Review of draft-ietf-sidr-arch-01.txt

Steve Kent

BBN Technologies

Document Outline

- PKI Overview
  - CA & EE Certificates
  - Trust anchors
  - **ERX**
- ROAs
- Repositories & **Manifests**
- **Local Cache Maintenance**
- Common Operations
  - Certificate issuance
  - ROA management
  - Route filter generation

bold/red = new material

PKI Section

- All certificates are “resource certificates”
  - Attest to holdings of address space and/or AS numbers
- CA certificates
  - Every resource holder is a CA
  - Resource holders can have multiple certificates
- EE certificates
  - Used to verify non-PKI signed objects, e.g., ROAs and manifests
  - 1-1 correspondence with signed objects enables simple revocation
  - Single-use private key model improves security
- Trust anchors
  - Choice of a TA is up to each relying party
  - the RIRs (or IANA) are the default TAs

PKI Section Major Changes

- Added certificate subject name conventions
  - Complements the certificate profile I-D
- Added discussion of RIRs vs. IANA as candidate, default TAs
  - no conclusion, just a discussion of pros and cons
- Added ERX discussion and diagram
  - Discusses how RIRs manage early registration allocations and how this is represented in the PKI

ROA Section

- ROA definition
- ROA content discussion
- ROA syntax
- ROA semantics
- ROA revocation

ROA Section Changes

- Added cites to ROA I-D
- Revised syntax to add exact match flag
  - In response to on-list discussion
- Added a diagram showing how allocations to one ISP from two sources affect certificate and ROA management
- Need to add discussion of how to match prefix(es) represented in a ROA to RFC 3779 syntax in an EE certificate for ROA validation

Repository System Section

- What is stored
  - Certificates
  - CRLs
  - Signed objects that all users require, e.g., ROAs & manifests
- Security considerations
  - Integrity of contents that are already signed
  - Availability
  - Need for access controls (but no spec for them)
- Repository operations
  - Upload
  - Download
  - Change/delete

Repository Section Changes

- Removed allusions to various details, will point to repository document for them
- Inserted rough diagram showing how CRLDP, AIA and SIA link repository elements
- Added discussion of manifests (syntax & semantics)
  - A manifest is a per-CA, signed blob used to detect certain forms of active attacks against the repository
  - Do we want a separate, short manifest document, like the ROA document?

Local Cache Management Section

- A new section, added to explain part of how the repository is used by relying parties
- Provides a simple algorithm describing how to maintain the local cache
- Probably needs more details: please provide feedback

Common Operations Section

- Certificate issuance
- ROA management
  - Ties to repository management
  - Single-homed subscribers
  - Multi-homed subscribers
  - Portable allocations
- Constructing route filters using ROAs

Operations Section Changes

- Added discussion of when certificates DON'T need to be issued
- Added a discussion of dealing with 4-byte AS numbers in ASes that understand only 2-byte AS numbers
- Still need to add top level discussion of certificate revocation and renewal, not just issuance
- Cite <???> for certificate issuance, renewal, and revocation details
- Need to add a discussion of how to match ROAs to BGP UPDATEs (should we do that here or in ROA document?)
- Still need to add a discussion of how an ISP can use ROAs to verify that a subscriber is the holder of address space the subscriber wants the ISP to advertise

Questions?