DEFECT REPORT FORM

1.   Defect Report Number: 215 (Access Controls on Modifying RDN)

2.   Source: ISO Rapporteur

3.   Addressed to: ISO/IEC/JTC1/SC6/WG and ITU-T Study Group VII Q.15 (the Directory)

4.   (a)   WG Secretariat: US (ANSI)
          (b)   ITU-T WP: WP4

5.   Date Circulated by WG Secretariat:

6.   Deadline for Response from Editor:

7.   Defect Report Concerning:
(number and title of IS or DIS final text/ITU-T Recommendation)

      X.501/ ISO 9594-2 The Directory - (Final text)

8.   Qualifier: (e.g: error, omission, clarification required)

      Omission

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

      16.2.3

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

The independence of Access Control permissions has in general been adopted. However, one exception exists. The standard explicitly states that ModifyRDN permission grants Modify permission on attributes (plural) in the RDN. Specifically it prevents a DSA administrator from setting up a natural scenario where a user has permission to modify one attribute in a multi-attribute RDN and not another. Many directories (e.g. Entrust) use CN and uniqueidentifier (or similar) to identify organisational users. If we wished to allow the CN to be changed by end users or their agents, but wish to maintain control over the unique identifier, we cannot do this as the standard currently stands.

11.   Solution Proposed by the Source: (optional)

The proposed behaviour is for ModifyRDN and Modify permissions to be independent, in line with the rest of the permissions. So to change an RDN, both ModifyRDN permission and Modify permission are needed for any attribute in the RDN to be altered.

With the current permissions, one can construct an ACI so that a user may change a value if it is in an RDN, but not change a non-RDN value, and this ability would be lost with the proposed change. However, it is difficult to construct a real scenario where anyone would

want this capability, and so the gain is far more than the loss.

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/CCITT Recommendation or Draft
            Recommendation is attached separately to this completed report).