RFC3278-update

draft-ietf-smime-rfc3278-update-00.txt

Sean Turner

Why

- Decide to put ECC requirements in informational RFC
- RFC 3278 defined use of ECC algorithms and CMS but it does not include SHA2 algorithms
- This ID, which updates RFC3278, adds these algorithms

What’s Updated

- Updates clauses: 2.1.1, 8, 9, and security considerations
- Allows the use of SHA-224, SHA-256, SHA-384, and SHA-512
- Adds OIDs for SHA-224, SHA-256, SHA-384, and SHA-512
- Adds OIDs for SHA-224, SHA-256, SHA-384, and SHA-512 with ECDSA
- Removed text about needing an update when SHA-256, SHA-384, and SHA-512 are defined.

Questions

?