

## DEFECT REPORT FORM

1. **Defect Report Number :** 9594/226  
Title: CA system operational characteristics
2. **Source:** : ISO/IEC 9594-8 Editor
3. **Addressed to:** ISO/IEC JTC1/SC6 and ITU-T Study Group 7  
Editor Group on the Directory
4. (a) WG Secretariat : US (ANSI)  
(b) IUT-T WP : SG 7/WP 4
5. **Date Circulated by WG Secretariat**
6. **Deadline for Response from Editor**
7. **Defect Report Concerning :**  
  
X.509 (1997) and ISO/IEC 9594-8 (1998)  
The Directory: Authentication Framework
8. **Qualifier:** (e.g. error, omission, clarification required)  
  
Error
9. **References in Document:**  
  
11.2 Management of Certificates
10. **Nature of Defect :**  
  
The 2<sup>nd</sup> paragraph appears to be text that might have been relevant for the 1993 edition but not for 1997 and current conditions. For example, the first sentence reads “The production of a certificate occurs offline and shall not be performed with an automatic query/response mechanism. Note that the protocols

currently defined by the IETF PKIX WG (PKIX CMP and PKIX CMC) are both query/response protocols that facilitate certificate request/response messages.

Also, because this paragraph deals with the operating conditions of a CA system it is really outside the scope of X.509.

#### **11.Solution Proposed by the Source:**

Delete the second paragraph of 11.2 “The production of a certificate ... compromise unlikely.”.

#### **12. Editor' s Response:**