RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Recent Developments in RPKI

And what's coming next

Riccardo Stagni | 10 May 2023 | ITNOG7

What is RPKI?

- Resource Public Key Infrastructure
- Certification Authority hierarchy with
  - 5x RIR trust anchors
  - And 2x AS0 trust anchors (APNIC + LACNIC)
- Signed objects with different payloads
  - Currently only ROAs (containing VRPs) are of active practical use (for ROV)

- Streamlining a lot of things that were glued together with scripts

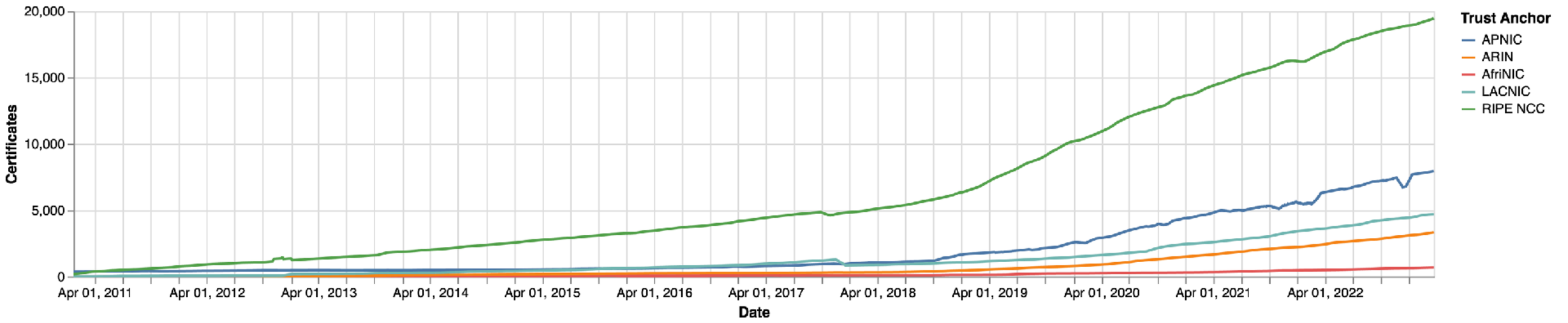
Status and Statistics (1)

- RPKI covers about 37% of IPv4 and 32% of IPv6
  - https://ftp.ripe.net/pub/stats/ripencc/nro-adoption/latest

- About 3000 RPKI validators running globally
- About 2500 unique IPv4 /24 or IPv6 /48 running RPKI validators
  - https://rov-measurements.nlnetlabs.net/stats/

Status and Statistics (2)

- Steady growth of adoption and number of ROAs
  - https://certification-stats.ripe.net/



So now what?

- RPKI ensures
  - That resource holders are certifiably linked to the resources that they manage
  - And that reliable data is available to make informed decisions
- We all know this, right?
- If not:
  - https://rpki.readthedocs.io/
  - https://www.manrs.org/
  - https://academy.ripe.net/

So your network will be more...

- Secure
- Stable
- Boring :)

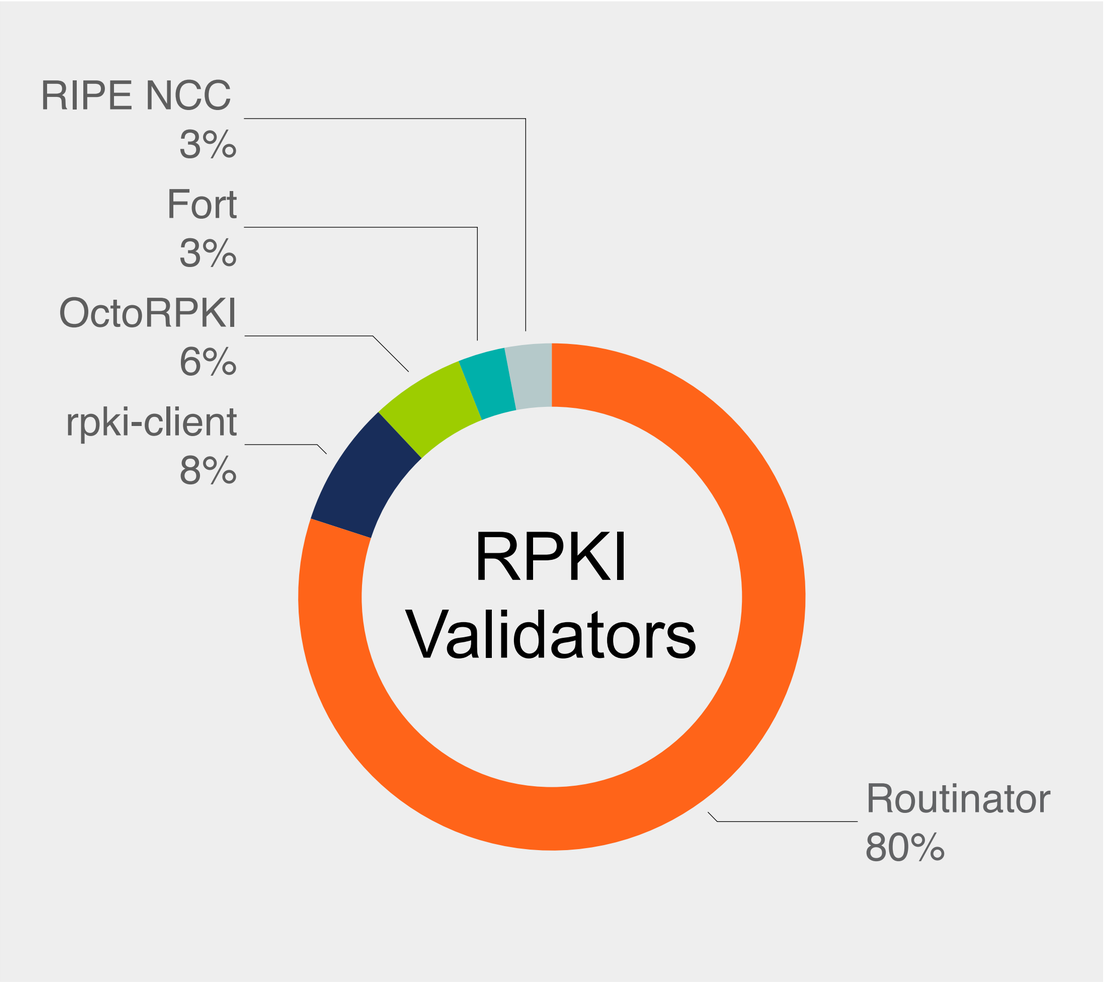
- Is there something that we can do about it?

And Now for Something Completely Different

Eh, you said recent developments right?

RPKI validators are mature

- Installation, configuration, documentation is way better
- Research on vulnerabilities in 2021
  - https://arxiv.org/abs/2203.00993
  - Multiple fixes in all validators (mostly addressing potential DoS attacks)
- But there is a risk of monoculture, so run different ones
  - https://rov-measurements.nlnetlabs.net/stats/
  - Stop using the RIPE NCC validator!



Trendy: Publication as a Service (1)

- There are two flavours of RPKI
  - Hosted: your RIR maintains your CA, creates objects and publishes them for you
  - Delegated: you maintain your CA, create objects and publish them in your own repo
- Publication as a Service is an in-between flavour
  - You maintain the CA, create objects and then send them to the RIR*
  - The RIR* publishes your objects in its repository
  - * (which RIR is left as exercise for the reader)
- Supported by APNIC, ARIN, RIPE NCC
- AKA “Publish in parent” or “Hybrid RPKI”

Trendy: Publication as a Service (2)

- Win-Win for smaller delegated CAs
  - You keep control of the delicate crypto stuff
  - You use your own platform
  - RIRs have vast experience in maintaining consistency and usually have better availability
- Well documented and easy to set up
- Fun fact: You don’t need 100% availability
  - ARIN did a test with simulated outage of ~60 minutes
  - Validators cache everything anyway, objects do not expire for hours
  - RFC 9286 aligns validators’ behaviour in such cases

Coming Soon: ASPA (1)

- Autonomous System Provider Authorisation
  - https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile
  - https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification
  - drafts, about to become RFC
- Validation of AS_PATH
  - ROAs with VRPs > ASPAs with VAPs
- Supported by RIPE NCC's API in pilot environment
  - Planned support in LIR Portal UI
  - (but difficult doing something automagical due to hidden paths)
  - ...meanwhile you can use delegated/hybrid CA :)

Coming Soon: ASPA (2)

- Already supported by a couple of validators out there
- RPKI-to-Router support - RFC 8210bis, final draft
- Support in OpenBGPD and NIST BGP-SRx

- Someone is running it in production:
  - https://mailman.nanog.org/pipermail/nanog/2023-February/221471.html
  - https://datatracker.ietf.org/meeting/116/materials/slides-116-sidrops-aspa-deployment-experience-yycix-00.pdf
  - https://www.manrs.org/2023/02/unpacking-the-first-route-leak-prevented-by-aspa/

Coming Next: RSC

- RPKI Signed Checklists (RFC 9323)
  - A resource holder can sign arbitrary files with a specific set of Internet Number Resources
  - The recipient of an RSC can then verify that the holder of those resources produced it
- Use cases:
  - Automated Bring Your Own IP (BYOIP) on-boarding
  - PeeringDB or other databases
  - Content Provider/CDN portal
  - https://www.manrs.org/2023/02/the-benefits-of-rpki-signed-checklists/
- Not (yet) in LIR Portal UI, but PaaS or self-hosted do work

More?

- BGPSec certificates are kinda usable
  - Not (yet) in LIR Portal UI, but PaaS or self-hosted do work
  - Let us know!
- Other things happening behind the scenes:
  - Audits, UI revamp, rsync capacity, new HSMs...
  - https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/rpki-planning-and-roadmap
  - https://www.ripe.net/participate/mail/ripe-mailing-lists/routing-wg

Conclusion

- RPKI has become a mature ecosystem
  - ROV prevents some mistakes and malicious activity
  - ROA + ASPA will prevent the majority of mistakes and malicious activity
  - RSC will make easier deploying cloud-hosted services, or dealing with CDNs, or whatever you can think of
- RPKI deployment effort is manageable
- Go for it if you still have not

Conclusion

- RPKI has become a mature ecosystem
  - ROV prevents some mistakes and malicious activity
  - ROA + ASPA will prevent the majority of mistakes and malicious activity
  - RSC will make easier deploying cloud-hosted services, or dealing with CDNs, or whatever you can think of
- RPKI deployment effort is manageable
- Go for it if you still have not
  - And then, once your network is secure, you can go back focusing on deploying IPv6 :)


Join us at
RIPE 86
Rotterdam, Netherlands
22 - 26 May 2023

Questions

rstagni@ripe.net
rpki@ripe.net