DEFECT REPORT FORM

1. Defect Report Number: 299

Title: Clarify digitalSignature and NonRepudiation in the Key Usage extension

2. Source: Collaborative ITU-T & ISO/IEC meeting on Directory, Washington Sept 2002

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

5. Date circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning: Confusion over definition of digital signature and non-repudiation bits

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

8. Qualifier: Clarification

9. References in Document:

4th edition, 2000 clause 8.2.2.3
3rd edition, 1997, clause 12.2.2.3

10. Nature of Defect:

There is confusion over the text that explains the meaning of the digital signature and non-repudiation bits. These have been interpreted in different ways by various communities of interest. The purpose of this DR is to attempt to clarify the meaning of the bits, while at the same time support backward compatibility with the way the extension has been used in existing systems.

11. Solution Proposed by the Source:

In 8.2.2.3 (4th edition) and in 12.2.2.3 (3rd edition), replace list items a) and b) with the following:

If either **digitalSignature** or **nonRepudiation** or both bits are set, the certificate can be used to verify digital signatures that have purposes other than those identified in f) or g) below. Applications should document which of these two bits are appropriate for their use. Further understanding of the presence or absence of the **nonRepudiation** bit in an instance of the **keyUsage** extension if needed, is defined by policy. This policy may be reflected in a certificate policy definition, a contract, or other specification.

a) **digitalSignature**: for verifying digital signatures;

b) **nonRepudiation**: for verifying digital signatures which are intended to be used as evidence if a subsequent dispute arises, to prevent a signer from falsely denying involvement in a transaction. This bit does not, in itself, provide this assurance, but can be used together with other tools, such as an assertion of intent by the signer, an assertion from a third party notary to the transaction, a binding contract, policy statements etc, to assist in determining whether a signer's denial of involvement is a true or false claim.

NOTE - Policy may state, for example, that if the non-repudiation bit is set, the certificate may be used to verify signatures that are intended to be non-repudiable as well as those that are not.

In 8.2.2.3(4th edition) and 12.2.2.3 (3rd edition) , add the following as a new paragraph immediately following the bulleted list:

More than one bit may be set in an instance of the **keyUsage** extension. The setting of multiple bits shall not change the meaning of each individual bit but indicates that the certificate can be used for all of the purposes indicated by the set bits.

12. Editor's Response:

Accepted solution proposed by source.