draft-ietf-pki4ipsec-ikecert-profile-09

network resonance

Brian Korver
briank@networkresonance.com

Changes Since -06 (IETF 64)

A few minor editorial changes, for instance:

- § 3.2.2 changed "signing certificate" to "a certificate used for signing"
- § 3.1 changed table numbering from [1]…[4] to [a]…[d]

But also…

§ 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.

§ 4.3. Strength of Signature Hashing Algorithms

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