draft-ietf-pki4ipsec-ikecert-profile-09

network resonance

Brian Korver
briank@networkresonance.com

Changes in -07

- § 3.2.2 changed "signing certificate" to "a certificate used for signing"
- § 3.1 changed table numbering from [1]…[4] to [a]…[d]
- § 4.1 added Bill Sommerfeld's "escape clause" re: implications of disabling certificate checks
- § 4.1.3.2 removed "If told (by configuration) to ignore KeyUsage (KU), accept cert regardless of its markings" from pseudocode
- § 4.1.3.12 clearer text from Bill Sommerfeld
- § 4.1.3.12 removed similar text from pseudocode
- § 4.1.3.17 removed gratuitous "private" modifier from SubjectInfoAccess section
- § 4.2.2.4.2 clarified delta CRL text so that it no longer could be read as implying that full CRLs can't be issued at the time a certificate is revoked

Changes in -07

§ 6.3. Disabling Certificate Checks

It is important to note that anywhere this document suggests implementors provide users with the configuration option to simplify, modify, or disable a feature or verification step, there may be security consequences for doing so. Deployment experience has shown that such flexibility may be required in some environments, but making use of such flexibility can be inappropriate in others. Such configuration options MUST default to "enabled" and it is appropriate to provide warnings to users when disabling such features.

Changes in -08

§ 3.3.6 clarified text, making clear that it applies to Main Mode only

§ Strength of Signature Hashing Algorithms added to Security Considerations

Describes the current state of MD5 and SHA-1 and proposes SHA-256 as something to consider implementing.

Changes in -09

§ 3.2.6 clarified text, making clear that it applies to Main Mode only

§ 4.3 Moved text regarding SHA-256 from security consideration