TRUST IN RPKI

UNDERSTANDING THE MOVING PARTS IN RESOURCE PUBLIC KEY INFRASTRUCTURE

ALEX BAND

NLNETLABS

NLNET LABS?

Purveyors of fine
open source software
since 1999

NSD

unbound

RPKI
QUICK START

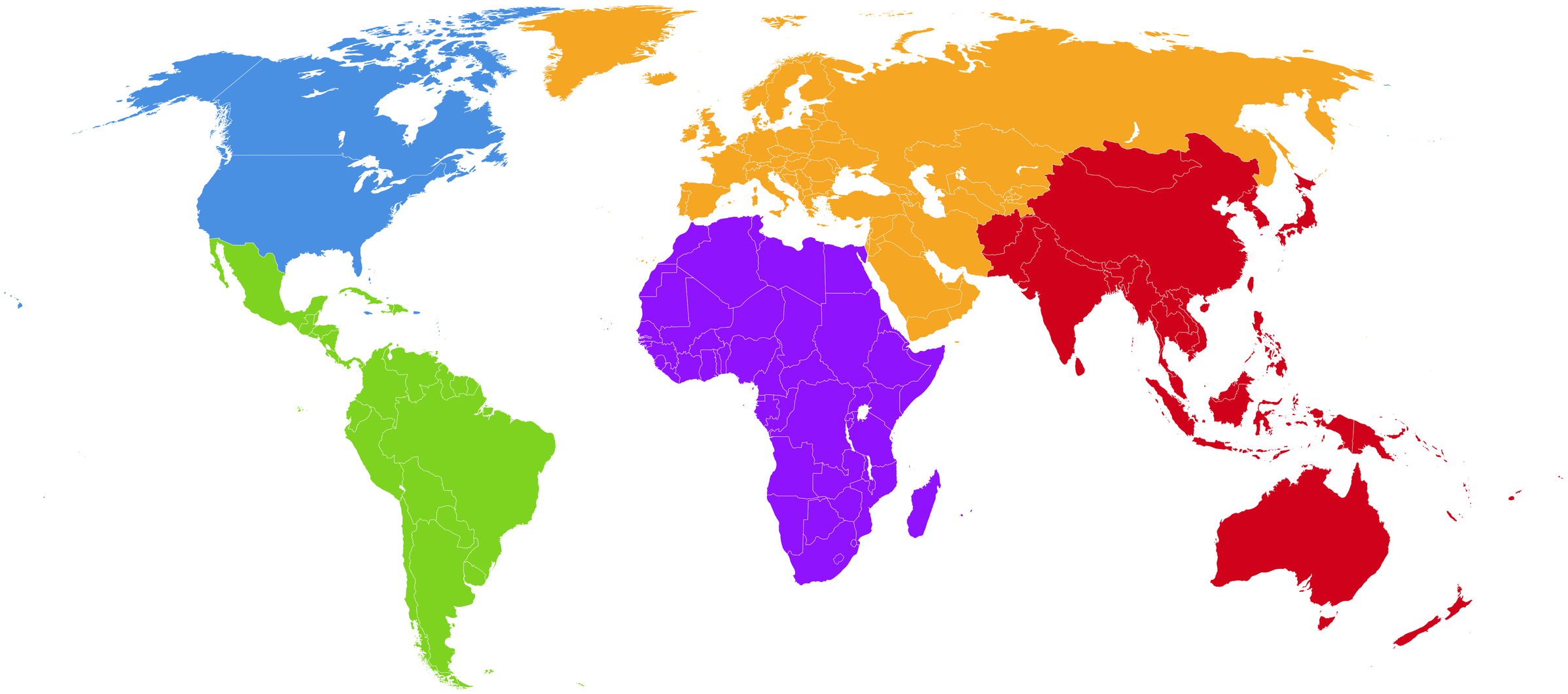
RESOURCE CERTIFICATION

"A security framework that proves the association between specific IP address blocks or AS numbers and the custodians of those Internet number resources"

— APNIC

X.509 PKI TRUST CONSIDERATIONS

- X.509 certificates are typically used for authenticating an individual or, for example, a website.
- However, in RPKI certificates do **not** include identity information
  - Their only purpose is to transfer the right to use Internet number resources.
- RPKI relies on just **five** trust anchors, run by the Regional Internet Registries
  - Well established, openly governed, not-for-profit organisations



ARIN LACNIC AFRINIC RIPE NCC APNIC

RPKI USE CASES

- **Resource** Public Key Infrastructure (RFC 6480 - 6493)
- Currently aimed at making Internet routing more secure
  - Provide Route Origin Validation (ROV) now
    - Stepping stone to Autonomous system provider authorisation (ASPA)
    - Future towards Path Validation, BGPSec (?)
- Resource Tagged Attestations (RTA) & Resource Signed Checklist (RSC) emerging
  - Think BYOIP, resource transfers...

THE MOVING PARTS

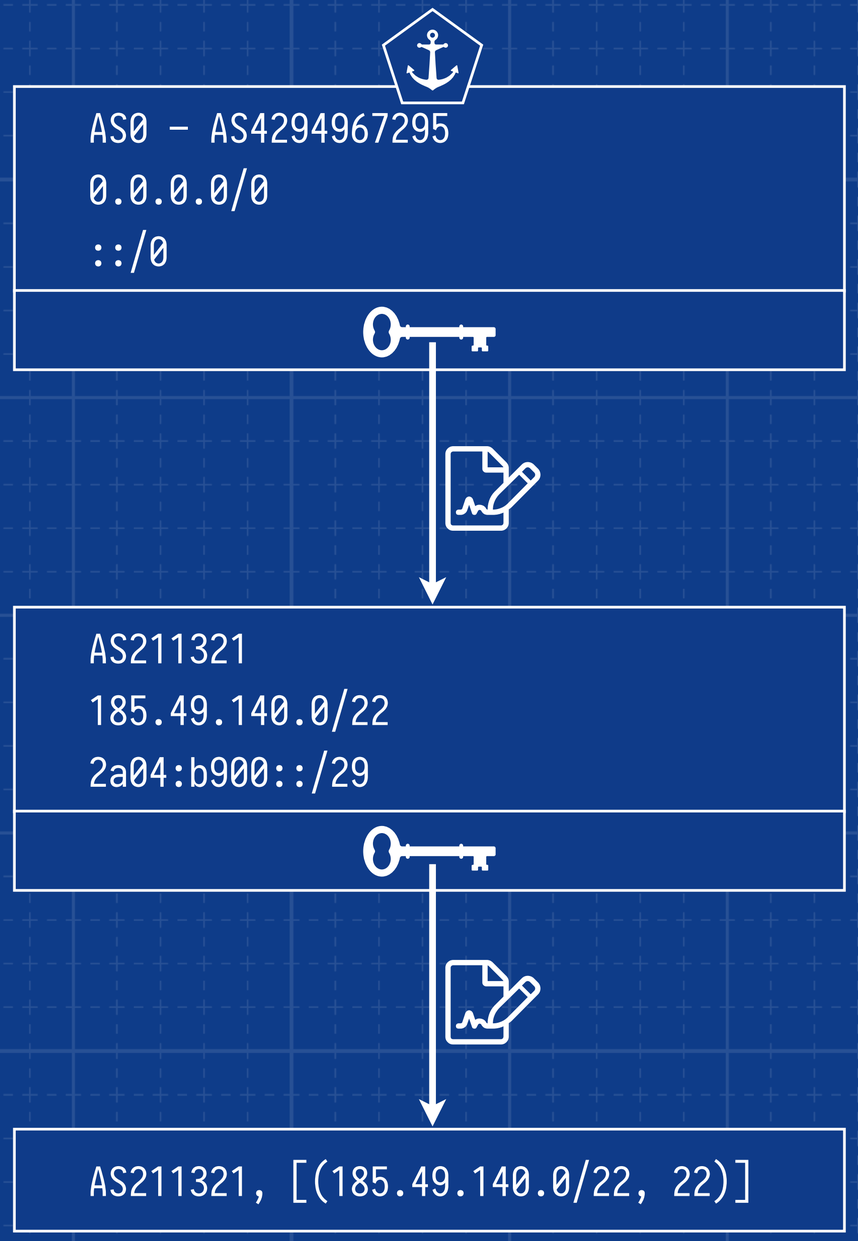
ROUTE ORIGIN VALIDATION

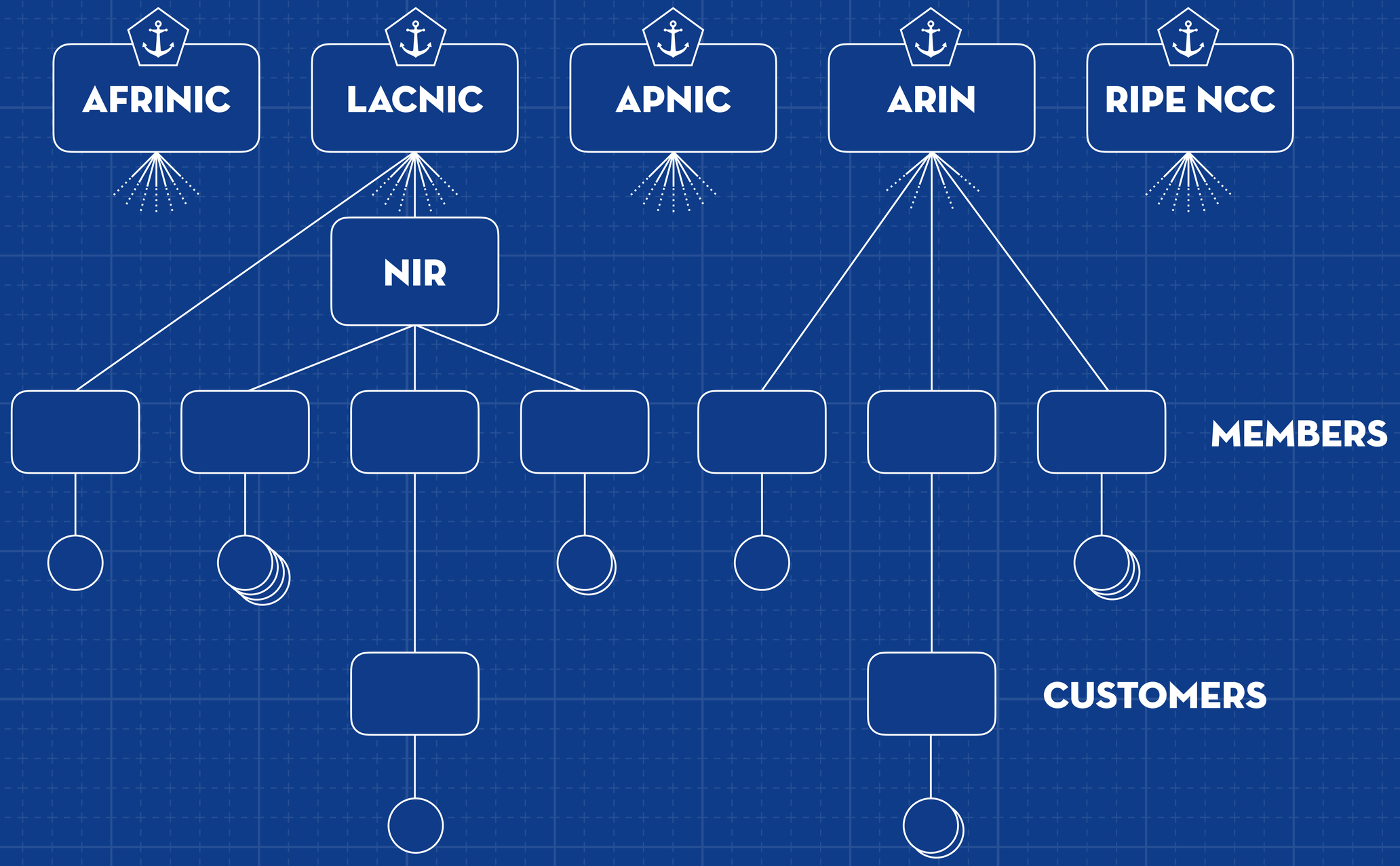
- Organisation holds certificate containing all Internet Resources
- Uses it to make authoritative statements about intended BGP routing
  - Signed objects called Route Origin Attestation (ROAs)
- Other operators — “Relying Parties” — download and verify ROAs
  - Make routing decisions based on the outcome;
  - *Valid*, *Invalid* or *NotFound*

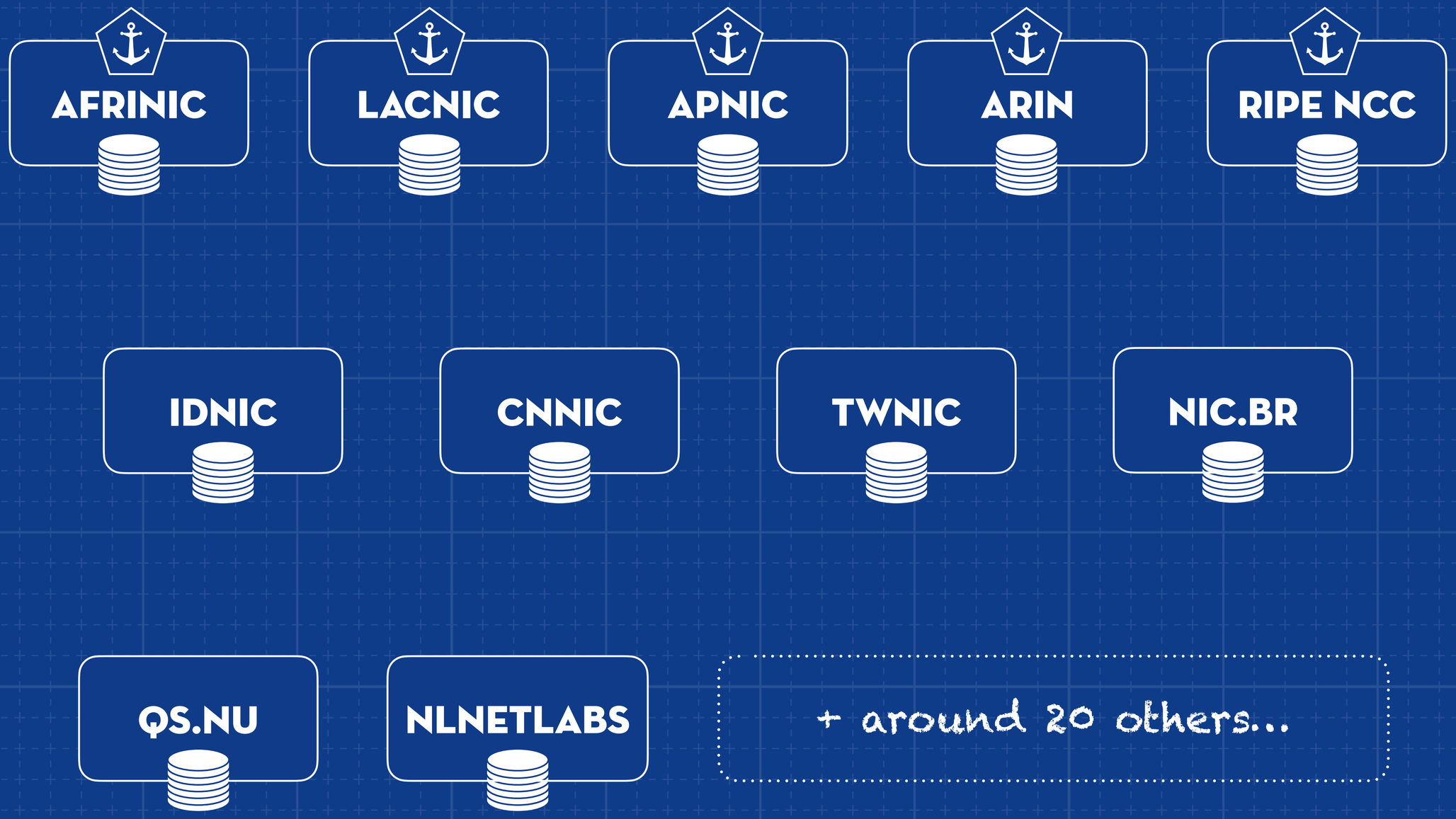
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

NLNETLABS

```
route:    185.49.140.0/22
origin:   AS199664
more:     stuff
```




AFRINIC
LACNIC
APNIC
ARIN
RIPE NCC
NIR
MEMBERS
CUSTOMERS


AFRINIC
LACNIC
APNIC
ARIN
RIPE NCC
IDNIC
CNNIC
TWNIC
NIC.BR
QS.NU
NLNETLABS
+ around 20 others...

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 lets you publish them yourself

HOSTED RPKI

- All five RIR have been offering Hosted RPKI since 2011
- Request certificate and issue ROAs through web portal or API
- Implementations vary across regions:
  - Preview of the effect a ROA is going to have on BGP routes
  - Alerting for misconfigurations and possible hijacks
  - Create matching `route:` objects in the IRR

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

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

Revoke hosted CA

Important

Once your hosted CA (Certificate Authority) will be revoked, **it cannot be restored**, and **all of your ROAs will be deleted**.

Please note that if you want to keep using RPKI, you will need to initialise a new hosted or non-hosted CA. We recommend that you keep a copy of your ROAs to be able to recreate them later.

When would you revoke a CA?

- You intend to switch from a hosted to a delegated CA.

Revoke CA

- [ ] **I want to revoke the hosted CA.** I understand that I need to initialise a new CA to keep using RPKI.
- [ ] **I am aware that my ROAs are going to be deleted.**
- [ ] **I am aware that alerts for conflicting announcements will no longer be sent.**
- [ ] **I have made a backup of my ROAs (if needed).**

Reg-ID

net.example

Confirm that you want to REVOKE the CA:

REVOKE

Revoke

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

WHY RUN DELEGATED RPKI?

- Manage RPKI for all your resources in a single system, because:
  - You represent multiple organisations under a single RIR
  - You have address space in multiple RIR regions
- You want to delegate RPKI management to business units or customers
- You want an API to automate ROA management and alerting
- You will be the only one in possession of the private key

CHOOSING DELEGATED RPKI

“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
  - Run a public HTTPS and rsync server yourself
  - Outsource it! (Currently offered by APNIC and NIC.br)

Krill

English

Certificate Authority **NLnetLabs**

ROAs | Parents | Repository

Search for ASN, prefix, state...

Download CSV

Show BGP info

ASN	Prefix	State
1133	2001:7fc::/47-47	NOT SEEN
1133	151.216.0.0/23-23	NOT SEEN
8587	2a04:b900::/29-29	SEEN 1
8587	185.49.140.0/22-22	SEEN 1
14618	2a04:b902::/32-32	NOT SEEN
14618	151.216.0.0/23-23	NOT SEEN
14618	185.49.143.0/24-24	NOT SEEN
16509	2001:7fc::/47-47	SEEN 1

Authorizes 1 announcements

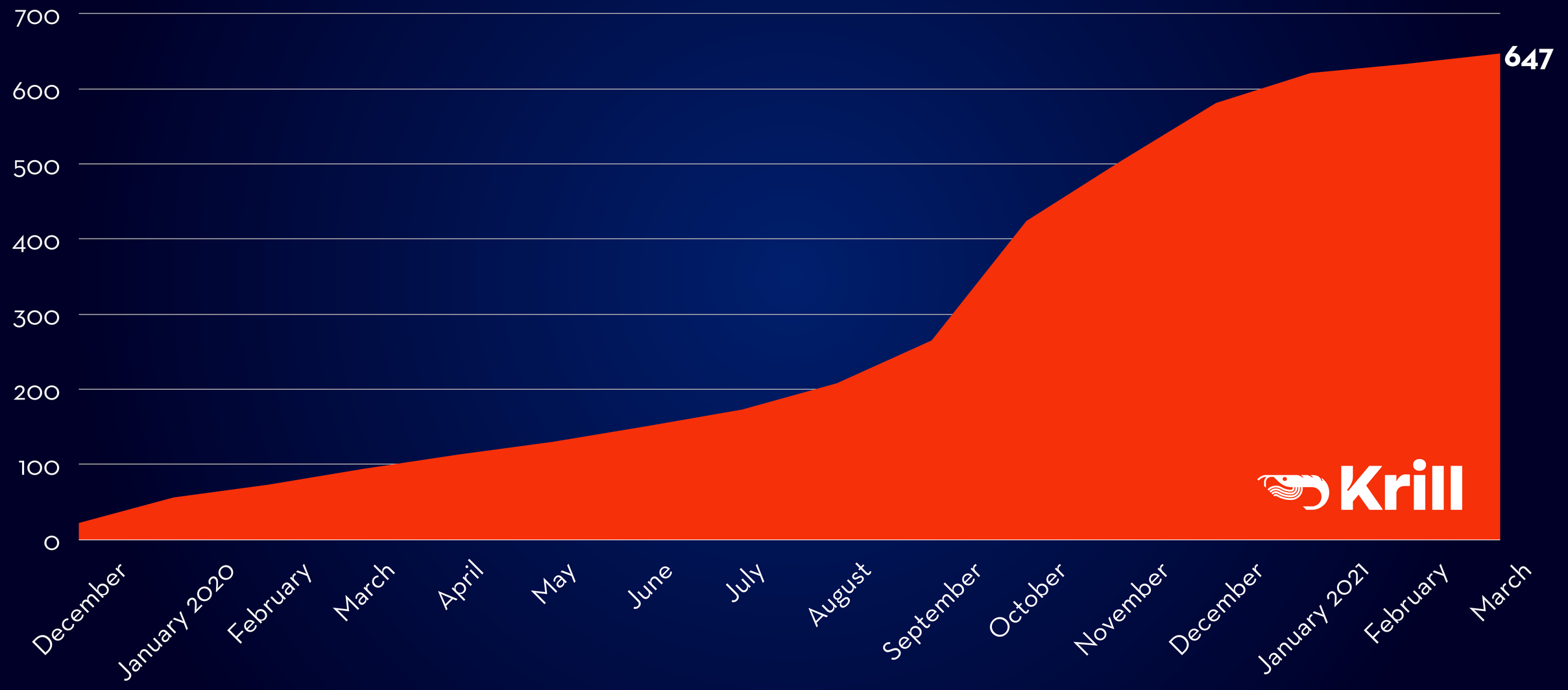
ASN	Prefix
16509	2001:7fc::/47

Disallows 0 announcements

ASN	Prefix
No data	

asn	
v4	151.216.0.0/23 185.49.140.0/22
v6	2001:7fc::/47 2a04:b900::/29

ORGANISATIONS RUNNING DELEGATED RPKI WITH KRILL



SO, DO YOU CHOOSE HOSTED OR DELEGATED?

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

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

YOU MAKE A DIFFERENCE

- Dropping RPKI Invalid routes has gained significant momentum in the last year

Telia Carrier, Cogent, GTT, NTT,
Cloudflare, Hurricane Electric, Netflix,
Scaleway, Wikimedia Foundation, TATA,
PCCW, AT&T and many more…

source: rpki.exposed

NLNETLABS

nlnetlabs.nl/rpki

rpki.readthedocs.io

github.com/nlnetlabs

rpki@lists.nlnetlabs.nl

@routinator3000

rpki on discord 68 online