DEFECT REPORT FORM

1. Defect Report Number: 9594/244

Title: Clarification of conformance to criticality

2. Source: X.509 Editor (on behalf of US Bridge CA project participants)

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

5. Date circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning:

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

8. Qualifier:

Error/Clarification

9. References in Document:

Several, See solution proposed by source

10. Nature of Defect:

X.509 clearly states what a certificate-using system is do in the case where certificate extensions are present and are are flagged critical. It also clearly states what a certificate-using system is to do in the case where certificate extensions are present, flagged non-critical, but are not recognized by a certificate-using system. However, there are errors, ambiguities and omissions about what a certificate-using system is to do when encountering a certificate extension flagged non-critical, that it does recognize and is capable of processing. To ensure that the requirements of certificate and CRL issuers, as well as requirements for consistent treatment of extensions by certificate-using systems, these errors must be fixed.

11. Solution Proposed by the Source:

In ITU-T Rec. X.509 and ISO/IEC 9594-8:

Change 1: In 1997 edition clause 8 and 2000 edition clause 7:

In the paragraph that begins "The extensions field allows addition of new ...", add the following two sentences to the end of the paragraph:

" When a certificate-using implementation recognizes and is able to process an extension, then the certificate-using implementation shall

process the extension regardless of the value of the criticality flag. Note that any extension that is flagged non-critical will cause inconsistent behaviour between certificate-using systems that will process the extension and certificate-using that do not recognize the extension and will ignore it."

Change 2: In 1997 edition clause 8 and 2000 edition clause 7:

Add the following immediately after the paragraph that begins "If unknown elements appear within the extension …":

A CA has three options with respect to an extension:

i) it can exclude the extension from the certificate;
ii) it can include the extension and flag it non-critical;
iii) it can include the extension and flag it critical.

A validation engine has two possible actions to take with respect to an extension:

i) it can ignore the extension and accept the certificate (all other things being equal);

ii) it can process the extension and accept or reject the certificate depending on the content of the extension and the conditions under which processing is occuring (e.g. the current values of the path processing variables).

Some extensions can ONLY be marked critical. In these cases a validation engine that understands the extension, processes it and acceptance/rejection of the certificate is dependent (at least in part) on the content of the extension. A validation engine that does not understand the extension rejects the certificate.

Some extensions can ONLY be marked non-critical. In these cases a validation engine that understands the extension processes it and acceptance/rejection of the certificate is dependent (at least in part) on the content of the extension. A validation engine that does not understand the extension accepts the certificate (unless factors other than this extension cause it to be rejected).

Some extensions can be marked critical or non-critical. In these cases a validation engine that understands the extension processes it and acceptance/rejection of the certificate is dependent (at least in part) on the content of the extension, regardless of the criticality flag. A validation engine that does not understand the extension accepts the certificate if the extension is marked non-critical (unless factors other than this extension cause it to be rejected) and rejects the certificate if the extension is marked critical.

When a CA considers including an extension in a certificate it does so withthe expectation that its intent will be adhered to wherever possible. If it is necessary that the content of the extension be considered prior to ANY reliance on the certificate, a CA would flag the extension critical. This must be done with the realization that any validation engine that does not process the extension will reject the certificate (probably limiting the set of applications that can verify

the certificate). The a CA may mark certain extensions non-critical to achieve backward compatibility with validation applications that cannot process the extensions. Where the need for backward compatibility and interoperability with validation applications incapable of processing the extensions is more vital than the ability of the CA to enforce the extensions, then these optionally critical extensions would be marked non-critical. It is most likely that CAs would set optionally critical extensions as non-critical during a transition period while the verifiers' certificate processing applications are upgraded to ones that can process the extensions.

Change 3: In 1997 edition clause 12.1 and 2000 edition clause 8:

In the paragraph that begins "In a certificate or CRL, an extension is flagged ...", add the following immediately after the third sentence that ends with "...ignoring the extension":

" If an extension is flagged non-critical, a certificate-using system that does recognize the extension, shall process the extension."

Change 4: In 1997 edition clause 12.2.2.3 and 2000 edition clause 8.2.2.3:

In the paragraph that begins "If the extension is flagged non-critical ...", replace the second sentence with the following:

"If this extension is present, and the certificate-using system recognizes and processes the keyUsage extension type, then the certificate using system shall ensure that the certificate shall be used only for a purpose for which the corresponding key usage bit is set to one."

Change 5: In 1997 edition clause 12.2.2.4 and 2000 edition clause 8.2.2.4:

In the paragraph that begins "If the extension is flagged non-critical ...", replace the second and third sentences with the following:

"If this extension is present, and the certificate-using system recognizes and processes the extendedKeyUsage extension type, then the certificate using system shall ensure that the certificate shall be used only for one of the purposes indicated."

Change 6: In 1997 edition clause 12.4.2.1 and 2000 edition clause 8.4.2.1:

In the 4th paragraph following the ASN.1, replace: "If this extension is present and is flagged critical then:" with the following:

"If this extension is present and is flagged critical, or is flagged non-critical but is recognized by the certificate-using system, then:"

Change 7: In 1997 edition clause 12.4.2.2 and 2000 edition clause 8.4.2.2:

Replace the last sentence "If this extension is present and is flagged critical ..." with the following:

"If this extension is present and is flagged critical, or is flagged non-critical but is recognized by the certificate-using system, then the certificate-using system shall check that the certification path being processed is consistent with the value in this extension."

12. Editor's Response:

Accepted solution provided by source.