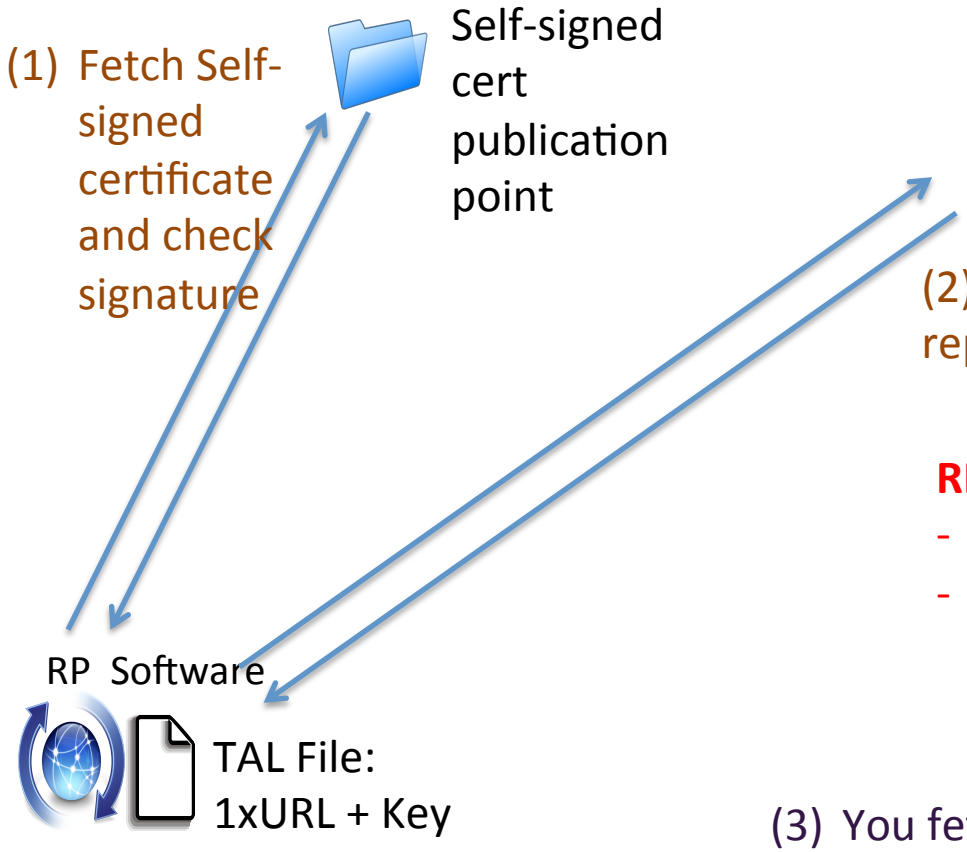
Multiple repository publication points for the RPKI

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

Roque Gagliano – Carlos Martinez

RPKI Repository structure + fetching today (top down)



RFC 6487:

- **AIA: is a "a single reference"**
- **SIA: order for access methods represents preference set by CA**

RFC 6490: Single URI per TAL

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

Proposal:

- New TAL format:

```
rsync://rpki.operator1.org/rpki/hedgehog/root.cer
rsync://rpki.operator2.net/rpki/hedgehog/root.cer
rsync://rpki.operator3.org/rpki/hedgehog/root.cer
  …
rsync://rpki.operatorN.com/rpki/hedgehog/root.cer
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAovWQL2lh6knDx
GUG5hbtCXvvh4AOzjhDkSHlj22qn/1oiM9IeDATIwP44vhQ6L/xvuk7W6
Kfa5yqmqQ+xOZOwTWPcrUbqaQyPNxokuivzyvqVZVDecOEqs78q58mSp9
nbtxmLRW7B67SJCBSzfa5XpVyXYEqYAjk3fpmefU+AcxtxvvHB5OVPIa
BfPcs80ICMqHQX+fphvute9XLxjfJKJWkhZqZ0v7pZm2uhkcPx1PMGcrG
ee0WSDC3fr3erLueaqpiLsFjwwpX6F+Ms8vqz45H+DKmYKvPSstZjCCq9
aJ0qANT9OtnfSDOS+aLRPjZryCNyvvBHxZXqj5YCGKtwIDAQAB
```

- 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]). ‘

- 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)

Scalable RPKI repository:

- Multiple CRL DP, AIA and SIA extensions (Showing CA cert only)

```
Authority Information Access:
    CA Issuers - URI:rsync://rpki.operator1.net/rpki/hedgehog/root.cer
    CA Issuers - URI:rsync://rpki.operator1.org/rpki/hedgehog/root.cer
    ...
    CA Issuers - URI:rsync://rpki.operator1.net/rpki/hedgehog/root.cer


 Subject Information Access:
    CA Repository - URI:rsync://rpki.operator1.net/member1/
    Manifest - URI:rsync://rpki.operator1.net/member1/CVPQSg.mft
    CA Repository - URI:rsync://rpki.operator2.org/member1/
    Manifest - URI:rsync://rpki.operator2.org/member1/CVPQSg.mft
    ...
    CA Repository - URI:rsync://rpki.operator3.net/member1/
    Manifest - URI:rsync://rpki.operator3.net/member1/CVPQSg.mft


X509v3 CRL Distribution Points:
    URI:rsync://rpki.operator1.net/member1/CVPQSg.mft
    URI:rsync://rpki.operator2.org/member1/CVPQSg.mft
     ...
    URI:rsync://rpki.operator3.net/member1/CVPQSg.mft
```

- 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?

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

THANK YOU!