Document Updates

Geoff Huston
CA Key Rollover procedure

Proposed BCP

Extracted from notes contained in Certificate Profile draft:

- generate NEW CA instance with new key, same repository publication point
- re-issue all subordinate products using NEW CA
- flip CURRENT CA to OLD and NEW to CURRENT
- revoke and remove OLD CA
draft-ietf-sidr-keyroll-04.txt

• No further revisions planned for this draft
• WG Last Call requested
draft-ietf-sidr-res-certs-20.txt

• Resource Certificate Profile
• Proposed Standard
• Recent changes:
  – revised to simplify text and reduce overlap with RFC5280
  – removed description of multi-use EE certificates
  – clarified Subject Name construction
  – added notes in the Security Consideration section about potential hazards in subject name collision scenarios
draft-ietf-sidr-res-certs-20.txt

• No further revisions planned for this draft
• WG Last Call requested
draft-ietf-sidr-repos-struct-06.txt

- Distributed Repository Profile
- Proposed BCP
- Recent changes:
  - revised to simplify text
  - removed references to multi-use EE certificates and associated repositories
  - added recommendations on repository management to synchronise with manifest state
draft-ietf-sidr-repos-struct-06.txt

- No further revisions planned for this draft
- WG Last Call requested
• Issuer / Subject certificate management protocol
• Proposed Standard
• Recent changes:
  – removed reference to HTTPS and TLS transport
  – added CMS signing time constraint (signing time >= signing time of the previous message from the same sender)
  – noted proof of possession test in Issuance request
draft-ietf-sidr-rescerts-provisioning-08.txt

• No further revisions planned for this draft
• WG Last Call requested
• Defines semantics of ROA
• Proposed Informational RFC
• Recent changes:
  – clarifying text on validity state
  – grappled with AGGREGATOR in (proxy) aggregated paths and Origin AS
• I’m not happy with this rev of the draft:
  – Either revert to -07 draft definition of Origin AS
  – OR wait for IDR to deprecate AS_SETs
• Algorithm Specification for the RPKI
• Proposed Standard
• Recent changes:
  – text clean up
  – removed text relating to 3072 and 4096 bit key sizes
draft-ietf-sidr-rpki-algs-04.txt

• No further revisions planned for this draft
• WG Last Call requested
• Defines manifests in the RPKI repository system
• Proposed Standard
• Recent changes:
  – reference signed-object draft
  – simplify manifest generation text
  – remove reference to multi-use EE certs and associated repository manifest
draft-ietf-sidr-rpki-manifests-09.txt

• No further revisions planned for this document
• WG Last Call requested