SHOULD I RUN MY OWN RPKI CERTIFICATE AUTHORITY?

MARTIN HOFFMANN

NANOG 75
NLNET LABS?
Purveyors of fine open source software since 1899
RPKI QUICK START

- Resource Public Key Infrastructure
- Aimed at making Internet routing more secure
  - Provide Route Origin Validation (ROV) now
  - Stepping stone to Path Validation
ORIGIN VALIDATION QUICK START

- Organisation holds certificate containing all Internet Resources

- Uses it to make authoritative statements about intended routing
  - Signed objects called Route Origin Authorizations (ROAs)
  - Other operators — “Relying Parties” — download and validate 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?”
THE MOVING PARTS
RPKI CERTIFICATE STRUCTURE

AFRINIC

LACNIC

APNIC

ARIN

RIPE NCC

NIR

LIR

LIR

LIR

LIR

LIR

LIR

LIR

ISP

ISP
SEPARATE COMPONENTS

CERTIFICATE AUTHORITY
creates & signs

PUBLICATION SERVER
makes available
RPKI VALIDATION

LACNIC repository

ARIN repository

NIR repository

LIR repository

RELYING PARTY SOFTWARE

validated cache

rsync

RPKI-RTR

Relying Party Software

validated cache

rsync

RPKI-RTR
ORIGIN VS. PATH VALIDATION

- Route Origin Validation (ROV) already provides value for most issues:
  - Most mis-originations are accidental – “fat-fingering”
  - For many networks, the most important prefixes are one hop away
- Practical Path Validation is achievable, drafts are in progress:
  - draft-azimov-sidrops-aspa-profile
  - draft-azimov-sidrops-aspa-verification
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
All five RIR have been offering Hosted RPKI since 2011

Request certificate and issue ROAs through web portal

Implementations vary across regions:

- ROA Request Generation Key Pairs in ARIN
- User interface guidance to create high quality ROAs
- Setting up alerts for misconfigurations and possible hijacks
RIPE NCC
RIPE Network Coordination Centre

You are here: Home > Manage IPs and ASNs > LIR Portal

My LIR

Resources
- My Resources
- Request Resources
- Request Transfer
- IPv4 Transfer Listing Service
- RPKI Dashboard

RIPE Database

**RPKI Dashboard**

<table>
<thead>
<tr>
<th>2 BGP Announcements</th>
<th>2 ROAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>![2 Valid](2 Valid)</td>
<td>![2 OK](2 OK)</td>
</tr>
<tr>
<td>![0 Invalid](0 Invalid)</td>
<td>![0 Causing problems](0 Causing problems)</td>
</tr>
<tr>
<td>![0 Unknown](0 Unknown)</td>
<td></td>
</tr>
</tbody>
</table>

**BGP Announcements**

- **Discard Changes**
- **Delete ROAs**

<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><img src="1" alt="1" /></td>
</tr>
<tr>
<td>AS199664</td>
<td>185.49.140.0/22</td>
<td>22</td>
<td><img src="1" alt="1" /></td>
</tr>
</tbody>
</table>

Show 25 of 2 items
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
  - When a relying party connects to the Trust Anchor, it will automatically follow the chain down to your publication point
WHICH ONE IS RIGHT FOR ME?
Whatever you choose, go all in!

- It’s better to create no ROAs than bad ones
- Once you start create ROAs, maintain them!
- Make RPKI part of standard operations
- Set up monitoring and alerting
- Train your first line help desk
On 2018-11-12 @Orange_France AS3215 replaced multiple /16 BGP announcements with /17s, unfortunately they didn't update their #RPKI ROAs causing big junks of IP space to become RPKI-unreachable.

This increases the RPKI unreachable IP space to >10k /24s

nusenu.github.io/RPKI-Observato...
HOSTED RPKI

- No cost of hardware, operations, key storage, publication, etc.
- No worries about uptime or availability (at least not first hand)
- Easy to get started and use
- Great to gain operational experience with the system
- Almost nothing to manage
DELEGATED RPKI

- Better integration with operator’s own systems
- Organization will be the only one in possession of their private key
- Organization is operationally independent from the parent RIR
- Operator of a global network can operate a single system, rather than maintain ROAs in up to five web interfaces
CHOOSING
DELEGATED RPKI
“What kind of setup will I need, in terms of software, hardware and services?”
OPEN SOURCE CA SOFTWARE

- rpkid, by Dragon Research Labs
  - Python-based solution
- Krill, by NLnet Labs
  - Rust-based solution
  - Coming late 2019
**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
THE HYBRID OPTION

- Hosted publication server
  - No worries about uptime, DDOS attacks, etc.
  - At least one $cloud provider has offered to run this as a free service
- RIR-Independent Hosted CA
  - RPKI-as-a-Service
  - Business Model?
• RPKI relies on rsync for distribution for now

• RRDP, which uses HTTPS, is its replacement (RFC8182)
  • 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!
SHOULD I CHOOSSE DELEGATED RPKI?

• Is Delegated RPKI more secure? No!
  
  • The RIR giveth, the RIR taketh away;
    they can always revoke your certificate anyway

• Is Delegated RPKI more convenient? It depends...

• How many prefixes do you manage (across the globe) and how often do they change?

• Is the pain of running your own software less than clicking around one or more web interfaces at 3AM
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 “Not Found” state, as if RPKI were never used
FURTHER READING
RPKI DOCUMENTATION PROJECT

https://rpki.readthedocs.io