RPKI Retrieval Delta Protocol - RRDP

Tim Bruijnzeels
Oleg Muravskiy
Bryan Weber
Rob Austein
David Mandelberg

IETF93 | Prague | 24 July 2015

Update

- Running code deployed to RIPE NCC pilot environment

```
rsync://localcert.ripe.net/repository/ripe-ncc-pilot.cer
```


```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuxBjHKulutVC6gLcpQSUC3d3S
7738XLIQgwRF4EMAPj/jZ+yavGZq6v0oBsxlnr9nNUiyX+UPw+tYEDz7H2bAN3CWcg6fh
0Mt3uMPZqztvL/O4Yhz+dAhXDXcZ8Ae4GWx2RjPam2H3spNqoUwJImfRc8PKN4Tgwv3bq
GnTVQeWWjBzMmwenfKWG5zkS2WdaihmkD6xM04zfCsHWawm9t3BT9av0lXtCq/e2Ys7Qz
Iyhmv7zQ0zsYdrmJ3wbIvaNR60jfz4+GhSTNV47ZPYuFUb8Svpw9xakBFVN1kQPsREb0V
si+eEx0xZMs062eNulcK09OCa03XWLoH2M7HqYG4QIDAQAB
```

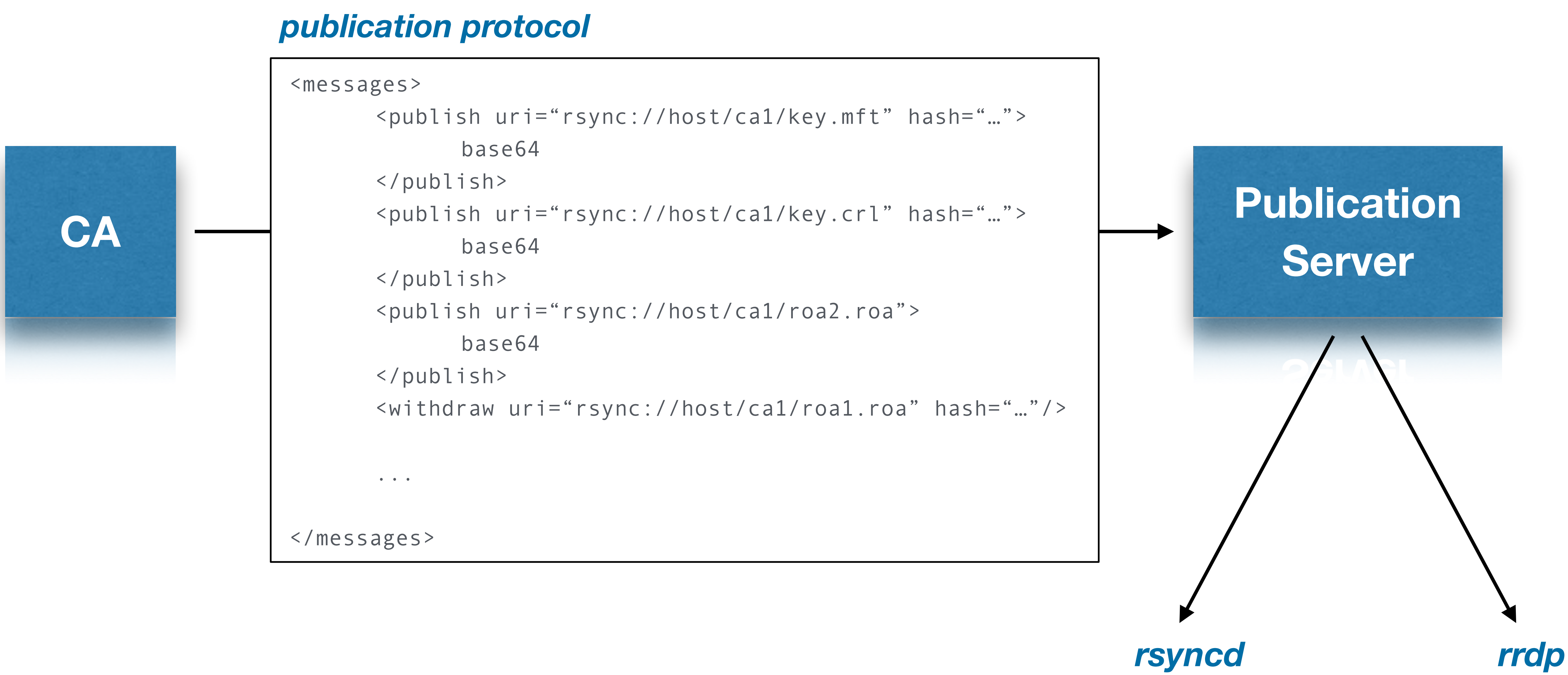

- Publication Server
  - https://localcert.ripe.net/rrdp/notification.xml
  - https://github.com/RIPE-NCC/rpki-publication-server

- Validator
  - http://localcert.ripe.net:8088/
  - https://github.com/RIPE-NCC/rpki-validator

Quick Overview

```
...
Issuer : CN=ripe-ncc-pilot
Subject: CN=ripe-ncc-pilot
Not Before: Jul 20 13:32:36 2015 GMT
Not After : Jul 20 13:32:36 2020 GMT
 Subject Information Access:
  1.3.6.1.5.5.7.48.5  - URI:rsync://localcert.ripe.net/repository/
  1.3.6.1.5.5.7.48.10 - URI:rsync://localcert.ripe.net/repository/ripe-ncc-pilot.mft
  1.3.6.1.5.5.7.48.13 - URI:https://localcert.ripe.net/rrdp/notification.xml
...
```

Quick Overview



Quick Overview

publication-protocol → **Publication Server**

https://localcert.ripe.net/rrdp/notification.xml

```
<notify … session="…" serial="…" version="1">
      <snapshot uri="…"  hash="…" />
      <delta serial="…" uri="…" hash="…"/>
      <delta serial="…" uri="…" hash="…"/>
      ...
</notify>
```

updated regularly at stable (https) URL

https://localcert.ripe.net/rrdp/a…9/718/delta.xml

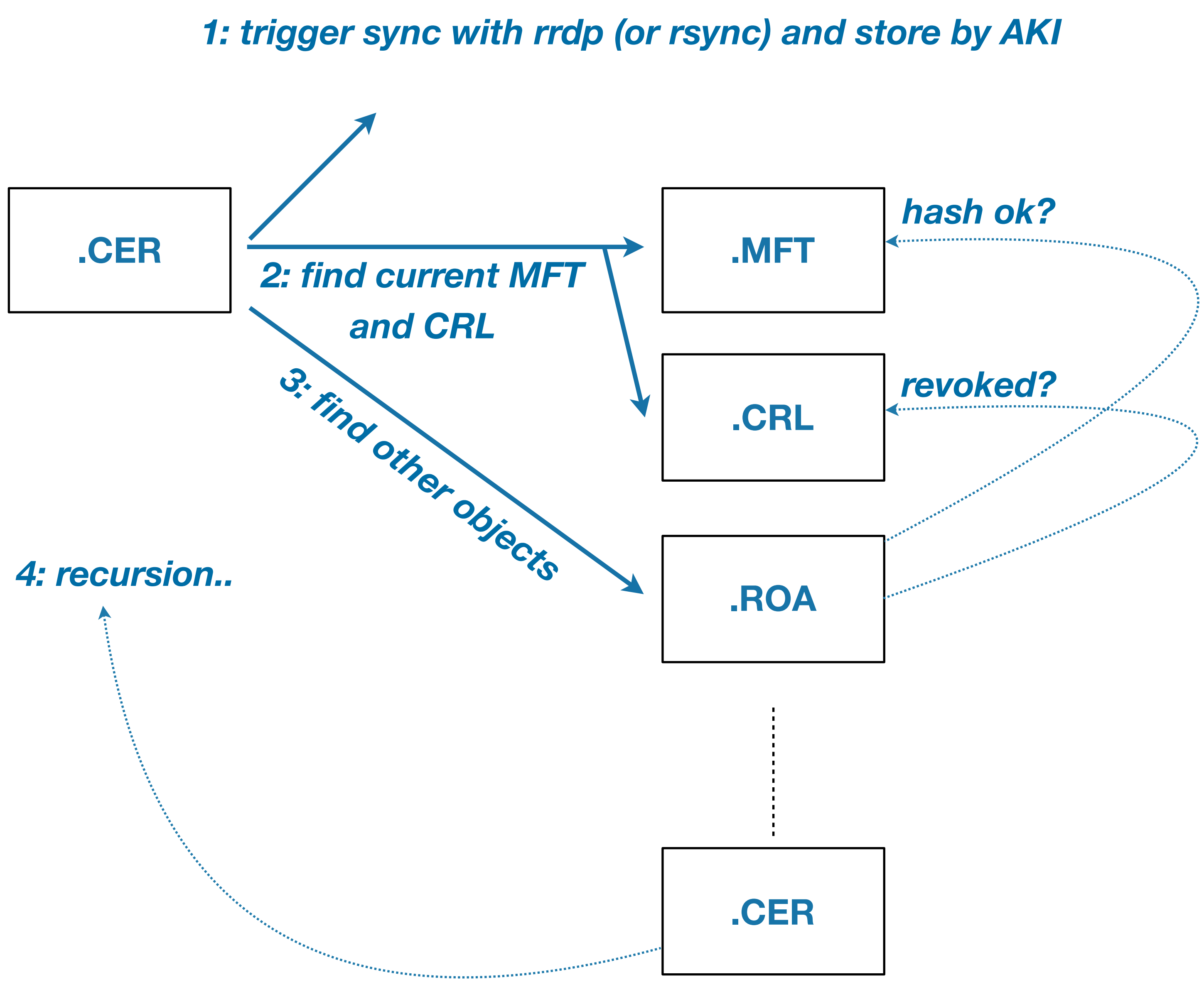
```
<delta session="…" serial="…" version="1">
  <publish uri="rsync://host/ca1/key.mft" hash="…">
    base64
  </publish>
  <publish uri="rsync://host/ca1/key.crl" hash="…">
    base64
  </publish>
  <publish uri="rsync://host/ca1/roa2.roa">
    base64
  </publish>
  <withdraw uri="rsync://host/ca1/roa1.roa" hash="…"/>
...
</delta>
```

https://localcert.ripe.net/rrdp/a…9/718/snapshot.xml

```
<snapshot session="…" serial="…" version="1">
  <publish uri="rsync://host/ca1.cer">
    base64
  </publish>
  <publish uri="rsync://host/ca2.cer">
    base64
  </publish>
  <publish uri="rsync://host/ca1/roa2.roa">
    base64
  </publish>
  <publish uri="rsync://host/ca2/roa1.roa">
    base64
  </publish>
...
</snapshot>
```

Immutable data for a given session and version - published at unique (https) URLs to allow caching (CDN)

One way to validate: Key Identifiers and Hashes



@1:

Retrieve objects and store in cache

Skip retrieval if needed

@2:

Manifest with EE cert AKI matching .cer SKI

Valid signature

Highest manifest number

Having 1 CRL that can be found by hash

Not revoked

@3:

Find all other objects by hash

Ignore CRLDP, use CRL found in step 2

Matching URIs (for now)

@4:

For any valid .cer found

RIPE NCC implementation findings

- Unvalidated cache
  - Distrusting 'withdraw', deleting objects X days after they are last encountered in validation
- Clean up old snapshots and deltas on publication server
  - 60 minutes after they are no longer included on notify.xml
  - Only have deltas up to size of snapshot
  - Other strategies?
- Publication clarifications
  - Whole set rejected if there is one or more error
  - Report 'success' on object before an error
  - Stop processing on error
  - Error codes (e.g. object not found, not authorized, internal error)
  - Recommended: CA performs "<list>" request

Next steps

- Testing!
  - Monitor pilot
  - Interop testing with rpstir and rcynic

- Experimenting
  - Use caching server and / or CDN
  - Load test server using multiple validators
  - Experiment with cache settings

Next steps

- Update delta document
  - https - TAs for https certificate?
  - otherwise, only small nits so-far
  - recommendations (caching, how many deltas) - extract to informational doc?
- Update publication document with clarifications and error codes
- Informational document on validation

Questions? Comments?