Additional Key Identifier Methods

draft-turner-additional-methods-4kis-00

Steve Kent
Sean Turner

IETF 78
26 July 2010

draft-turner-additional-methods-4kis-00.txt

- RFC 5280 currently defines two examples for how to generate key identifiers.
- Neither example is required, but <some|many> developers interpret the examples as required (the only algorithmic ways to generate key IDs)
- We want to explicitly add more methods that are similar to the example that's already there:
  - The keyIdentifier is composed of the least significant 160-bits of the SHA-224/256/384/512 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).

Comments

- We also could add a qualifier/type identifier for folks who want to know how the key ID was generated
- We could add a new extension to indicate the qualification, but that is a separate question
- We do NOT propose putting any bits in the current extensions (AKI/SKI) to indicate the hash algorithm used to generate the ID

Way Ahead

- Adopt as WG item?