RSA/SHA-2

draft-ietf-dnsext-dnssec-rsasha2-03

Jelte Jansen

Changes in -03

- Key and signature sizes
- Better wording

Open issues

- 2 new algorithms in IANA list
  - Optional
  - Mandatory

Open issues

- NSEC3
  - Leave out
  - 2 more algorithms
    - SHA256/NSEC3
    - SHA512/NSEC3
  - Mandatory
    - If you understand SHA-2, you understand NSEC3

Questions?