DEFECT REPORT FORM

1. Defect Report Number: 304rev1

Title: RSA encryption algorithm OID

2. Source: S. Boeyen (Entrust)

3. Addressed to:
4. (a)
   (b)

5. Date circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning: OID assignment for RSA encryption algorithm

ITU-T X.509 (1997) | ISO/IEC 9594-8: 1998 & ITU-T X.509 (2000) | ISO/IEC 9594-8: 2000

8. Qualifier: Clarification

9. References in Document:

3rd edition Annex H & 4th edition, Annex F

10. Nature of Defect:

In the 1st edition of X.509 (1988), an OID was assigned to the RSA encryption algorithm (2.5.8.1.1). However, the PKCS #1 specification assigned a different OID to the RSA encryption algorithm (1.2.840.113549.1.1.1). The signature process defined by the use of the OID in the X.509 Annex does not describe how to properly format the data, compute the message digest or otherwise process the signature beyond the basic mathematics of the RSA algorithm whereas the PKCS specification does. The PKCS#1 OID is the one that industry has adopted and profiled (e.g. in RFC 3279, RFC 3370) and there is a risk of interoperability problems if the X.509 defined OID is used.

11. Solution Proposed by the Source:

In 3rd edition Annex H and in 4th edition Annex F, deprecate the use of the id-ea-rsa OID (2.5.8.1.1)

12. Editor's Response: