RIPE NCC
RIPE NETWORK COORDINATION CENTRE

News From Your RPKI Trust Anchor

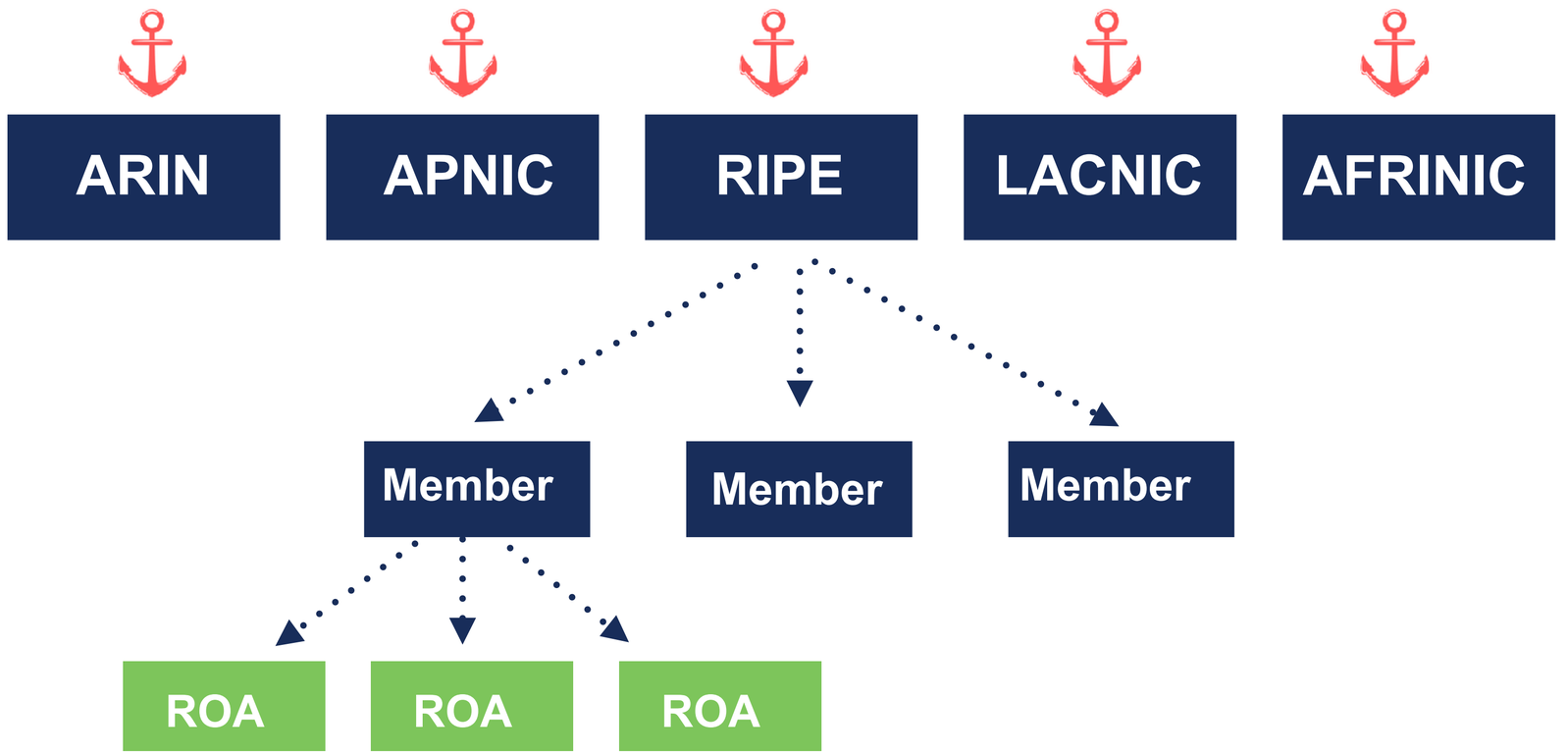
Nathalie Trenaman
Routing Security Programme Manager

Resource Public Key Infrastructure

- Ties IP addresses and ASNs to public keys
- Follows the hierarchy of the registries
- Authorised statements from resource holders
  - “ASN X is authorised to announce my Prefix Y”
  - Signed, holder of Y

RPKI Certificate Structure

Certificate hierarchy follows allocation hierarchy



What is an RPKI Trust Anchor?

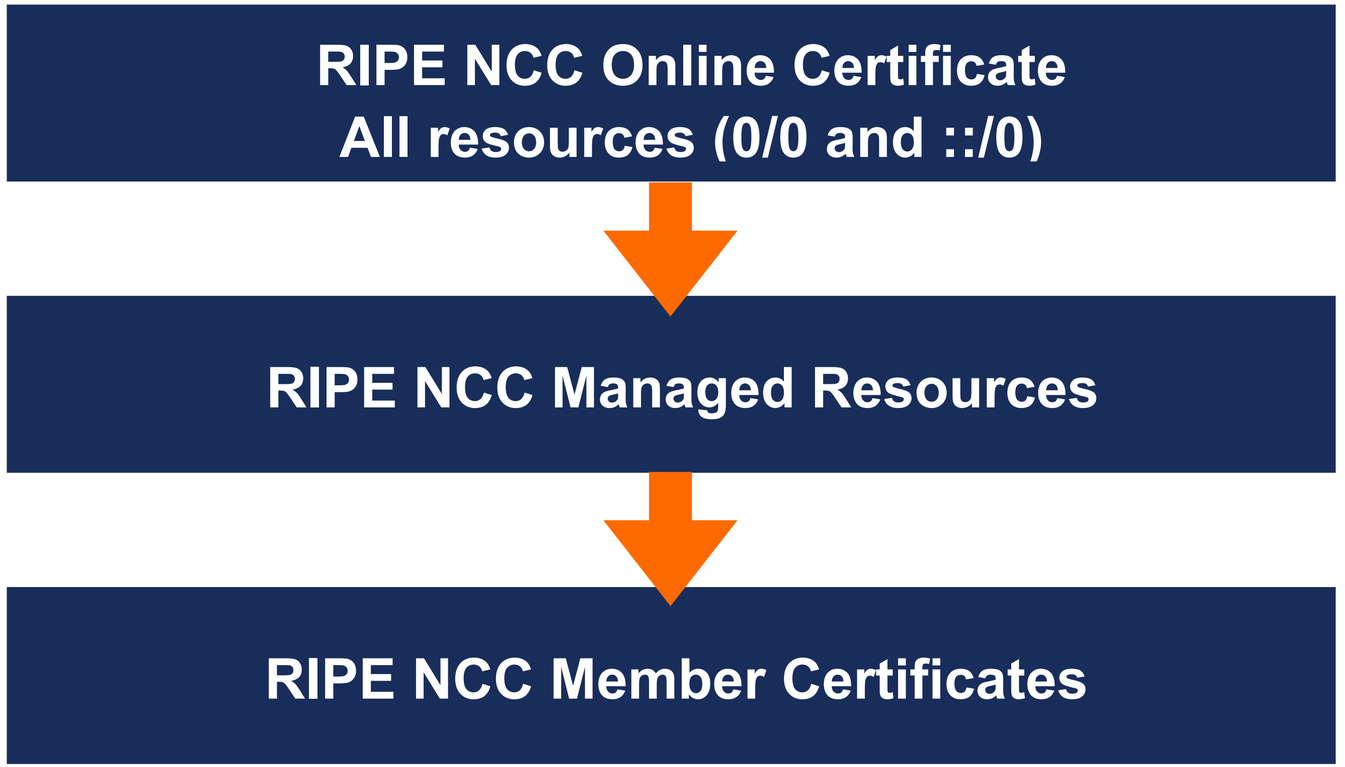
"A Trust Anchor is an authoritative entity for which trust is assumed and not derived"

RIPE NCC Offline Trust Anchor
All resources (0/0 and ::/0)

- Contains the URLs and certificate public key

-https://rpki.ripe.net/ta/ripe-ncc-ta.cer
-rsync://rpki.ripe.net/ta/ripe-ncc-ta.cer

What Lives Below?



Trust is Important

- When you run a Trust Anchor you must be:
  - Secure
  - Transparent
  - Auditable

Secure

- We recently finished a migration to a new offline Hardware Security Module (HSM)
  - RIPE Labs article coming soon!
- And plan to migrate to a new online HSM later this year
  - This is a bigger project
- Regular penetration tests for our software
- Red Team test coming this year
  - Overall security exercise

Transparent

- There is a RIPE NCC Certificate Practice Statement:
  - https://www.ripe.net/publications/docs/ripe-751
  - Next version must be reviewed by the community
- We publish all our security test reports from external parties online:
  - https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/security-and-compliance
- We are transparent about our priorities and publish our quarterly plans:
  - https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/rpki-planning-and-roadmap

Transparent (2)

- We open sourced our RPKI Core this year!
  - https://github.com/RIPE-NCC/rpki-core
  - Other parts were already open source

- We will present this work and the challenges we faced at RIPE 84

Auditable

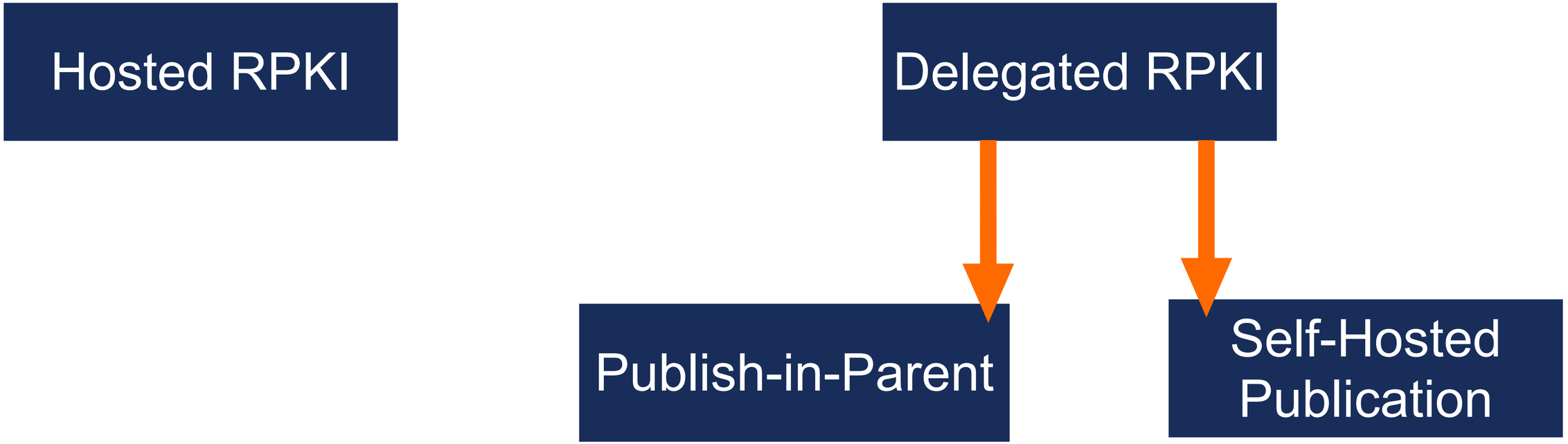
- RIPE NCC established an RPKI audit framework.
- SOC2/Type 2 turned into ISAE3000 Type 1 & 2

- Type 1: Audit the framework
- Type 2: Audit RPKI

- We expect to have Type 1 done this year
- Next steps?

Other Work…

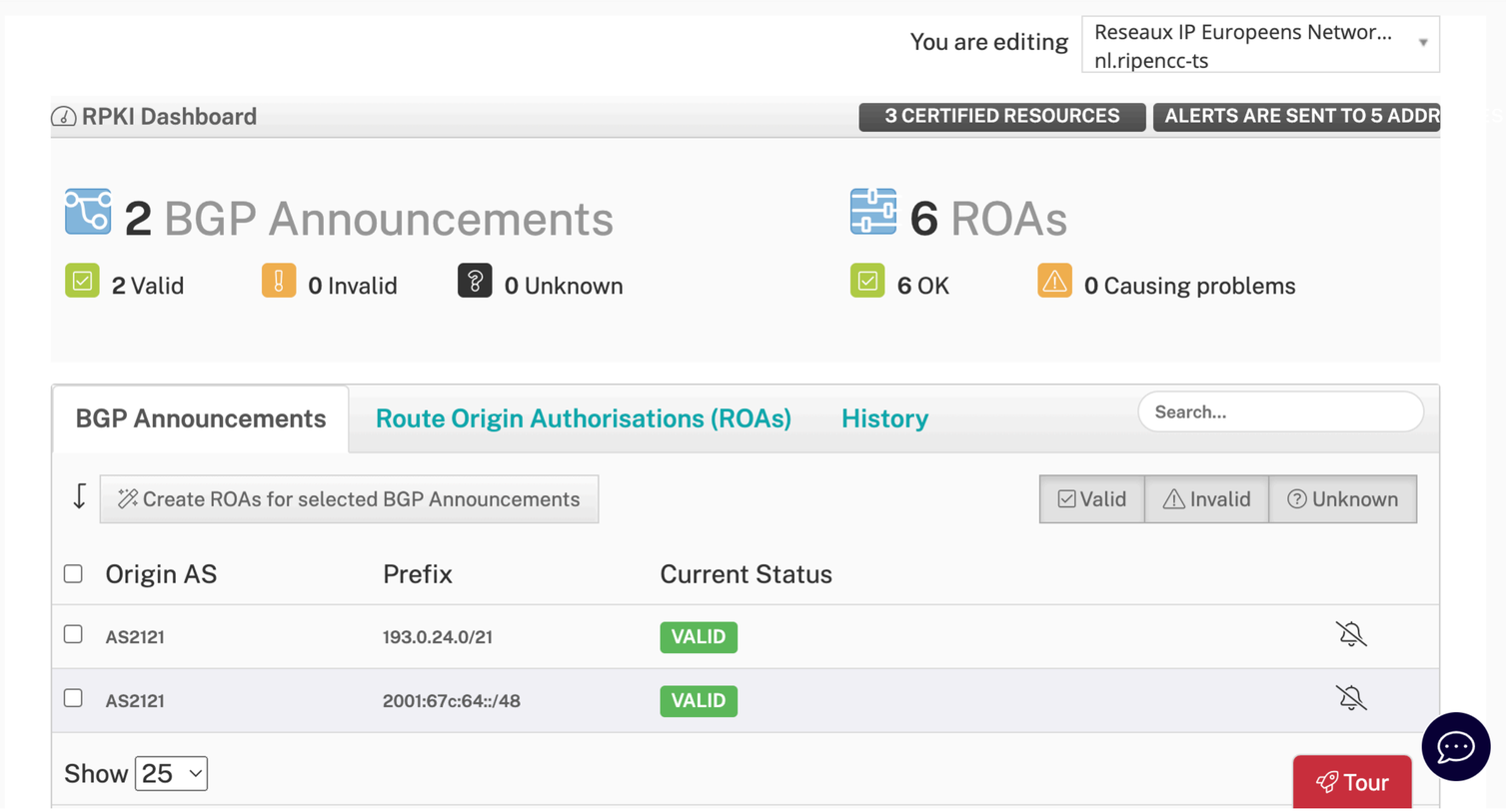
- We’re working on a Publication Service for Delegated RPKI
- Also known as: Publish-in-Parent



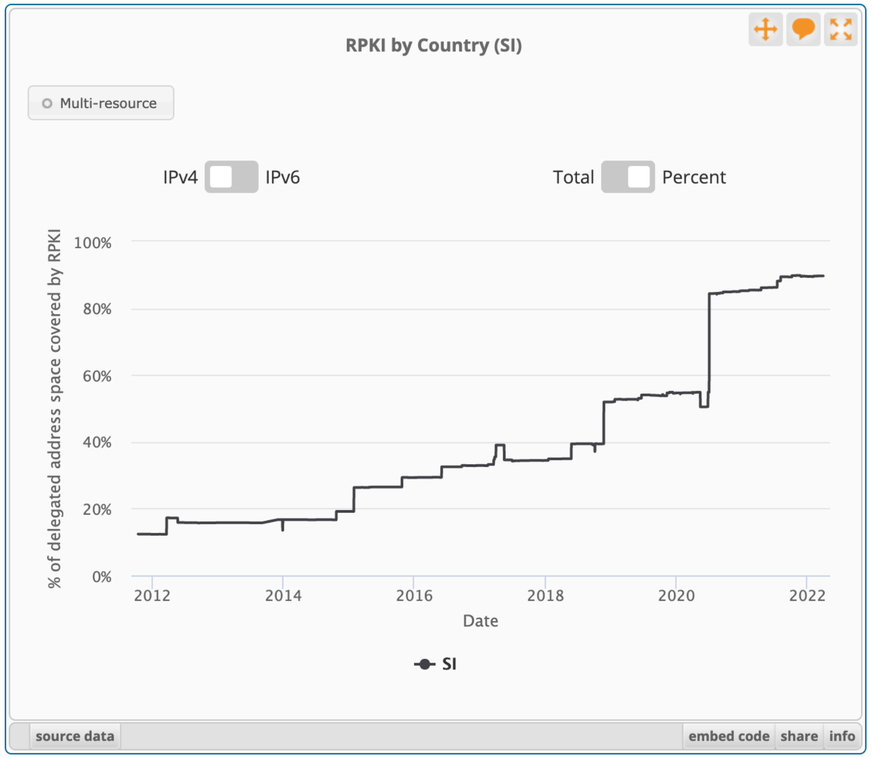
And Finally…

- We need your feedback on the RPKI Dashboard!
  - What do you like?
  - What can be improved?
  - What do you think is bad?

- Send us your thoughts:
  - rpki@ripe.net

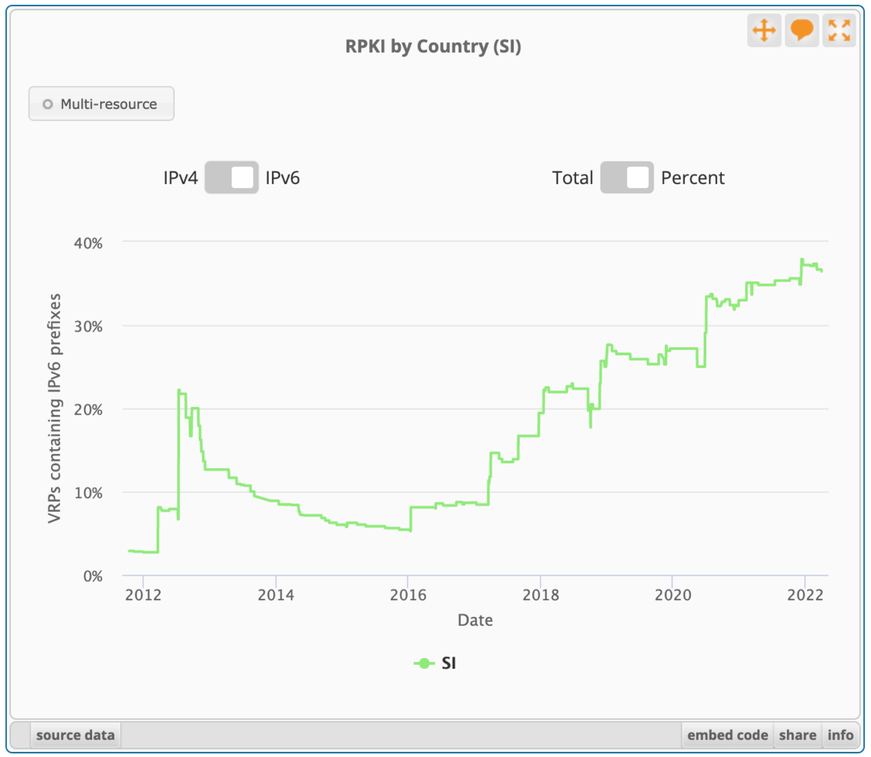


One More Thing



IPv4:

90%



IPv6:

37%

- IPv6 is important!

Questions

nathalie@ripe.net
rpki@ripe.net