the **SimpleCredential** data type to allowed for generalized time. However, The ASN.1 is faulty. The **COMPONENT OF** is not allowed in a **CHOICE** construct. Even if it were, the tags would be the same for both choices. Only the second tag of each component would be different.

The definition proposed by these corrigenda is as follows:

```
SimpleCredentials ::= SEQUENCE {
        name                [0]     DistinguishedName,
        validity            [1]     SET {
        validityPeriod              CHOICE {
                                        COMPONENTS OF ValidityPeriodUTC,  -- UTC when v1
                                        COMPONENTS OF ValidityPeriodGT },  -- GT when > than v1
                random1             [2]     BIT STRING  OPTIONAL,
                random2             [3]     BIT STRING  OPTIONAL } OPTIONAL,
        password            [2]     CHOICE {
                unprotected                 OCTET STRING,
                protected                   SIGNATURE {OCTET STRING} } OPTIONAL}
```

```
ValidityPeriodUTC  ::=  SET  {
        time1          [0]     UTCTime OPTIONAL,
        time2          [1]     UTCTime OPTIONAL }

ValidityPeriodGT  ::=  SET  {
        time1          [0]     GeneralizedTime OPTIONAL,
        time2          [1]     GeneralizedTime OPTIONAL }
```

The notes suggested for 7.10 and 8.1.1 express requirement and should be normal normative text.

11. Solution Proposed by the Source: (optional)

The following construct should be used in 8.1.1 and Annex A instead of the ASN.1 proposed in technical corrigendum 4 to edition 2 and technical corrigendum 2 to edition 3.

```
SimpleCredentials  ::=  SEQUENCE  {
        name                [0]     DistinguishedName,
        validity            [1]     SET {
                time1               [0]     CHOICE {
                        utc                 UTCTime,
                        gt                  GeneralizedTime } OPTIONAL,
                time2               [1]     CHOICE {
                        utc                 UTCTime,
                        gt                  GeneralizedTime } OPTIONAL,
                random1             [2]     BIT STRING  OPTIONAL,
                random2             [3]     BIT STRING  OPTIONAL },
        password            [2]     CHOICE {
                unprotected                 OCTET STRING,
                protected                   SIGNATURE {OCTET STRING} } OPTIONAL}
```

Make the notes suggested by the technical corrigendum 4 to edition 2 and technical corrigendum 2 to edition 3 to normative text.

12. Editor's Response:

(any material proposed for processing as an erratum to, an amendment to, or a commentary on the IS or DIS final text/ITU Recommendation or Draft Recommendation is attached separately to this completed report).