NEW ADVENTURES IN

RPKI

JAAP AKKERHUIS

NLNETLABS

ROUTING SECURITY

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

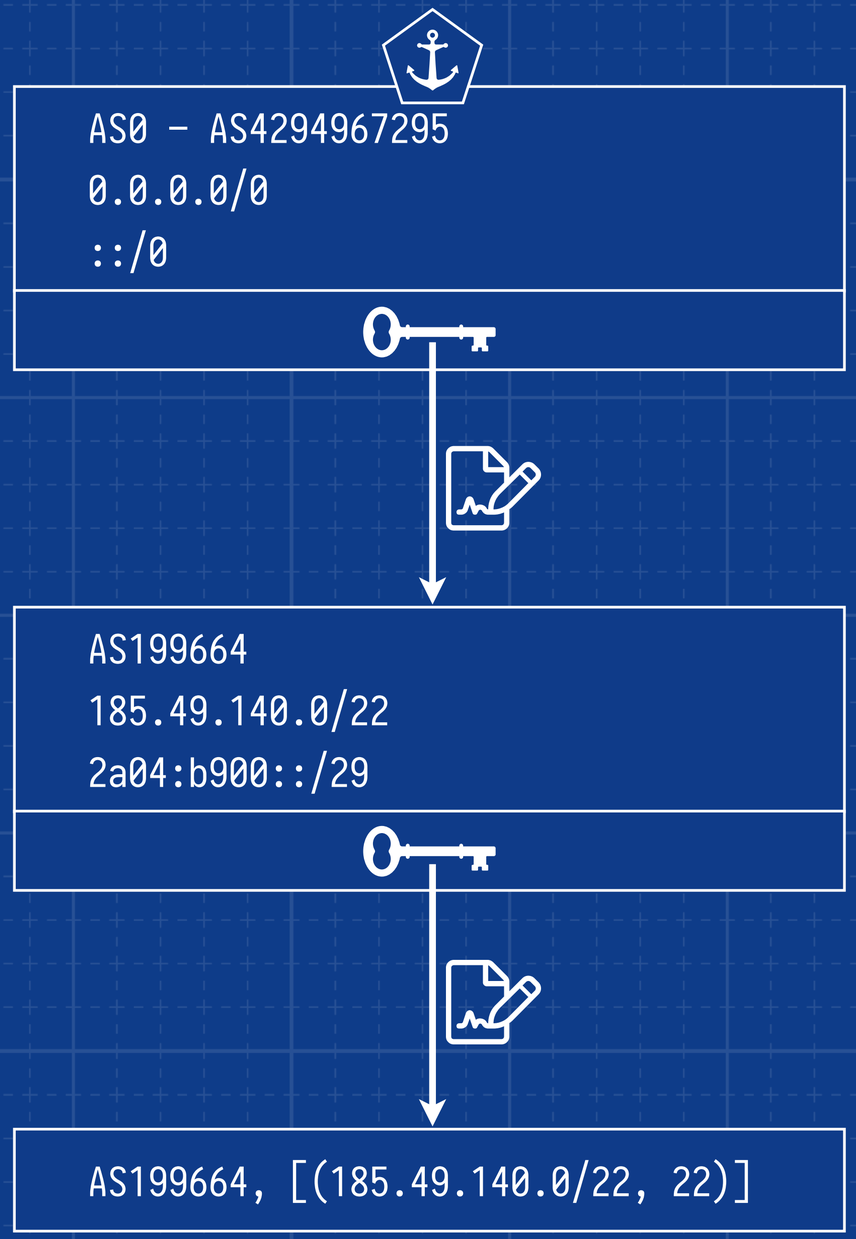
- Organisation holds certificate containing all Internet Resources
- Uses it to make authoritative statements about intended BGP routing
  - Signed objects called Route Origin Attestation (ROAs)
- Other operators — “Relying Parties” — download and verify ROAs
  - Make routing decisions based on the outcome;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

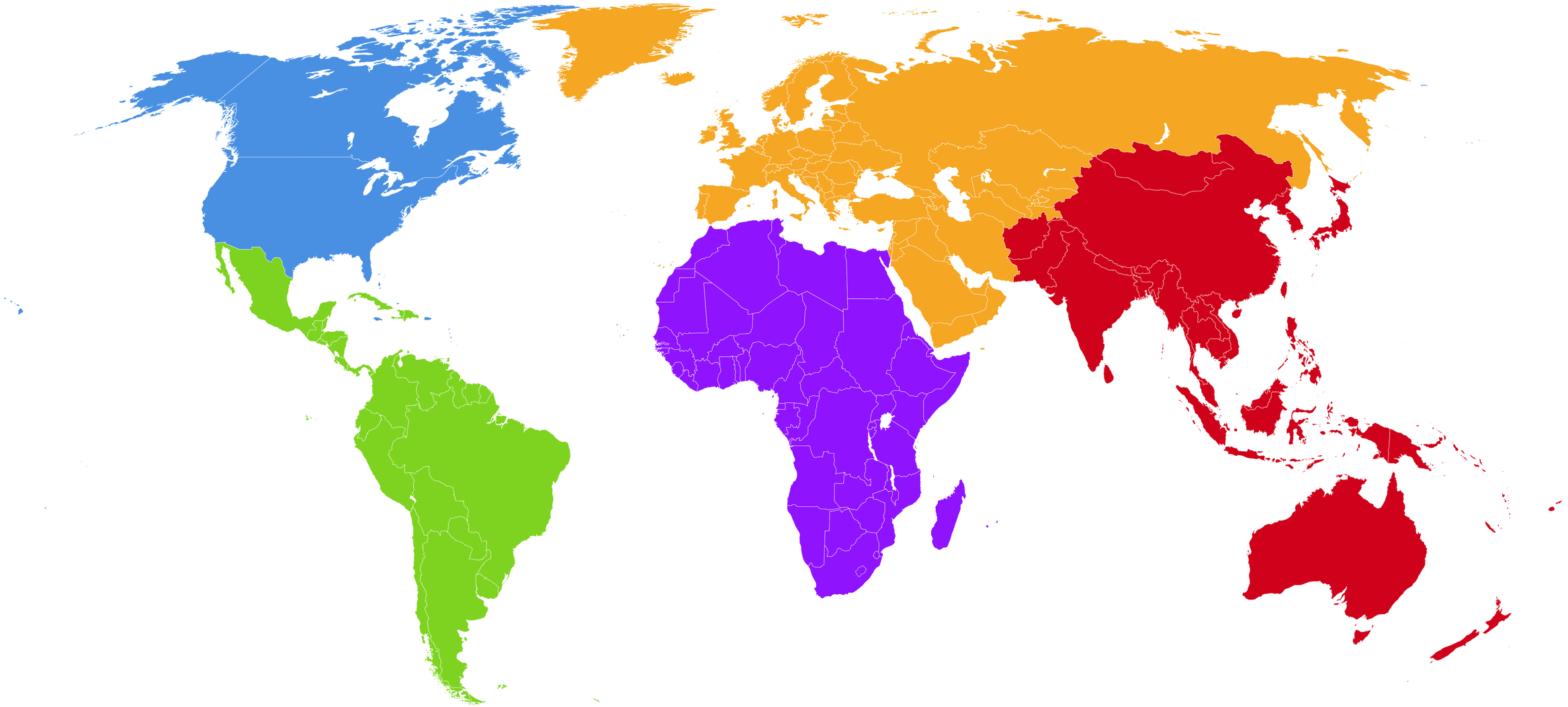
“Is this BGP route origination authorised by the legitimate holder of the IP space?”

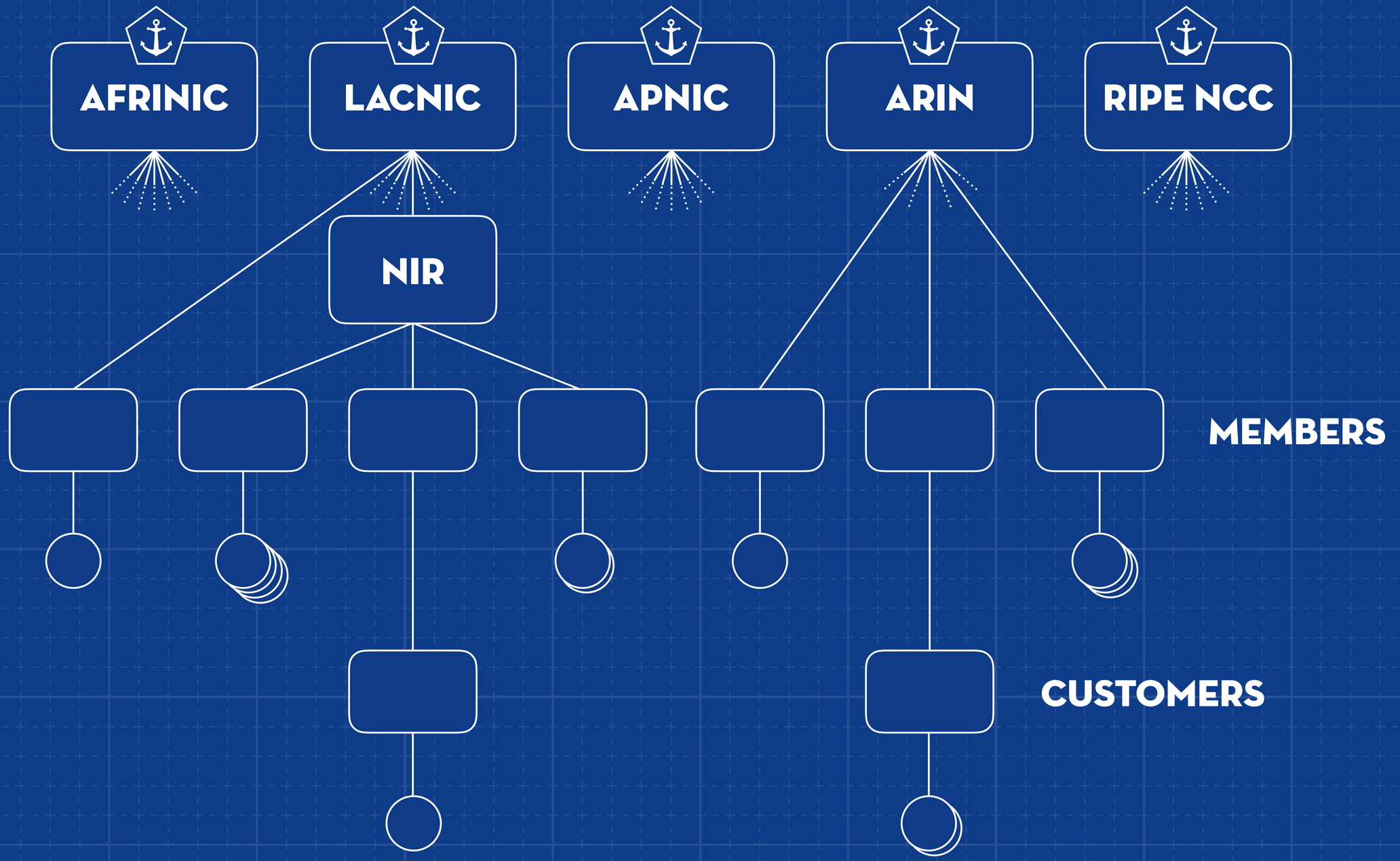
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

NLNETLABS

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




ARIN
LACNIC
AFRINIC
RIPE NCC
APNIC


AFRINIC
LACNIC
APNIC
ARIN
RIPE NCC
NIR
MEMBERS
CUSTOMERS

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)

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

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

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

FUNDING?


DigitalOcean


nic.br


JUNIPER
NETWORKS


RIPE NCC
Community Projects Fund


CISCO


moz://a


Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie


NOKIA

Krill

KRILL ROADMAP

✔ Event sourcing architecture with API, CLI and UI

✔ Creation of RPKI objects

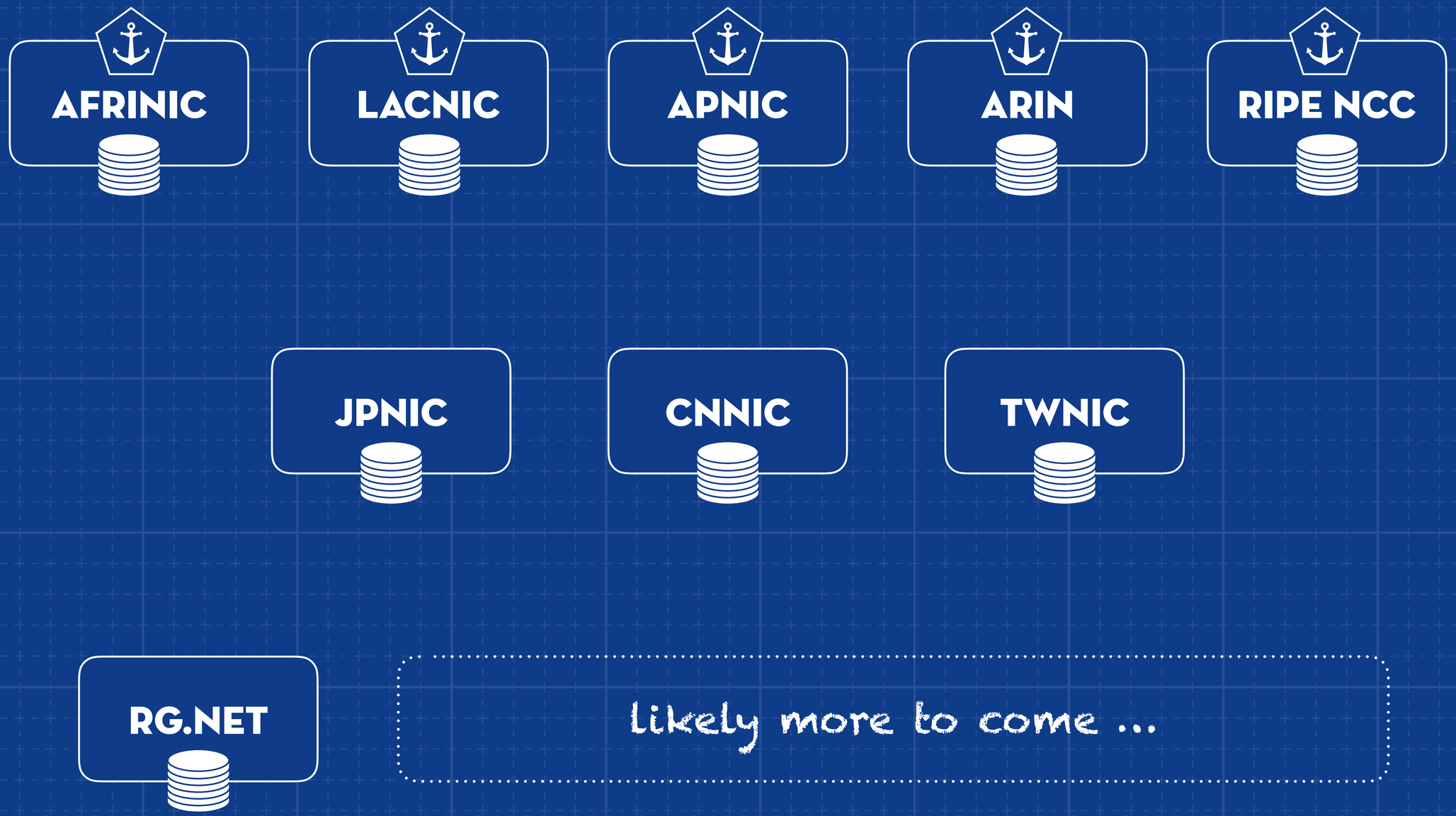
✔ RFC compliant publication server

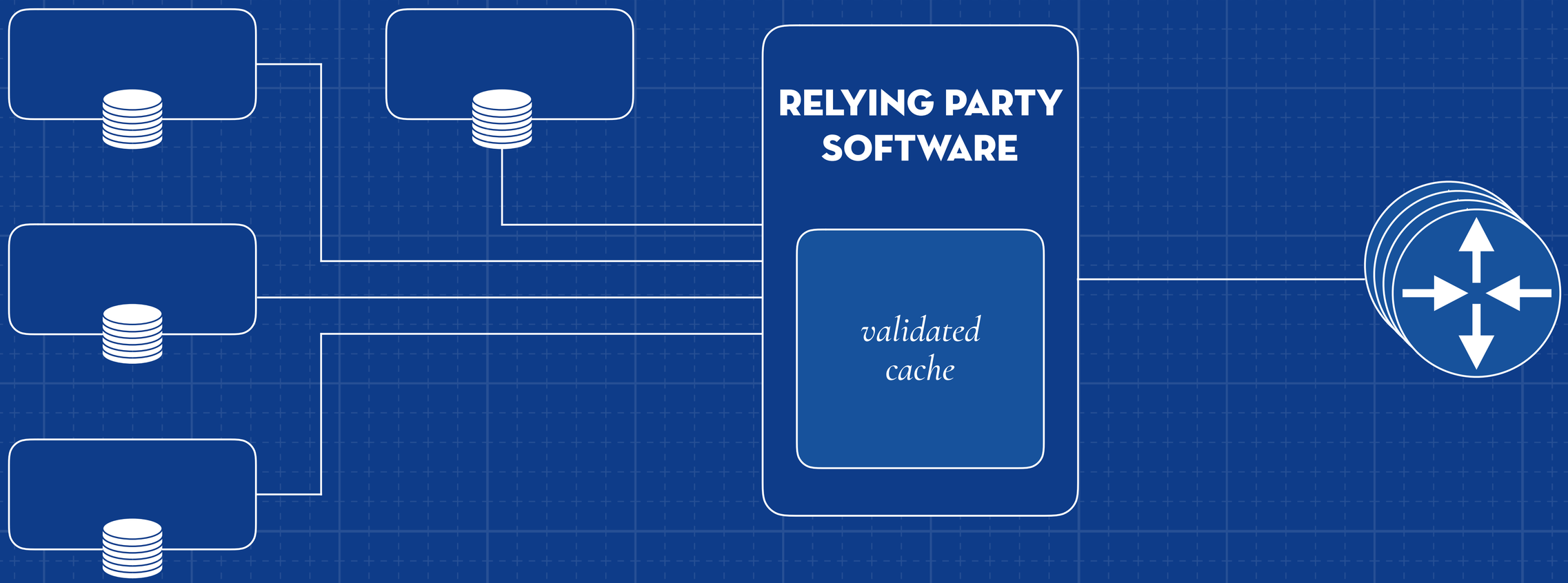
✔ Embedded Trust Anchor for testing

- Operate under remote parent
- ROA suggestions, Multi-master support, HSM support (if desired)

Krill will launch in production at NIC.br in December 2019


ROUTINATOR


AFRINIC
LACNIC
APNIC
ARIN
RIPE NCC
JPNIC
CNNIC
TWNIC
RG.NET
likely more to come ...


RELYING PARTY SOFTWARE
validated cache

RPKI DEPLOYMENT

- Healthy ecosystem with seven different RPKI Validator implementations
- NIC.br will launch with Krill in production in December 2019
- Strict validation happening on all Cloudflare PoPs
- AT&T, Nordunet, KPN and Telia reject invalids on all EBGP sessions
- Route server filtering at YYCIX, INEX, AMS-IX, DE-CIX, France-IX, Netnod

RPKI DOCUMENTATION AND FAQ

rpki.readthedocs.io

nlnetlabs.nl/rpki

rpki.readthedocs.io

github.com/nlnetlabs

rpki@nlnetlabs.nl

@routinator3000

NLNETLABS