Multiple Publication Points

draft-rogaglia-sidr-multiple-publication-points-02

sidr@ietf86

R. Gagliano

T. Manderson

C. Martínez

The idea

- Provide means for repository operators to indicate the presence of *multiple publication points* of repository data
- Motivation
  - An additional tool for repository HA engineering
  - Multiple transport protocols for the same repo data
  - Break free from DNS tyranny ☺

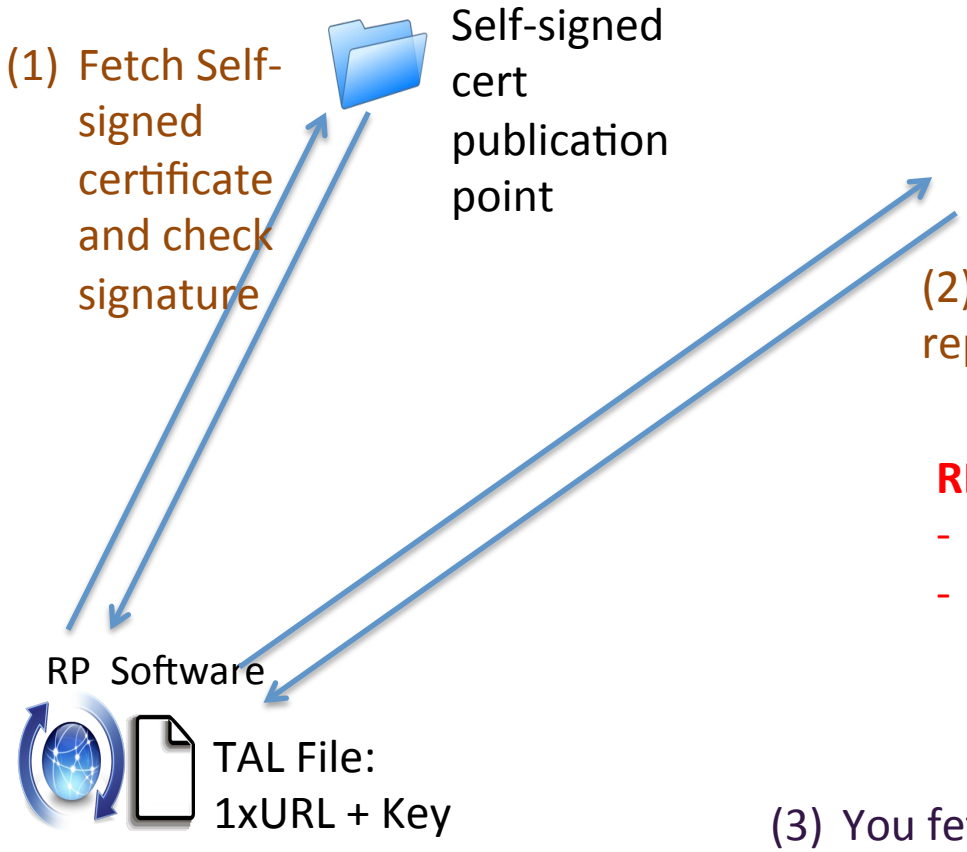
Repository HA Options

- Use already deployed (commercial?) CDNs
  - None of them supports rsync as of today**
  - Does not address DNS resolution diversity
- Load-balance your own server farm using DNS round-robin

Progress since Atlanta

- Rewrote most of the introduction / problem statement section:
  - Better explained HA issues as perceived by authors
    - Current options not entirely satisfactory
  - Proposed solution allows for:
    - Routing path and DNS resolution diversity
    - Multiple transport protocols

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.biz/rpki/hedgehog/root.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAovWQL2lh6knDx
GUG5hbtCXvvh4AOzjhDkSHlj22gn/loiM9IeDATIwP44vhQ6L/xvuk7W6
Kfa5ygmqQ+xOZOwTWPcrUbqaQyPNxokuivzyvqVZVDecOEqs78q58mSp9
nbtxmLRW7B67SJCBSzfa5XpVyXYEgYAjkk3fpmefU+AcxtxvvHB5OVPIa
BfPcs80ICMgHQX+fphvute9XLxjfJKJWkhZqZ0v7pZm2uhkcPx1PMGcrG
ee0WSDC3fr3erLueagpiLsFjwwpX6F+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/CVPQ0g.mft
    CA Repository - URI:rsync://rpki.operator2.org/member1/
    Manifest - URI:rsync://rpki.operator2.org/member1/CVPQ0g.mft
    ...
    CA Repository - URI:rsync://rpki.operator3.net/member1/
    Manifest - URI:rsync://rpki.operator3.net/member1/CVPQ0g.mft


X509v3 CRL Distribution Points:
    URI:rsync://rpki.operator1.net/member1/CVPQ0g.mft
    URI:rsync://rpki.operator2.org/member1/CVPQ0g.mft
     ...
    URI:rsync://rpki.operator3.net/member1/CVPQ0g.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

THANK YOU !