DSA & ECDSA with SHA2s OIDs

Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA <draft-ietf-pkix-sha2-dsa-ecdsa-06.txt>

Draft Status

- Current Draft is -06
- Changes Since IETF 73 (-05)
  - Only editorial changes (e.g., boilerplate, updated references).
  - Blocked on publication of FIPS 186-3
- Known (Non-editorial) Issues
  - Three minor changes proposed
  - References to update

Proposed Change 1:
Section 3, 2nd Para., 2nd Sentence

OLD

"The certificate or CRL indicates the algorithm through an identifier, which appears in the signatureAlgorithm field within the Certificate or CertificateList."

NEW

"The certificate or CRL indicates the algorithm through an identifier, which appears in the signatureAlgorithm field within the Certificate or CerttificateList and in the signature field within the Certificate's TBSCertificate or the CertificateList's TBSCertlist, respectively."

Proposed Change 2:
Section 5, Last Para., Last Sentence

OLD

"…a CA should use the same or greater size hash function than the hash function in the digital signature algorithm in the certificate. "

NEW

"…a CA should sign a digital signature certificate with a digital signature algorithm which has equivalent or stronger security strength of the digital signature algorithm conveyed in the certificate."

Proposed Change 3:
Section 5, Para. 6th, Last Sentence

OLD

"The purpose of this is to ensure the keying material is in the proper format, the domain parameters are valid, the possession of the private key, the validity of the public key, and that the request is coming from an authorized source. "

NEW

"This Recommendation provides methods to ensure the validity of the public key, the validity of the domain parameters, the possession of the private key, the proper formatting of the keying material, and the authorization of the source of the request."

Last Call

- Questions & Comments?
- Is this document ready for last call?