SHOULD I RUN MY OWN RPKI CERTIFICATE AUTHORITY?

ALEX BAND

NLNETLABS

RIPE 78 EDITION
NLNET LABS?
Purveyors of fine open source software since 1999
BGP?
RPKI!
ROUTING SECURITY
The RIPE Meeting network, AS2121, is now doing #RPKI Origin Validation invalid=reject
#routingsecurity #RIPE78

5:21 PM · May 20, 2019 · TweetDeck

18 Retweets 32 Likes
Routing Working Group
Thursday, 23 May 11:00 - 12:30
Wait, how did we get here?
RPKI QUICK START

- Resource Public Key Infrastructure
- Standardised in RFC 6480 - 6493
- Aimed at making Internet routing more secure
  - Provide Route Origin Validation (ROV) now
  - Stepping stone to Path Validation
ROUTE ORIGIN VALIDATION

- Organisation holds certificate containing all Internet Resources
- Uses it to make authoritative statements about intended BGP routing
  - Signed objects called Route Origin Attestation (ROAs)
- Other operators — “Relying Parties” — download and verify ROAs
  - Make routing decisions based on the outcome;
  - Valid, Invalid or NotFound
“Is this BGP route origination authorised by the legitimate holder of the IP space?”
route: 185.49.140.0/22
descr: Stichting NLnet Labs
origin: AS199664
mnt-by: NLNETLABS-MNT
created: 2014-03-10T12:25:24Z
last-modified: 2015-02-23T11:56:03Z
source: RIPE
AFRINIC, ALTDB, AOLTW, APNIC, ARIN, BELL, BBOI, CANARIE, EASYNET, EPOCH, HOST, JPIRR, LEVEL3, NESTEGG, NTTCOM, OPENFACE, OTTIX, PANIX, RADB, REACH, RGNET, RIPE, RISQ, ROGERS, TC

irr.net/docs/list.html
route:  185.49.140.0/22
origin:  AS199664
more:  stuff
route: 185.49.140.0/22
origin: AS199664
more: stuff

Route Origin Attestation (ROA)

AS199664, [(185.49.140.0/22, 22)]
route: 185.49.140.0/22
origin: AS199664
more: stuff
route: 185.49.140.0/22
origin: AS199664
more: stuff
route: 185.49.140.0/22
origin: AS199664
more: stuff
HOSTED VS. DELEGATED RPKI

- **Hosted RPKI**
  - The resource issuer — RIR, NIR, LIR — offers RPKI as a service
  - Certificates, keys, and signed products are all kept and published in their infrastructure

- **Delegated RPKI**
  - Run your own Certificate Authority, generate your own signed products and publish them yourself
HOSTED RPKI

- All five RIR have been offering Hosted RPKI since 2011
- Easy to get started and use
- Great to gain operational experience with the technology
- No cost of hardware, operations, key storage, publication, etc.
- No worries about uptime or availability (at least not first hand)
RPKI Dashboard

**2 BGP Announcements**
- 2 Valid
- 0 Invalid
- 0 Unknown

**2 ROAs**
- 2 OK
- 0 Causing problems

<table>
<thead>
<tr>
<th>BGP Announcements</th>
<th>Route Origin Authorisations (ROAs)</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discard Changes</td>
<td>Delete ROAs</td>
<td>Causing Problems</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AS number</th>
<th>Prefix</th>
<th>Most specific length allowed</th>
<th>Affects</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS199664</td>
<td>2a04:b900::/29</td>
<td>29</td>
<td>1</td>
</tr>
<tr>
<td>AS199664</td>
<td>185.49.140.0/22</td>
<td>22</td>
<td>1</td>
</tr>
</tbody>
</table>
HOSTED RPKI — RIR DIFFERENCES

- Different user interfaces with varying functionality and guidance
- Possibilities for batch processing and auto-renewing ROAs
- Multi-user support, access control, two-factor authentication
- ROA publication interval (varies between minutes to several hours)
- Application Programming Interface
- Support level (24/7)
Delegated RPKI

- Run Certificate Authority (CA) as a child of the RIR/NIR/LIR
- Install and maintain software yourself
- Generate your own certificate, have it signed by the parent CA
- Publish signed objects yourself, or ask a third party to do it for you
DELEGATED RPKI

- You can be operationally independent from the parent RIR
- Allows better integration and automation with your own systems
- If you run a global network, you can operate a single system rather than maintain ROAs in up to five web interfaces
- You are in control of the ROA publication interval
- You can delegate or offer RPKI as a service to your customers
RPKI CA SOFTWARE

- rpkid, by Dragon Research Labs
DIVERSITY
FUNDING?
<table>
<thead>
<tr>
<th>Embedded Trust Anchor Details</th>
<th>IPv4 &amp; IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASNs</td>
<td></td>
</tr>
<tr>
<td>AS0-AS4294967295</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>

IPv6: ::/0
KRILL ROADMAP

✔ Event sourcing architecture with API, CLI and UI

✔ Creation of RPKI objects

✔ RFC compliant publication server

✔ Embedded Trust Anchor for testing

• Operate under remote parent

• ROA suggestions, Multi-master support, HSM support (if desired)
“What kind of setup will I need, in terms of software, hardware and services?”
HARDWARE & CONNECTIVITY

- Certificate Authority
  - Modest hardware is fine for most use cases
  - No HSM needed; keys on disk are fine, really
- Publication Server
  - Internet-facing, with all related consequences
  - Run it yourself, or outsource it – the hybrid option
Publication Infrastructure

- RPKI relies on rsync for distribution for now
- RPKI Repository Delta Protocol (RRDP), using HTTPS, is its replacement
  - Deployed by RIPE NCC and APNIC
  - ARIN has it on their suggested work items for 2019
  - Ideally suited for CDN participation in publication
- Note: CA doesn’t need uptime, your publication server does!
WHAT IF IT BREAKS?

- No DNSSEC horror story; e.g. unavailable zone due to signing mishap
- RPKI provides a positive statement on routing intent
- Lose your keys? Hardware failure? Publication server being DDOSed?

All routes will eventually fall back to the “NotFound” state, as if RPKI were never used
WHY RUN YOUR OWN RPKI CA

- Delegate ROA management to different business units or customers
- Offer Hosted RPKI to downstream customers
- Tight integration with your routing provisioning (API)
- Manage ROAs seamlessly and transparently across multiple RIRs
- Fine-grained access control
- Control over ROA publication interval