SHOULD I RUN MY OWN RPKI CERTIFICATE AUTHORITY?

MARTIN HOFFMANN

NLNETLABS

NANOG 75

NLNET LABS?


Purveyors of fine
open source software
since 1899

NSD

unbound

RPKI

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

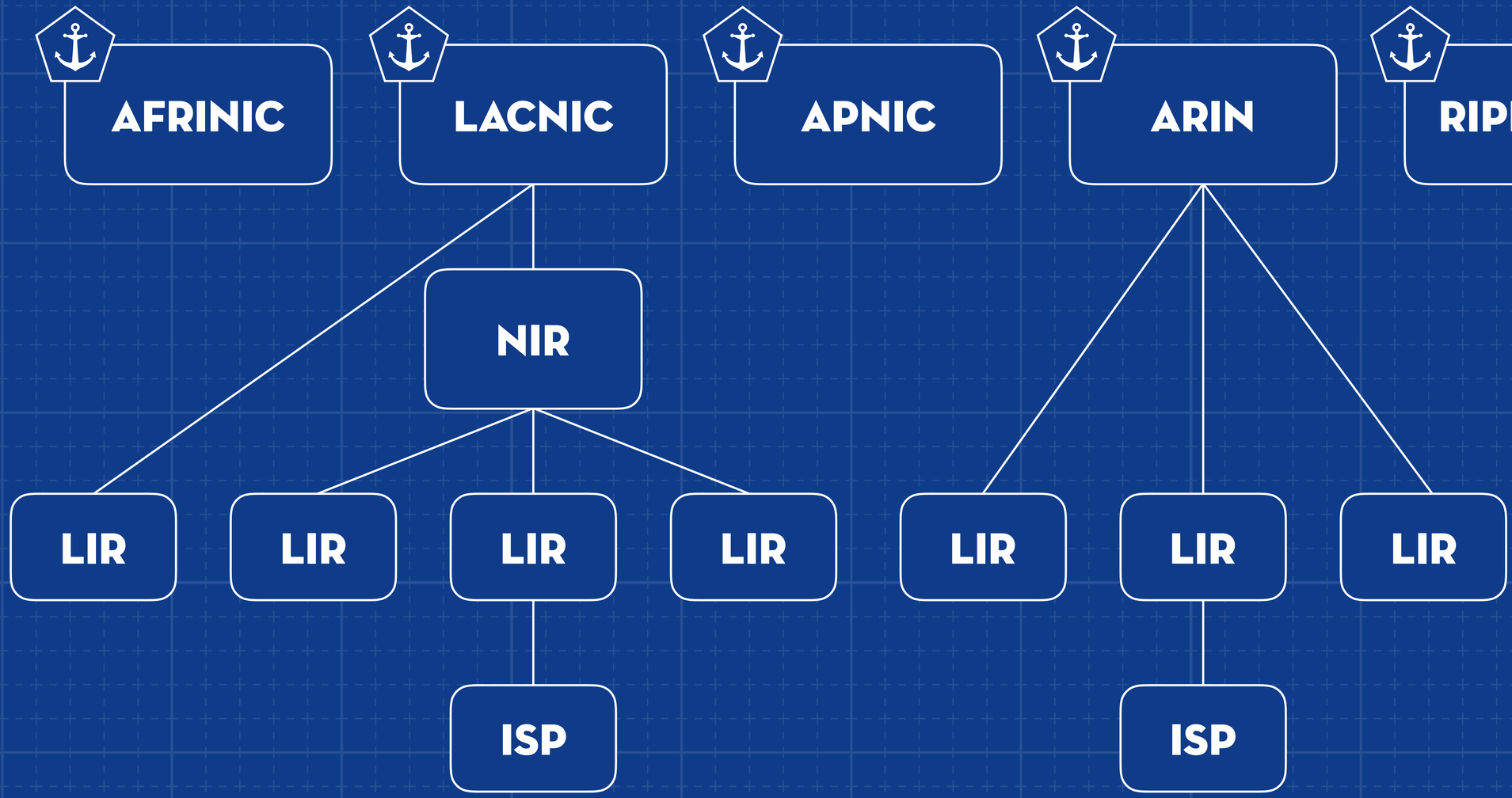
ORIGIN VALIDATION QUICK START

- 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

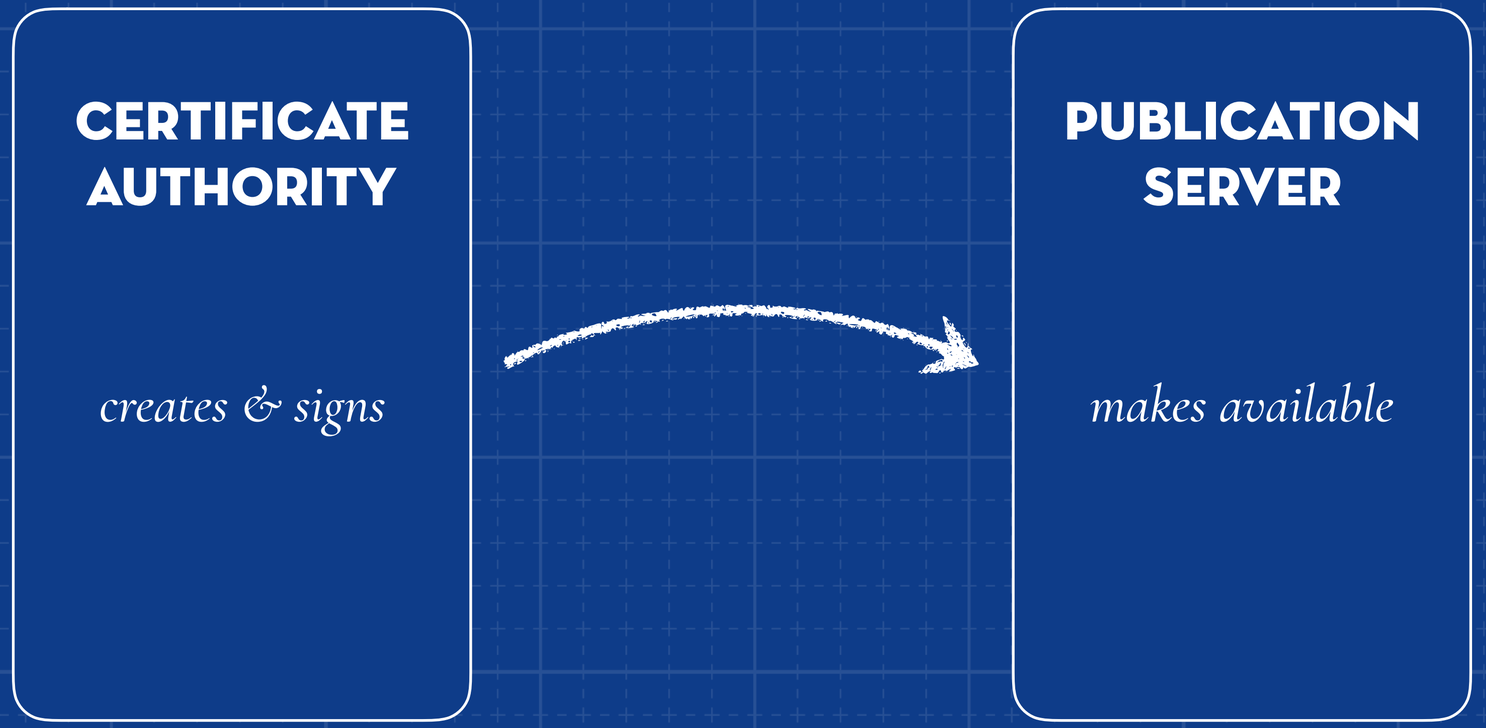
“Is this BGP route origination authorised by the legitimate holder of the IP space?”

THE MOVING PARTS

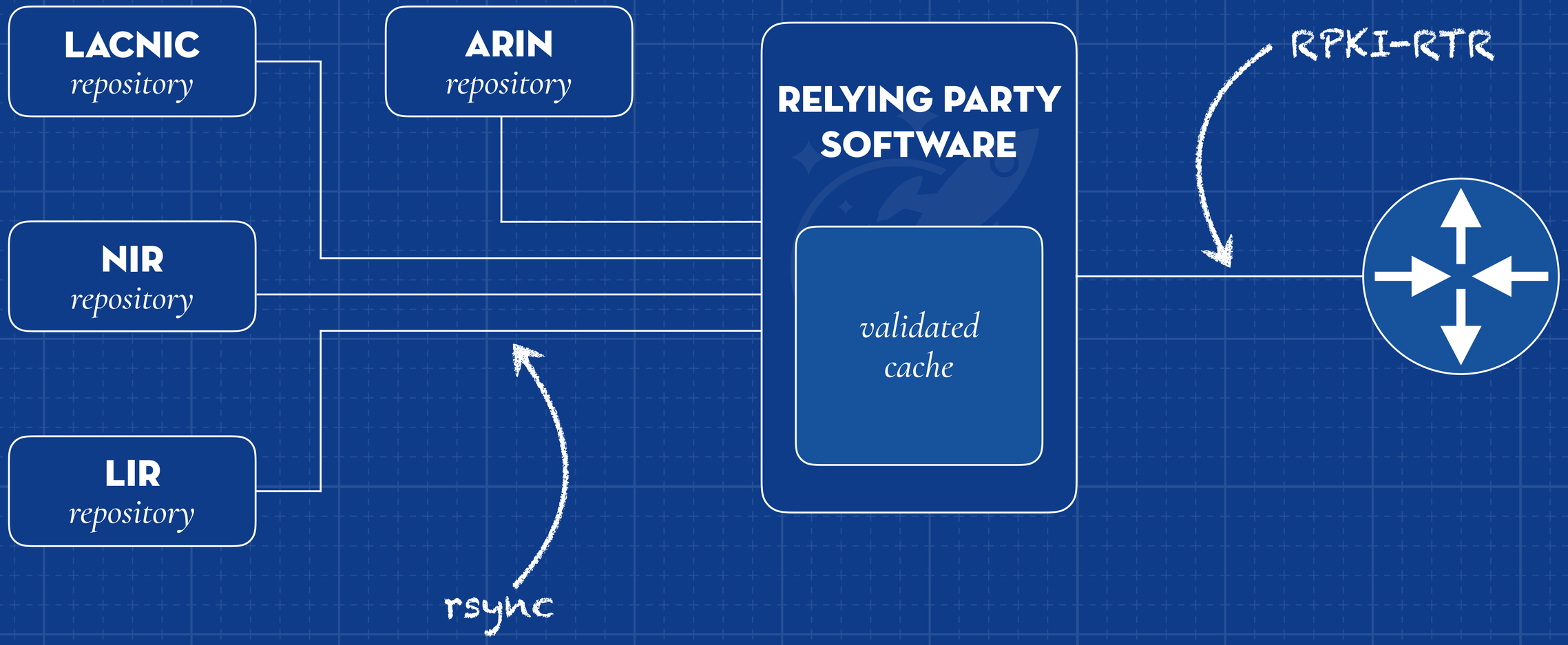
RPKI CERTIFICATE STRUCTURE



SEPARATE COMPONENTS



RPKI VALIDATION



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

HOSTED RPKI

- 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

RIPE Database (Whois) | Website

Search IP Address and ASN

Manage IPs and ASNs | Analyse | Participate | Get Support | Publications | About Us

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

You are editing: Stichting NLnet Labs

- My LIR
- Resources
  - My Resources
  - Request Resources
  - Request Transfer
  - IPv4 Transfer Listing Service
  - RPKI Dashboard
- RIPE Database

RPKI Dashboard

2 CERTIFIED RESOURCES | ALERTS ARE SENT TO 1 ADDRESS

2 BGP Announcements

2 Valid | 0 Invalid | 0 Unknown

2 ROAs

2 OK | 0 Causing problems

BGP Announcements | Route Origin Authorisations (ROAs) | History

Search...

Discard Changes | Delete ROAs | Causing Problems | Not Causing Problems | + New ROA

AS number	Prefix	Most specific length allowed	Affects
AS Number	Prefix	Max length	
AS199664	2a04:b900::/29	29	1
AS199664	185.49.140.0/22	22	1

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?

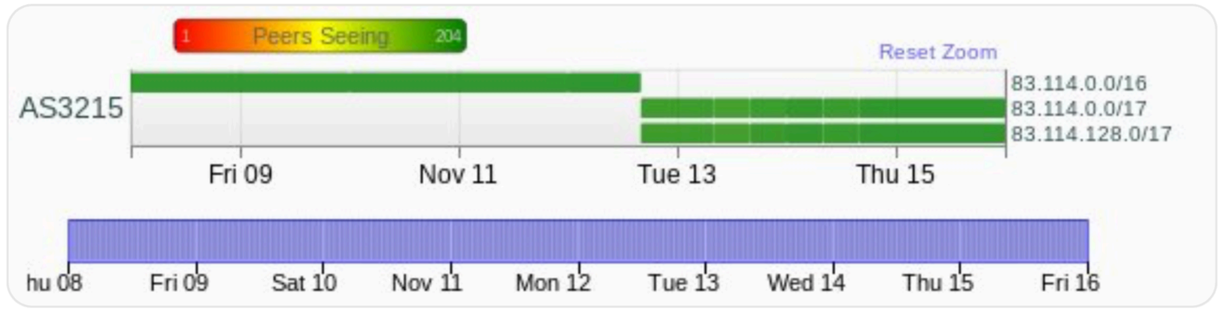
WHATEVER YOU CHOOSE, GO ALL IN!

- 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

nusenu
@nusenu_

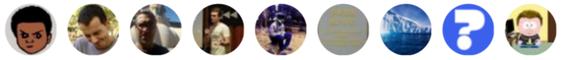
On 2018-11-12 @Orange_France AS3215 replaced multiple /16 BGP announcements with /17s, unfortunately they didn't update their #RPKI ROAs causing big junks of IP space to become RPKI-unreachable.

This increases the RPKI unreachable IP space to >10k /24s
nusenu.github.io/RPKI-Observato…



11:18 AM - 16 Nov 2018

16 Retweets **17** Likes



16 17

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?

PUBLICATION INFRASTRUCTURE

- 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 CHOOSE 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 "NotFound" state, as if RPKI were never used

FURTHER READING

RPKI DOCUMENTATION PROJECT

https://rpki.readthedocs.io

nlnetlabs.nl/rpki

rpki-team@nlnetlabs.nl

@nlnetlabs

NLNETLABS