



GTER48 - São Paulo - Brazil

Krill

by NLnet Labs

NLNET LABS?



*Makers of fine
open source software
since 1999*





NSD



unbound



BGP?

RPKI!

10+ years
experience

RPKI!



[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 v

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

<input type="checkbox"/>	AS number	Prefix	Most specific length allowed	Affects	
<input type="checkbox"/>	AS Number	Prefix	Max length		
<input type="checkbox"/>	AS199664	2a04:b900::/29	29	1	
<input type="checkbox"/>	AS199664	185.49.140.0/22	22	1	

Show 25 of 2 items

CERTIFICATION AUTHORITY FOR DELEGATED RPKI



ROUTING SECURITY





By Eduard Kovacs on August 07, 2018

Share Tweet Recommend 17 RSS

Several payment processing companies in the United States were targeted recently in BGP hijacking attacks whose goal was to redirect users to malicious websites, Oracle reported last week.

The Border Gateway Protocol (BGP) controls the route of data across the Web. BGP hijacking also known as prefix or route hijacking, is carried out by taking over IP address groups by corrupting the routing tables that store the path to a network.

In the past months, Oracle, which gained deep visibility into Web traffic after acquiring Dyn in 2016, has observed several instances of malicious actors trying to force users to their websites by targeting authoritative DNS servers in BGP hijacking attacks.

The attackers used rogue DNS servers to return forged DNS responses to users trying to access a certain website. They maximized the duration of an attack with long time-to-live (TTL) values in those forged responses so that DNS servers would hold the fake DNS entries in their cache for an extended period.

Turkey Hijacking IP addresses for popular Global DNS providers

Posted by Andree Toonk - March 29, 2014 - Hijack, News and Updates - 26 Comments

At BGPmon we see numerous BGP hijacks every single day, some are interesting because of size and scale of the hijack or as we've seen today because of the targeted hijacked prefixe all started last weekend when the Turkish president ordered the censorship of twitter.com. started with a block of twitter by returning false twitter IP addresses by Turk Telekom DNS servers. Soon users in Turkey discovered that changing DNS providers to Google DNS or OpenDNS was a good method of bypassing the censorship. But as of around 9am UTC today (Saturday March 29) this changed when Turk Telekom started to hijack the IP address for popular free and open DNS providers such as Google's 8.8.8.8, OpenDNS' 208.67.222.222 and 4.2.2.3's 4.2.2.2. BGP hijack Using the Turk Telekom looking glass we can see that AS9121 (Turk Telekom) has specific /32 routes for these IP addresses. Since this is the most specific route possible for an IPv4 address, this route will always be selected and the result is that traffic to this IP address is sent to this new bogus route.

BORDER GATEWAY PROTOCOL ATTACK —

Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency

Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.

DAN GOODIN - 4/24/2018, 9:00 PM



Amazon

Amazon lost control of a small number of its cloud services IP addresses for two hours on Tuesday morning when hackers exploited a known Internet-protocol weakness that let them to redirect traffic to rogue destinations. By subverting Amazon's domain-resolution service, the attackers managed to steal cryptocurrency website MyEtherWallet.com and stole about \$150,000 in digital coins from unwitting end users. They may have targeted other Amazon customers as well.

December 18, 2017 By Pierluigi Paganini

Traffic for Google, Apple, Facebook, Microsoft and other tech giants routed through Russia, experts believe it was an intentional BGP Hijacking.

Last week a suspicious event routed traffic for major tech companies (i.e. Google, Facebook, Apple, and Microsoft) through a previously unknown Russian Internet provider. The event occurred on Wednesday, researchers who investigated it believe the traffic was intentionally hijacked.

The incident involved the Internet's Border Gateway Protocol that is used to route traffic among Internet backbones, ISPs, and other large networks.



It started with a lengthy email to the NANOG mailing list on 25 June 2018: independent security researcher Ronald Guilmette detailed the suspicious routing activities of a company called Bitcanal, whom he referred to as a "Hijack Factory." In his post, Ronald detailed some of the Portuguese company's most recent BGP hijacks and asked the question: why Bitcanal's transit providers continue to carry its BGP hijacked routes on to the global internet?

This email kicked off a discussion that led to a concerted effort to kick this bad actor, who has hijacked with impunity for many years, off the internet.



3

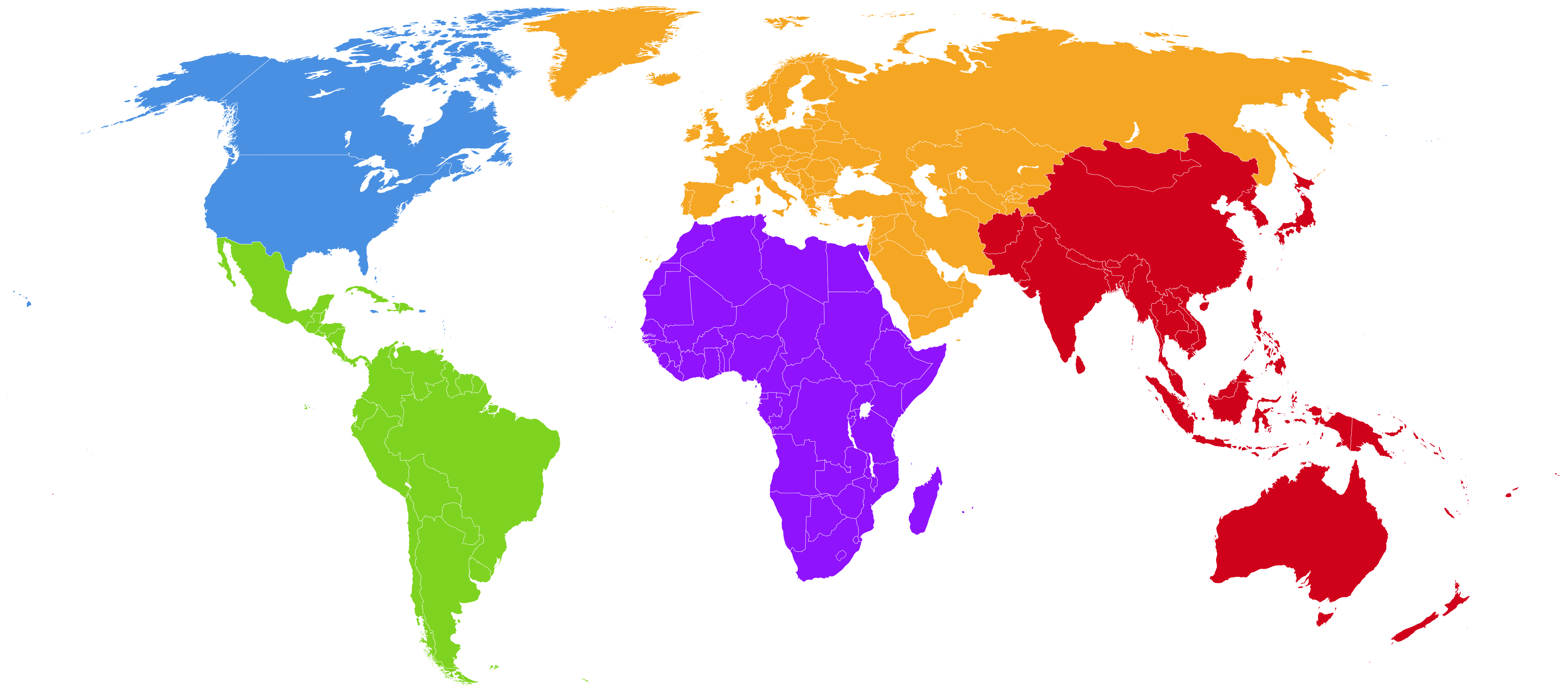
How Pakistan knocked YouTube offline (and how to make sure it never happens again)

YouTube becoming unreachable isn't the first time that Internet addresses were hijacked. But if it spurs interest in better security, it may be the last.



by Declan McCullagh

Updated: February 25, 2008 4:28 PM PST



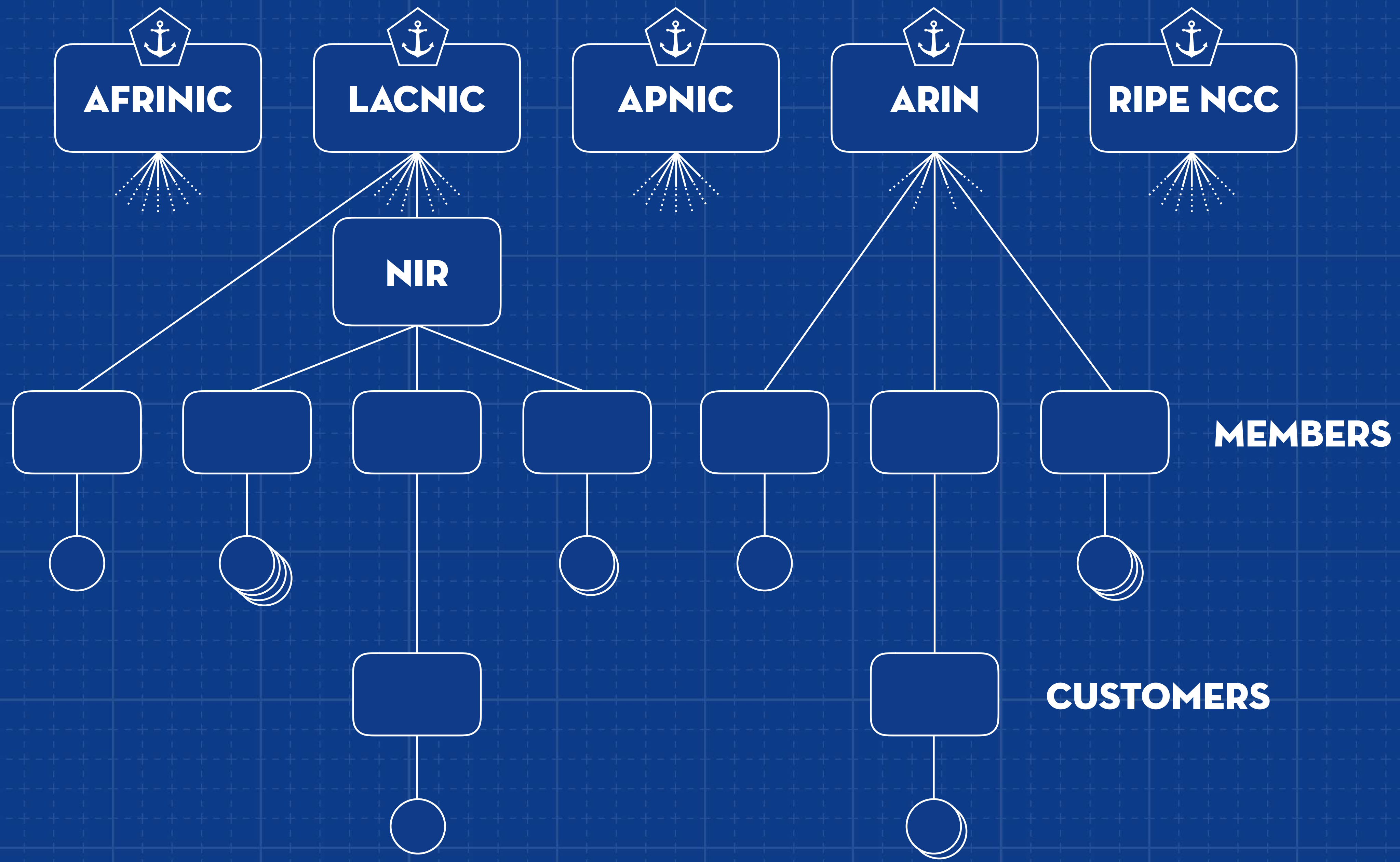
ARIN

LACNIC

AFRINIC

RIPE NCC

APNIC



SEPARATE COMPONENTS

**CERTIFICATION
AUTHORITY**

creates & signs

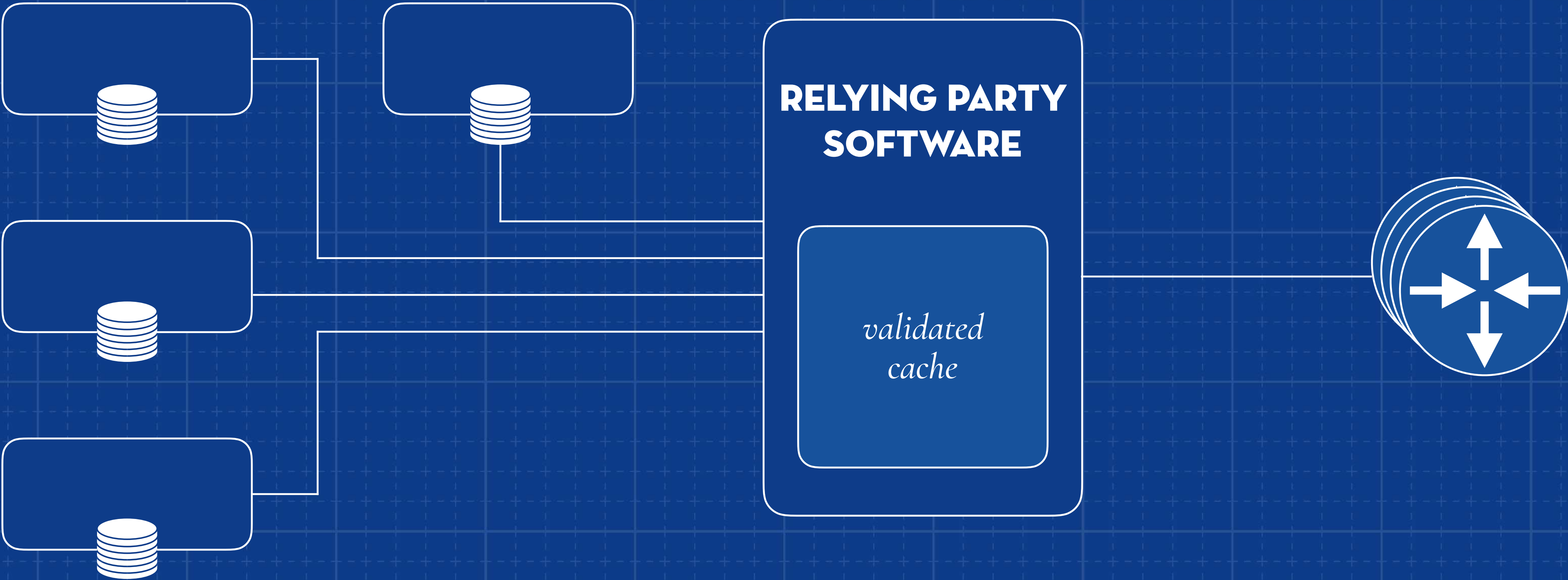


**PUBLICATION
SERVER**

makes available



More to come..



DELEGATED RPKI

- Run an RPKI Certification 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 are operationally independent from the parent
- Allows tight 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

FUNDING?

mozilla

 **DigitalOcean**

JUNIPER
NETWORKS

nic.br


CISCO



Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie



RIPE NCC
Community Projects Fund

NOKIA



**RPKI Certification Authority
and Publication Server**

KRILL CURRENT FUNCTIONALITY

- ✓ Event sourcing architecture with CLI and API
- ✓ Up: operate under multiple parent CAs
- ✓ Down: act as a parent for multiple child CAs
- ✓ Creation of ROAs
- ✓ Built-in Publication Server
- ✓ Allow remote publication

KRILL ROADMAP

- Web-based User Interface “Lagosta” – Coming soon!
 - Optional package, with multi-language support
- ROA suggestions, based on global or local view
- Packaging (Docker, *NIX Distributions)
- Monitoring (e.g. Prometheus)
- Multi-master and HSM support (if desired)

KRILL STRETCH GOALS

- Integration with IPAM Solutions
- Just-in-Time Authorisations
- Cloud Provider Marketplace offerings
- Krill-as-a-Service

LAGOSTA PREVIEW

Krill UI

localhost:8080/?#/cas/ca

Krill Certificate Authorities English

Certificate Authorities > ca

Repository




Type	Properties
Remote	Service URI: https://krill-ui-dev.do.nlnetlabs.nl/rfc8181/ca

Parents

Handle	Kind
	rfc8181

v4	10.0.0.0/8
v6	::/128

Route Authorizations

ASN	Prefix	Max Length	
8587	10.1.0.0/22	24	
199664	10.0.0.0/22		
3333	10.2.0.0/22	0	

Add ROA

SYSTEM REQUIREMENTS

HARDWARE & CONNECTIVITY

- Certificate Authority
 - Modest hardware is fine for most use cases
 - No HSM needed; keys on disk are fine, really
- Publication Server
 - Offered by NIC.br as a service
 - Publishing yourself will have all normal consequences of a public service

NLNET LABS RUNS 2 CPU / 2 GB RAM

```
top - 15:32:17 up 4 days, 59 min, 3 users, load average: 0.00, 0.00, 0.00
Tasks: 82 total, 1 running, 81 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.2 us, 0.2 sy, 0.0 ni, 99.5 id, 0.0 wa, 0.0 hi, 0.0 si, 0.2 st
MiB Mem : 1997.7 total, 858.2 free, 110.5 used, 1029.0 buff/cache
MiB Swap: 0.0 total, 0.0 free, 0.0 used. 1689.1 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1532	do-agent	20	0	706936	25308	11464	S	0.0	1.2	1:06.53	do-agent
4230	krill	20	0	831436	21820	13912	S	0.0	1.1	5:52.01	krill
20190	www-data	20	0	75016	11096	5312	S	0.0	0.5	6:29.93	nginx
1	root	20	0	170448	10264	7856	S	0.0	0.5	0:07.94	systemd
220	root	20	0	43096	9864	8336	S	0.3	0.5	3:08.91	systemd-journal
4268	root	20	0	71856	8596	6420	S	0.0	0.4	0:00.00	nginx
9854	root	20	0	16928	8436	7072	S	0.3	0.4	0:00.21	sshd
20188	www-data	20	0	72392	8344	5244	S	0.0	0.4	1:35.86	nginx
2613	root	20	0	21024	8220	7100	S	0.0	0.4	0:00.06	systemd

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?

All routes will eventually fall back to the “NotFound” state, as if RPKI were never used

WHATEVER YOU DO, 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

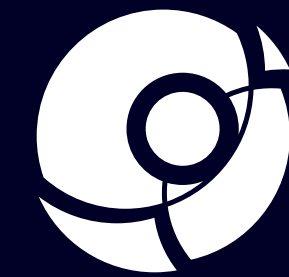
VIBRANT ECOSYSTEM

RELYING PARTY SOFTWARE

- FORT Validator, by NIC.mx & LACNIC (in C)
- Routinator 3000, by NLnet Labs (in Rust)
- OctoRPKI, by Cloudflare (in Go)
- RIPE NCC RPKI Validator (in Java)
- Dragon Research Labs Validating Cache (in Python)
- RPSTIR, by Raytheon BBN Technologies (in C)
- OpenBSD rpki-client(1) (in C)

RPKI SUPPORT

- FORT Project to support routing security in Latin America
- Documentation and FAQ – rpki.readthedocs.io
 - Community driven, allows translations
- Public mailing list with 200+ subscribers – rpki@nlnetlabs.nl
- Commercial support with SLA on Krill and Routinator



NLNETLABS



nlnetlabs.nl/rpki



rpki.readthedocs.io



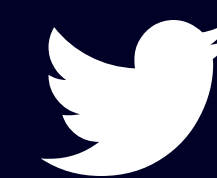
github.com/nlnetlabs



rpki@nlnetlabs.nl



[@krillrpki](https://twitter.com/krillrpki)



[@routinator3000](https://twitter.com/routinator3000)