Multiple repository publication points for the RPKI

draft-rogaglia-sidr-multiple-publication-points-00

Roque Gagliano – Carlos Martinez
RPKI Repository structure + fetching today (top down)

1. Fetch Self-signed certificate and check signature

2. RPs begin fetching information from repositories using parent certificate SIA.

   - RFC 6487:
     - AIA: is a “a single reference”
     - SIA: order for access methods represents preference set by CA

3. You fetch the publication point for the next valid CA until you obtain all the resources.

RFC 6490: Single URI per TAL
Proposal:

• New TAL format:

- Each “Root Operator” will host a copy of the self signed certificate
- Each “Root Operator” can scale its infrastructures using any available mechanisms
- No single dependency in DNS name resolution.
  - Could even use IP addresses in URIs
- RP can select “Root Operator” with similar algorithms as DNS resolvers
  - Yes, you create more complexity on the RP side.
  - Reduce “Layer 9” noise as you create a root operators group (just like DNSSEC)

Change proposal: RFC 6490 section 2.1

The TAL is an ordered sequence of:
1) An *At least one* rsync URI [RFC5781],
2) A `<CRLF>` or `<LF>` line break *after each URI,* and
3) A `subjectPublicKeyInfo` [RFC5280] in DER format [X.509], encoded in Base64 (see Section 4 of [RFC4648]).
Scalable RPKI repository:

- Multiple CRL DP, AIA and SIA extensions (Showing CA cert only)
- Compatible with current proposals for new fetching methods: HTTP, zones, deltas
- `accessMethod` selection can be decided by RP, taking CA stated pref into account
- Small changes to existing documents:
  - AIA support for multiple operators
  - SIA order irrelevant
Feedback (so far)

• #1
  – Support for the idea, several comments raised and discussed
  – Maybe revisit RFC 5914 for TAL format if complexity increases too much

• #2
  – Similar idea presented in the past
  – If TAL format to be reviewed, why not look at RFC 5914?

• #3 (off-list)
  – Support for the idea
  – Some concerns about RP implementation and expected semantics of the different repository copies
Questions and Next Steps:

• Should we add multiple URI to the TAL format defined in RFC6490?
  – Marker or URI count needed to simply parsing?
• Should we maintain the SIA to express the CA preference or just leave it up to the RP to choose the accessMethod?
• Working group adoption?
THANK YOU!