RFC 5280 Clarifications Update

Steve Kent

Peter Yee

Updates from -04 to -05

- Simplified and updated Introduction
- Section 3.2: updated self-signed cert as TA language (aka “The Tar Pit”)
- Section 6.2: Clarified language on using or ignoring info in self-signed certs for path validation
- New text in Security Considerations about non-use of one-way hash security properties

Updates from -05 to -06

- Section 3.2: added [RFC5914] pointer and generalized wording beyond just self-signed certs as trust anchors

Current, Proposed Text for 3.2

Add the following paragraph to the end of RFC 5280, Section 3.2:

Consistent with Section 3.4.61 of X.509 (11/2008) we note that use of self-issued certificates and self-signed certificates issued by other than CAs are outside the scope of this specification. Thus, for example, a web server or client might generate a self-signed certificate to identify itself. These certificates, and how a relying party uses them to authenticate asserted identities, are both outside the scope of RFC 5280.