draft-ietf-sidr-roa-format-06

draft-ietf-sidr-rpki-manifests-05

Matt Lepinski
BBN Technologies

Digest and Signature Algorithms

- Foolish to specify algorithms separately in:
  - Certificate Policy
  - Certificate Profile
  - ROA Format
  - Manifest Format
  - And all future signed object specifications?
- The latest versions of ROA Format and RPKI Manifest drafts now reference draft-ietf-sidr-rpki-algs which specifies digest and signature algorithms for RPKI use.

ROA Format

- No changes of substance since last IETF other than the algorithms change on the previous slide

- Currently in WGLC, please send comments to the list by Monday, November 23
  - Thanks to everyone who has already reviewed this document
- One comment so far:
  - Draft currently does not prescribe an order in which ROA validity checks must be performed
  - If you feel there is a correct order that should be prescribed in this draft, please send text to the list

RPKI Manifests

- Summary:
  - A manifest is a signed object that contains a listing of all the signed objects in a repository publication point associated with a certification authority.
  - Manifests are intended to expose potential attacks against relying parties of the Resource Public Key Infrastructure.
  - For example, manifests allow a relying party to detect of objects from a repository or insertion of stale objects into a repository.

RPKI Manifests

- No changes of substance other than the algorithms change discussed earlier
- Only outstanding issue is a minor nit (which will be corrected in the next version)
- The authors believe this document is ready for Working Group Last Call

Thank You