A QUICK INTRO TO

RPKI

ALEX BAND

NLNETLABS

NLNET LABS?

Purveyors of fine
open source software
since 1899

NSD

unbound

ROUTINATOR

A NEW NLNET LABS PROJECT

RPKI DEPLOYATHON

2019

Day 2

8 March 2019

09:00 – 09:30 Welcome

09:30 – 10:30 Talks

- How to deploy RPKI in a live network
- licy considerations:

r, Fusix Networks

NT

on, Cloudfare

Break

n Work in Teams

Work in Team

d Dri

cus on

KRILL

RPKI Certificate Authority

NLNETLABS
Projects
Support
Community
Research
Services
About
Blog
Support Us

RPKI TOOLS

About | Krill | Routinator | Analytics | FAQ | Funding and Support | RFC Compliance

Coverage
Analyse this!

IP or ASN scope: AS13335

Announcements

Valid	1155
Invalid ASN	0
Invalid Length	3
Not Found	28

Payloads

Verified ROA Payloads	805
Unseen	12

Show raw results

100.0%
88.9%
77.8%
66.7%
55.6%
44.5%
33.4%
22.3%
11.2%
0.1%

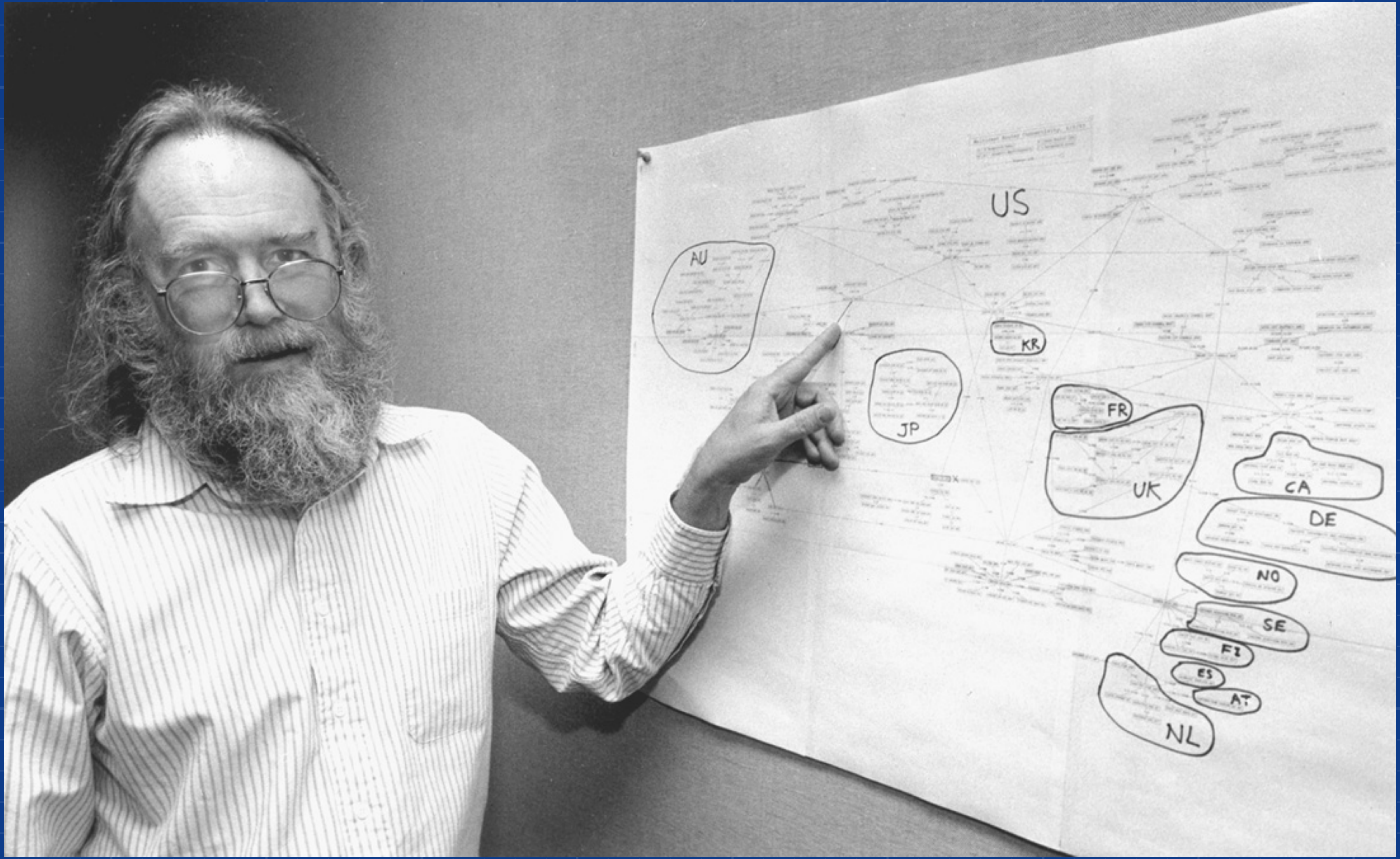
The fraction of announced IPv4 and IPv6 prefixes in BGP covered by RPKI ROAs.

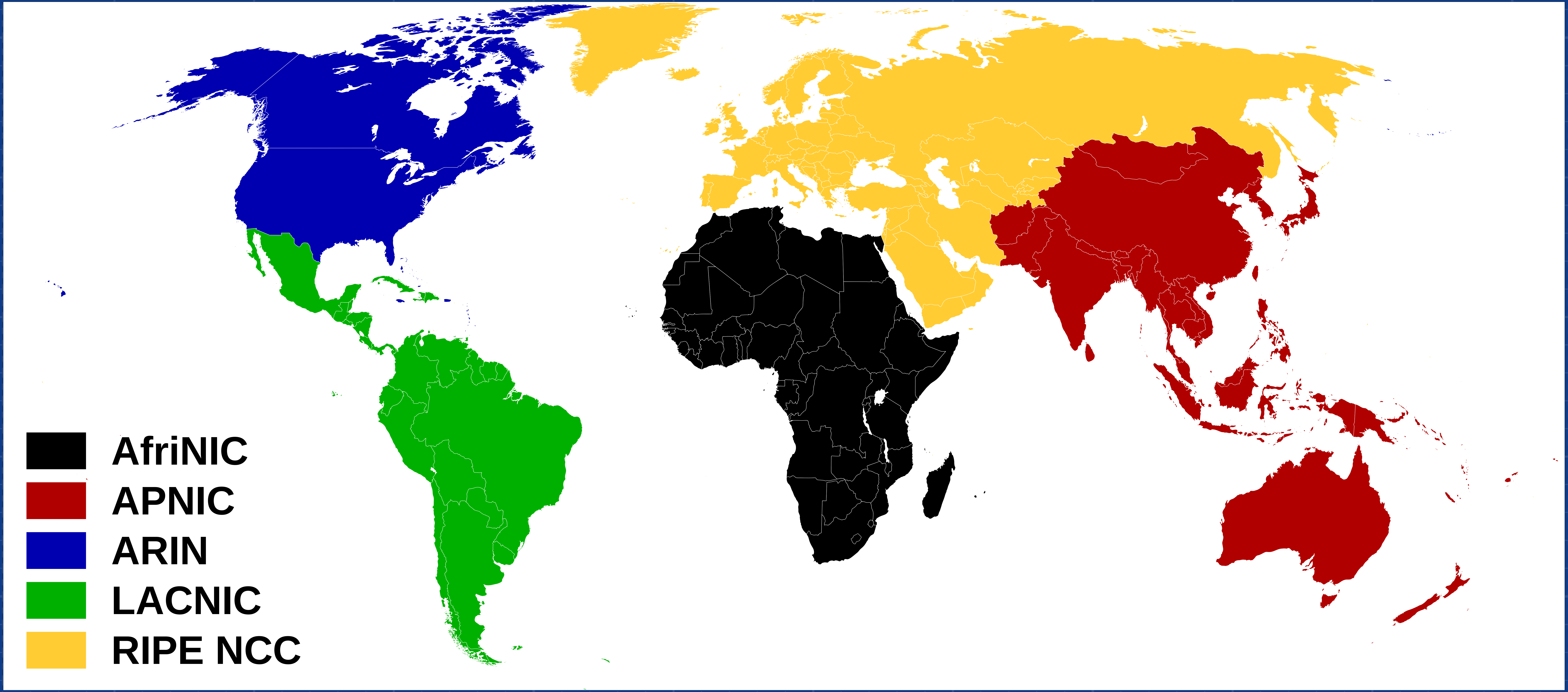
nlnetlabs.nl/projects/rpki/rpki-analytics/

RPKI

It’s all about Resources.

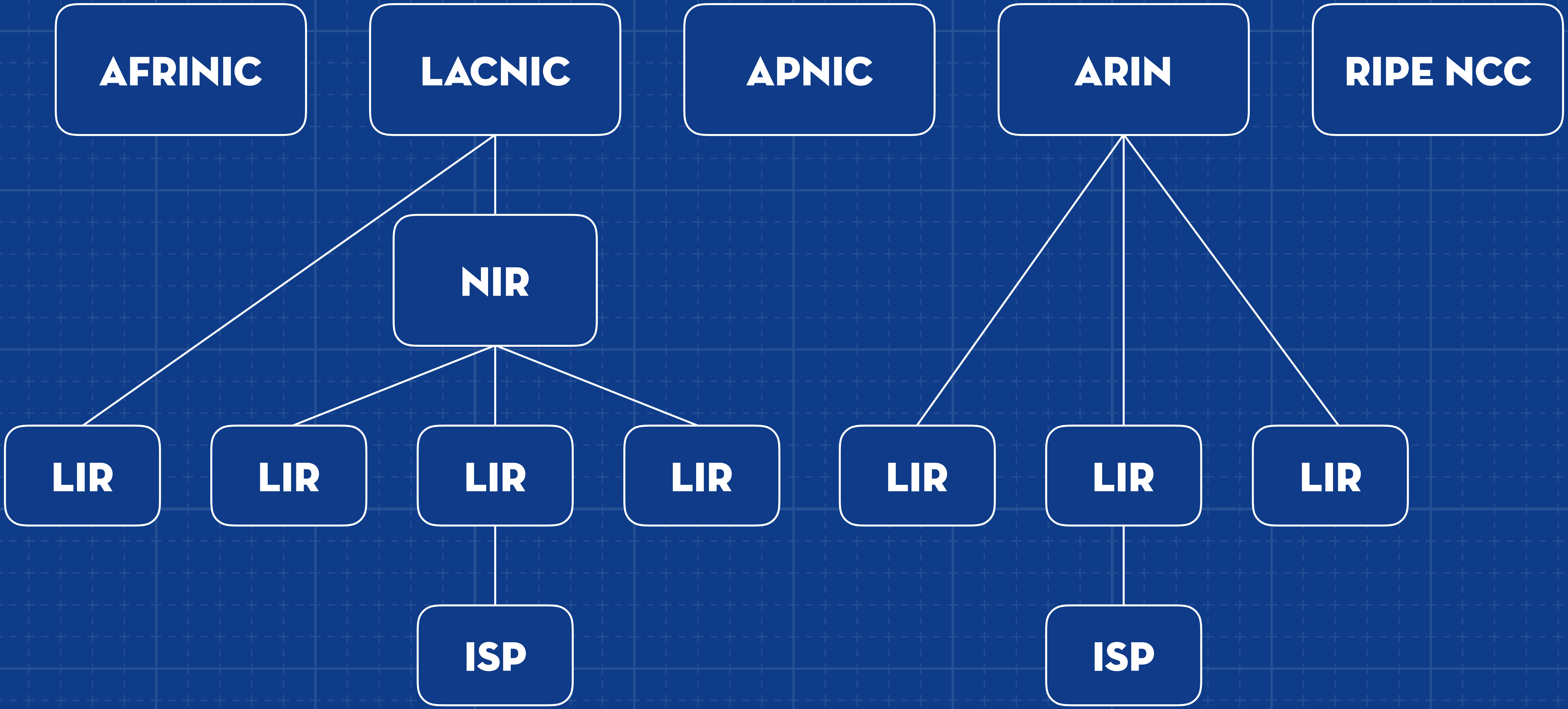
Internet Number Resources to be precise…


US
AU
KR
JP
FR
UK
CA
DE
NO
SE
FI
ES
AT
NL


AfriNIC
APNIC
ARIN
LACNIC
RIPE NCC

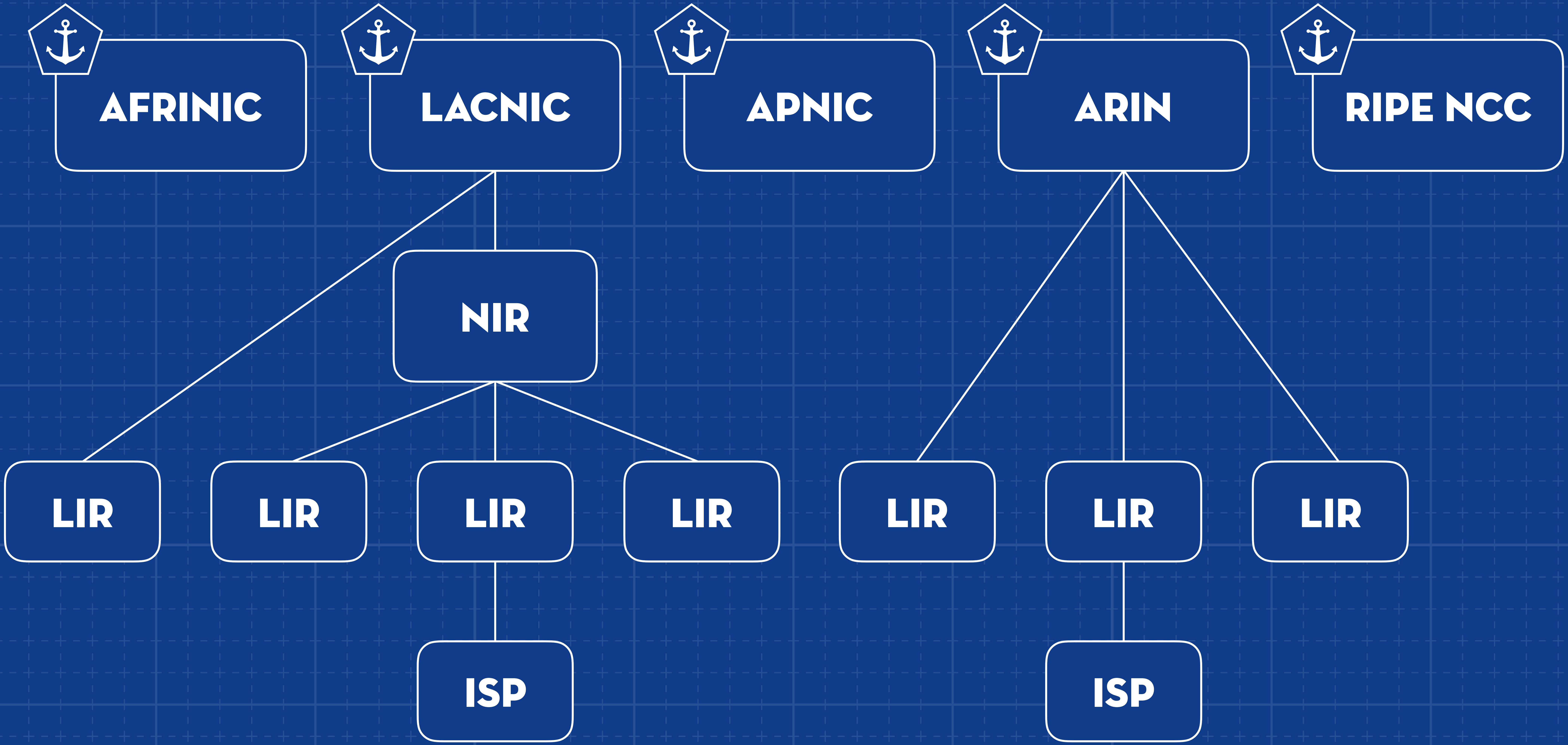
The RPKI certificate structure follows the Internet resource allocation hierarchy.

GLOBAL RESOURCE ALLOCATION

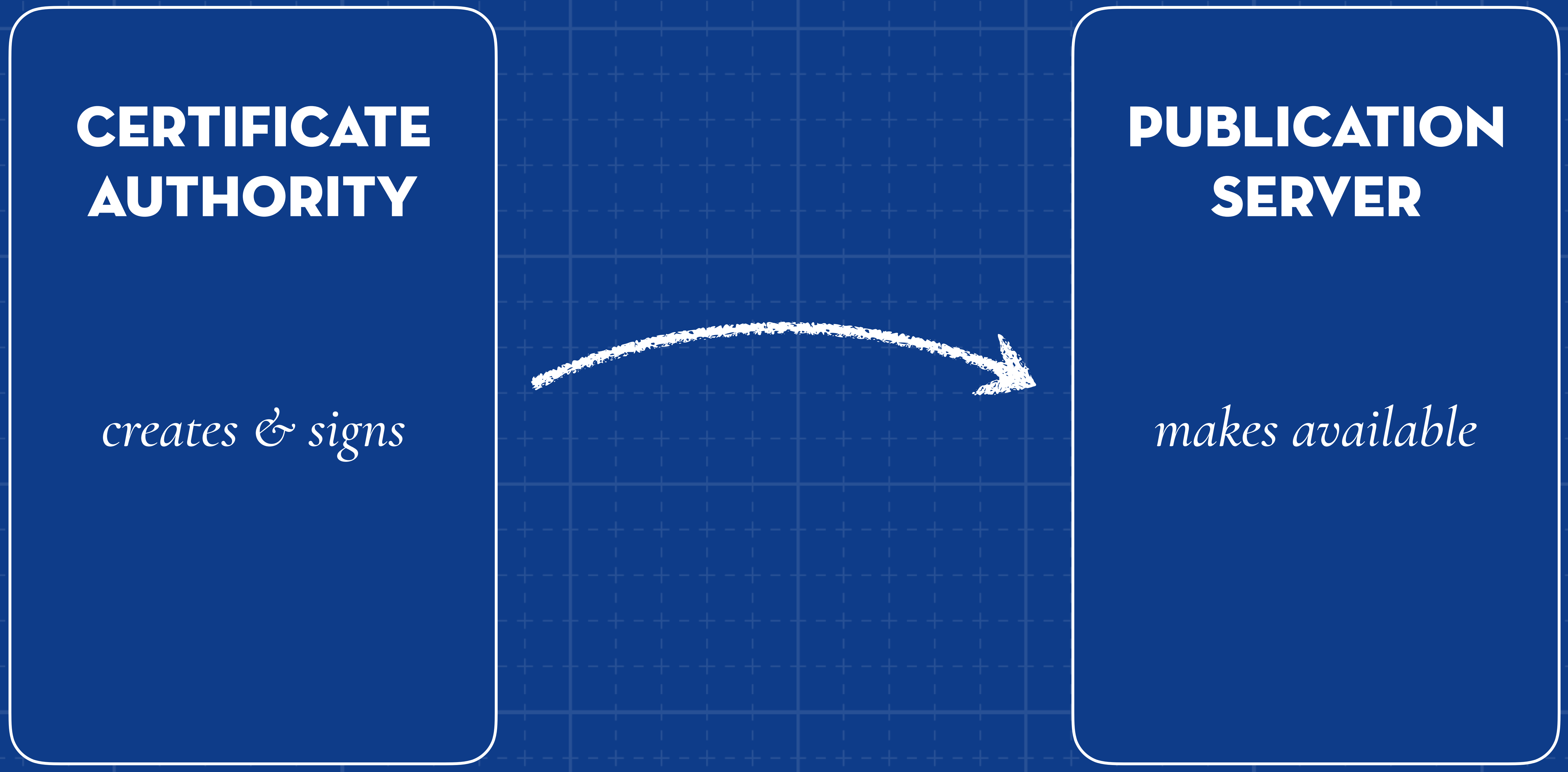


PUBLISHING RPKI DATA

RPKI CERTIFICATE STRUCTURE



SEPARATE COMPONENTS



CERTIFICATE AUTHORITY

creates & signs

PUBLICATION SERVER

makes available

ROUTE ORIGIN VALIDATION

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

ROUTE ORIGIN AUTHORISATION

- AS Number
- IP Prefix
- Maximum Prefix Length (maxLength)

Liberal usage of maxLength opens up the network to a forged origin attack. ROAs should be as precise as possible.

ROV: THREE POSSIBLE OUTCOMES

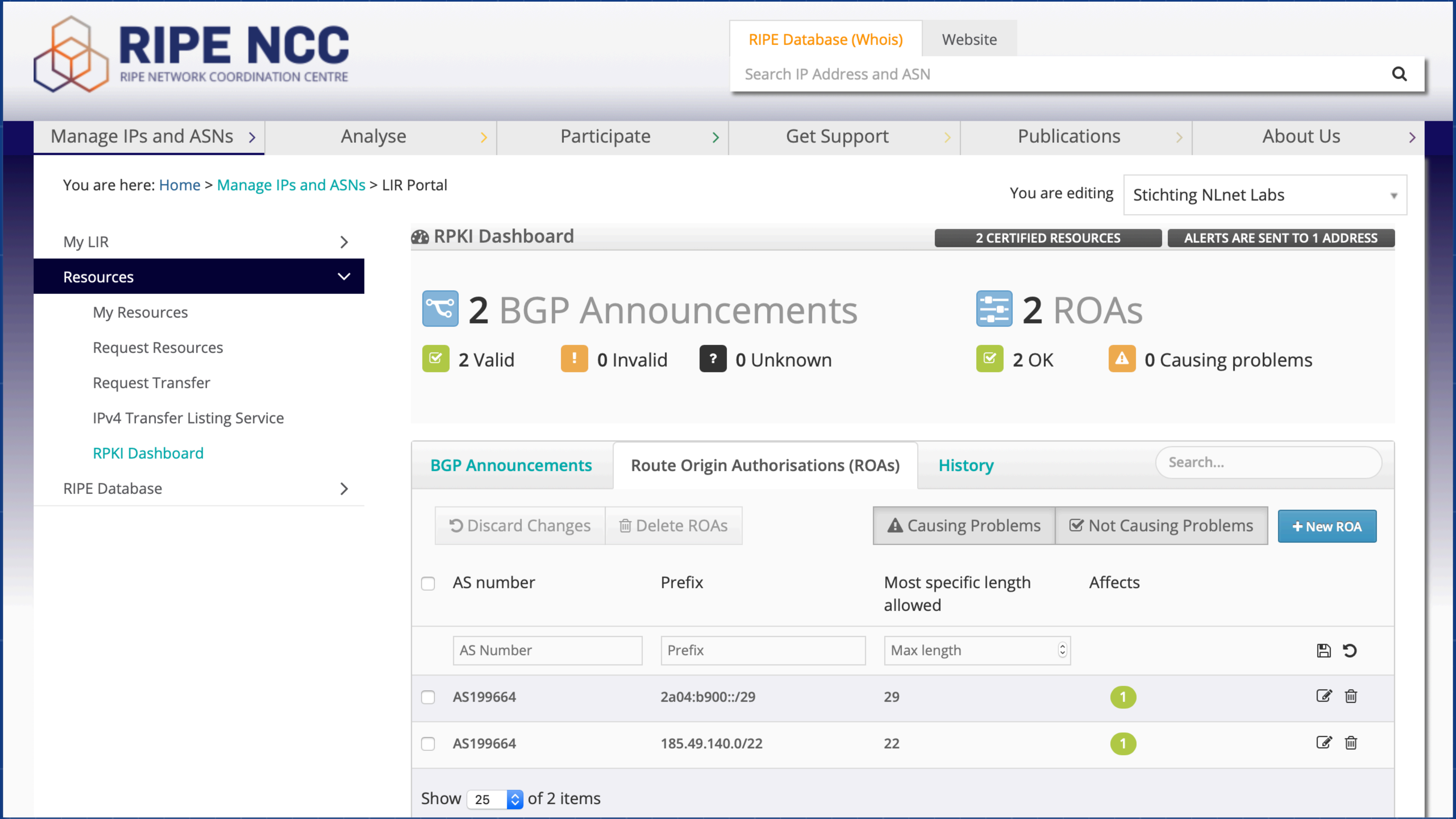
- **Valid**
  - The route announcement is covered by at least one Validated ROA Payload
- **Invalid**
  - The prefix is announced from an unauthorised AS, or the announcement is more specific than is allowed by the maxLength set in a VRP that matches the prefix and AS.
- **NotFound**

ORIGIN VS. PATH VALIDATION

- Route Origin Validation (ROV) 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 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

- 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

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

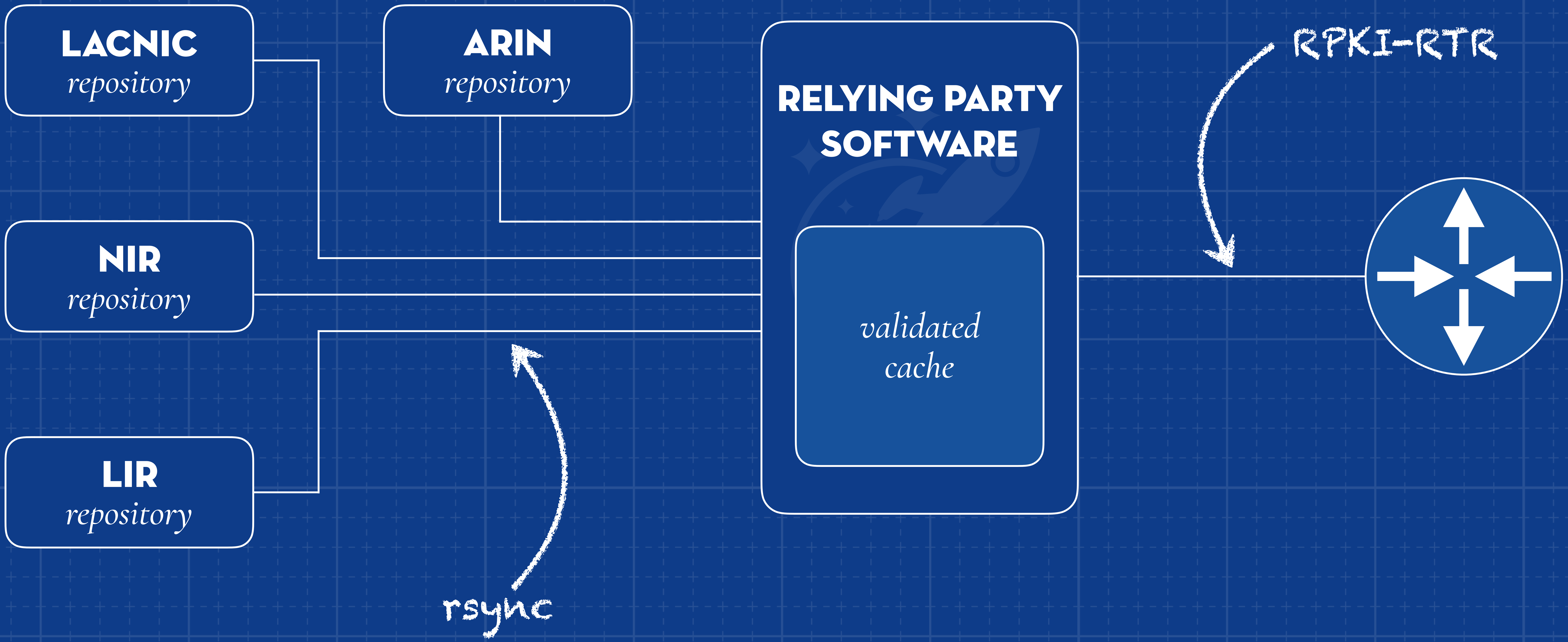
WHAT IF IT BREAKS?

- 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

USING RPKI DATA

RPKI VALIDATION



LACNIC *repository*

ARIN *repository*

NIR *repository*

LIR *repository*

RELYING PARTY SOFTWARE

validated cache

For ROV to succeed in its objective, operators should ultimately drop all BGP announcements that are marked as Invalid.

FURTHER READING

RPKI DOCUMENTATION PROJECT

https://rpki.readthedocs.io

nlnetlabs.nl/rpki

nlnetlabs.nl/mailman/listinfo/rpki

@ rpki-team@nlnetlabs.nl

@nlnetlabs

NLNETLABS