RFC4641-bis

Olaf M. Kolkman
NlnetLabs
olaf@NlnetLabs.nl
Administrivia


- Document is currently at version 2
  - Version 0: RFC4641 with nits corrected
  - Version 1: First attempt to address some issues

- http://www.nlnetlabs.nl/svn/rfc4641bis/trunk/open-issues
Resolved Issues

• HSM
  – Addressed in version 2 as part of rewrite of

• NSEC-NSEC3
  – New version 5
  – Remaining (non)issues:
    • NSEC responded with DO=0
    • Comment on RSASHA256

• REVIEW NIST
  – Scott Rose reported he reviewed and this issue can be closed
Resolved Issues continued

- ZSK-roll-frequency
- Cryptography_flawed
- Discussion_of_timescales
- Rollover_assumption

Issues are thought to be resolved by rewrite of section 3: Stressing operational considerations whereby the crypto parameters are a result of those and do not drive them.
Resolved Issues continued

• Non-cooperative-registies
  – Added as 4.4.5.2 Non Cooperating DNS Operators
  – Review of the figure needed but otherwise issue is closed
To Be Addressed

- trust_anchor_and_parent_keys
- differentiation_trustanchor_parent
- trust_anchor_configuration
- timing_technology

Added:
- Signature_validity
Question

• Please review the document on the issues thought to be resolved
  – I will close these issues in a few weeks

• Bring up new issues while you can