Manifests for the Resource Public Key Infrastructure

draft-ietf-sidr-rpki-manifests-01.txt

Summary

This document defines a "manifest" for use in the RPKI. A manifest is a signed object that contains a listing of all the signed objects in the repository publication point associated with an authority responsible for publishing in the repository.

Update Summary

- Changes since -00 (Jan 08):
  - Manifest scope defined (sec 2.1)
    - Scope of all products signed by a CA and subordinate single-use EE certs or all products sugned by a multi-use EE cert
  - Manifest syntax defined (sec 2.2)
    - CMS wrapper MUST contain signing EE cert and CRL
  - CA Manifest generation modified wrt subordinate EE certs and signed products (sec 3.1)

Update Summary

- Changes (cont)
  - Manifest validation clarified (sec 5)
    - No changes to validation semantics
  - Relying Party use clarified (sec 6)
    - No changes to intended semantics

To Do

- Revise references for RFC5280
- Are we then done?