S/MIME v3.2
draft-ietf-smime-3850bis-01.txt
draft-ietf-smime-3851bis-01.txt

Sean Turner

Blake Ramsdell

What’s Updated (1 of 2)

- Because of ECC IPR issues we removed references to ECDSA/ECDH
- 3850bis:
  - Added definitions for SHOULD+, SHOULD-, and MUST-
  - Updated key size requirements:
    - Key sizes from 512 bits to 2048 bits MUST be supported
    - Key sizes from 1024 bits to 2048 bits MUST be supported

What’s Updated (2 of 2)

- 3851bis:
  - Reference to FIPS180-2 changed to FIPS180-3
  - Updated key size discussion in 4.1
    - Moved some of the historical text to security considerations.
    - Old: A user agent SHOULD generate RSA key pairs at a minimum key size of 768 bits. A user agent MUST NOT generate RSA key pairs less than 512 bits long.
    - New: A user agent SHOULD generate RSA key pairs at a minimum key size of 1024 bits. A user agent MUST NOT generate RSA key pairs less than 1024 bits long.

Questions

?