HOSTED VS. DELEGATED

RPKI

ALEX BAND

NLNETLABS

NLNET LABS?

Purveyors of fine
open source software
since 1999

NSD

unbound

Krill

ROUTINATOR

RPKI

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

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 will be the only one in possession of the private key

Krill

Free and open source

Krill
English
ROAs
Parents
Repository
Search for ASN, prefix, state...
Download CSV
Show BGP info

Certificate Authority **NLnetLabs**

	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

CORE FUNCTIONALITY

- ✔ Seamlessly operate under multiple parent CAs
- ✔ Sub-delegate resources to other units
- ✔ Act as a parent CA for customers and subdivisions
- ✔ Manage Route Origin Authorisations (ROAs)
- ✔ Stand-alone publication server
- ✔ Allow remote publication

ESSENTIALS

- ✔ Installation from Binary Packages, Docker or source
- ✔ User Interface, Command Line Interface and a REST-like HTTPS API
- ✔ Prometheus monitoring and alerting
- ✔ Multi-user support based on OpenID Connect
    - Granular authentication and authorisation (read-only vs. admin)
- ✔ Audit log

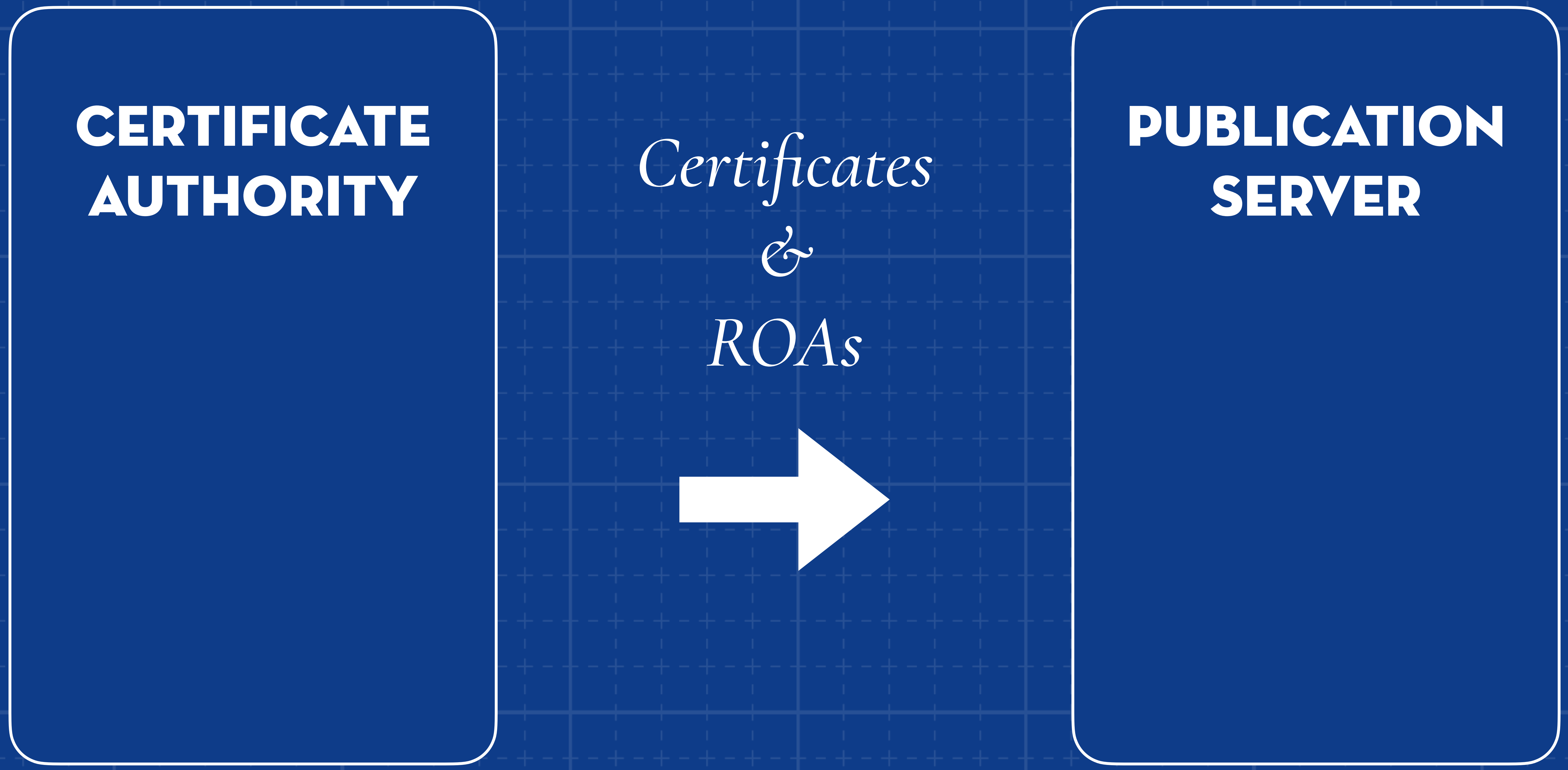
USER INTERFACE

- ✔ Multi-language support
- ✔ Parent CA and Publication Server configuration
- ✔ ROA suggestions and alerting based on BGP route collectors
  - Invalid announcements (incorrect ASN or prefix length), too permissive ROAs, redundant ROAs, etc.

2021 ROADMAP

- BGP listener: manage ROAs based on your own router's view
- Hardware Security Module (HSM) support: PKCS#11 and KMIP
- User interface refinements: audit log, bulk editing, etc.
- Your favourite thing?

SEPARATE COMPONENTS



CERTIFICATE AUTHORITY

Certificates

&

ROAs

PUBLICATION SERVER

RPKI PUBLICATION

- Publish yourself:
  - Using your own HTTPS + rsyncd server
  - Let customers / business units publish on yours
- Publish with a third party:
  - Currently, APNIC and NIC.br offer RPKI publication as a service
  - Other RIRs and cloud providers have this on their roadmap

USE APNIC FOR PUBLICATION

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?

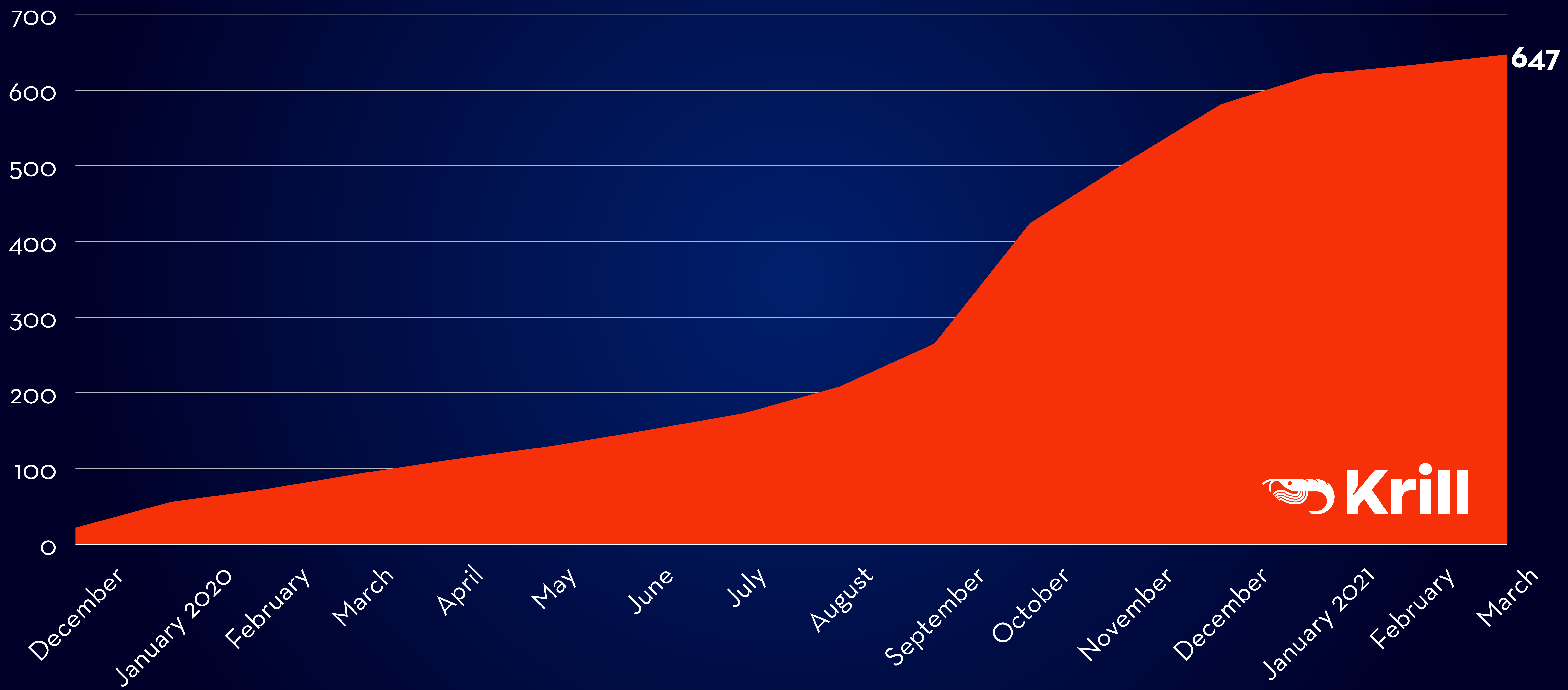
- Is Delegated RPKI more secure? No!
  - The RIR giveth, the RIR taketh away;
    they can always revoke your certificate anyway
- Is Delegated RPKI more convenient? It depends...
- How many prefixes do you manage (across the globe) and how often do they change?
- Is the pain of running your own software 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

ORGANISATIONS RUNNING DELEGATED RPKI WITH KRILL



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

VIBRANT ECOSYSTEM

- rpki.readthedocs.io – Documentation and FAQ
- JDR – A tool to help you explore, inspect and troubleshoot anything RPKI
- rpki@lists.nlnetlabs.nl – Mailing list with 500+ subscribers

@krillrpki & @routinator3000

RPKI Community on Discord