RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RPKI: introduction & activity update

TLDCON 13 September 2023

Bastiaan Goslings

Outline

- The RIPE NCC - who are we?
- BGP and routing incidents
- Recap RPKI - role RIPE NCC as RIR
- Statistics: regional deployment RPKI
- Actions RIPE NCC / what's next
  - Policy related
  - Technical

- Questions?

RIPE NCC - who are we?

- A Regional Internet Registry (‘RIR’)
- We manage the allocation and registration of ASNs and IP addresses in Europe, the Middle East and parts of Central Asia
  - Ensure unique holdership of these number resources (>20k members)
  - Document the holdership in the RIPE Database
  - Issue digital certificates for allocated IP resources
  - Enable operators to document use of their address space

https://www.ripe.net/about-us/what-we-do

BGP, the routing protocol of the Internet,
assumes everybody is telling the truth…

But is that always the case?

- **There is no built-in security in BGP**
  - Any AS can announce any prefix
  - Anyone can prepend any ASN to the BGP AS-path
  - BGP announcements are accepted without validation

- **Incorrect routing information can be propagated all over the Internet**

So, susceptible for incidents - and for abuse

- **An attacker may use a BGP hijack for malicious purposes…**
  - stealing cryptocurrency
  - traffic interception and eavesdropping
  - preventing an entire network from being reachable (null routing)
  - stealing credentials
  - sending spam…

(Mind you, not all BGP incidents are intentional!)

So, in order to make routing more secure…

- **Operators at least need to verify the routing information they receive**
  - Has an announced prefix been originated by the legitimate holder?
  - Has someone tampered with the AS path of the BGP update?
- **This can prevent propagation of incorrect routing information**

What about RPKI? How does it improve security?

- **It verifies the association between resource holders and their Internet number resources. This is the authorisation part**
  - Proves holdership through a public key and certificate infrastructure
- **This can then be used by others to validate the origin of BGP announcements**
  - Is the originating ASN authorised to originate a particular prefix?
- **Stepping stone to “Path Validation”**

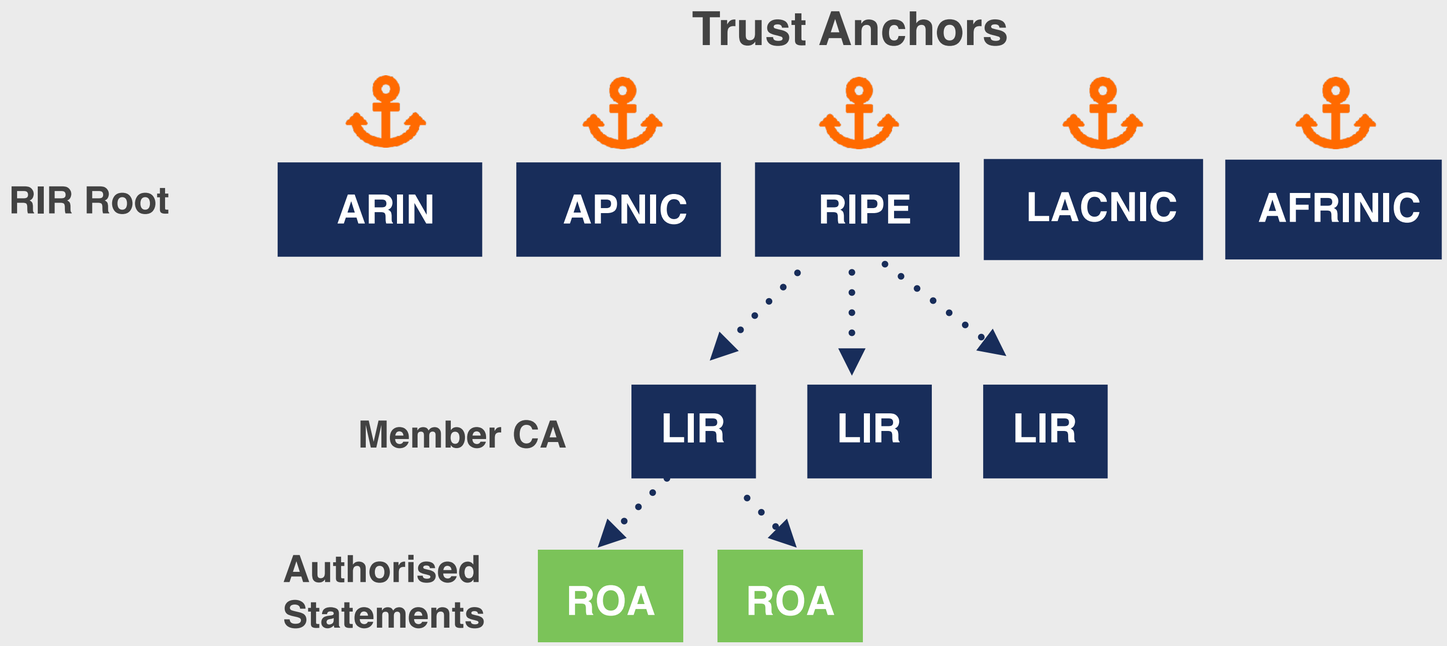
How does it work?

- RPKI attaches a digital certificate to IP addresses and AS numbers

- Digital signatures authorise the use of resources
  - Private key to sign, public key to validate

Where does an RIR like the RIPE NCC fit in?

- RPKI relies on the 5 RIRs as Trust Anchors
- Certificate structure follows the RIR hierarchy
- RIRs issue certificates to resource holders
- Digital signatures of resource holders authorise the use of resources



A global RPKI ecosystem enhances routing security

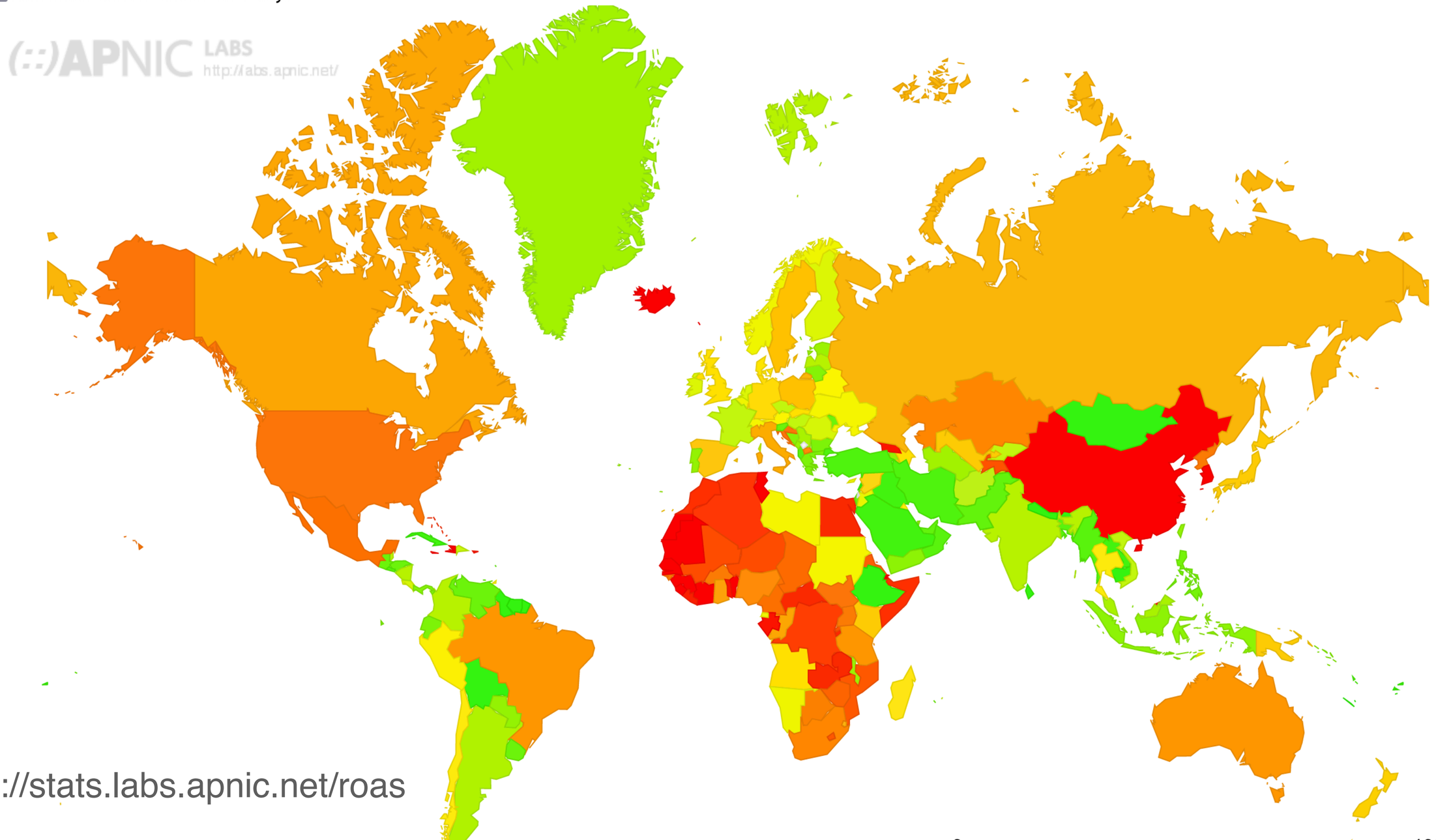
- RPKI is a powerful mechanism
  - Can prevent BGP hijacks, mis-originations (‘fat fingers’) and route leaks
  - Currently used for validating the origin AS
  - Stepping stone to BGP path validation
- However, RPKI is opt-in
  - It will only work if every network agrees to abide by it
- Currently ~35% of the Internet uses RPKI validation
  - BGP hijacking may cause significant damage unless the majority implements it

Some numbers when it comes to RPKI adoption

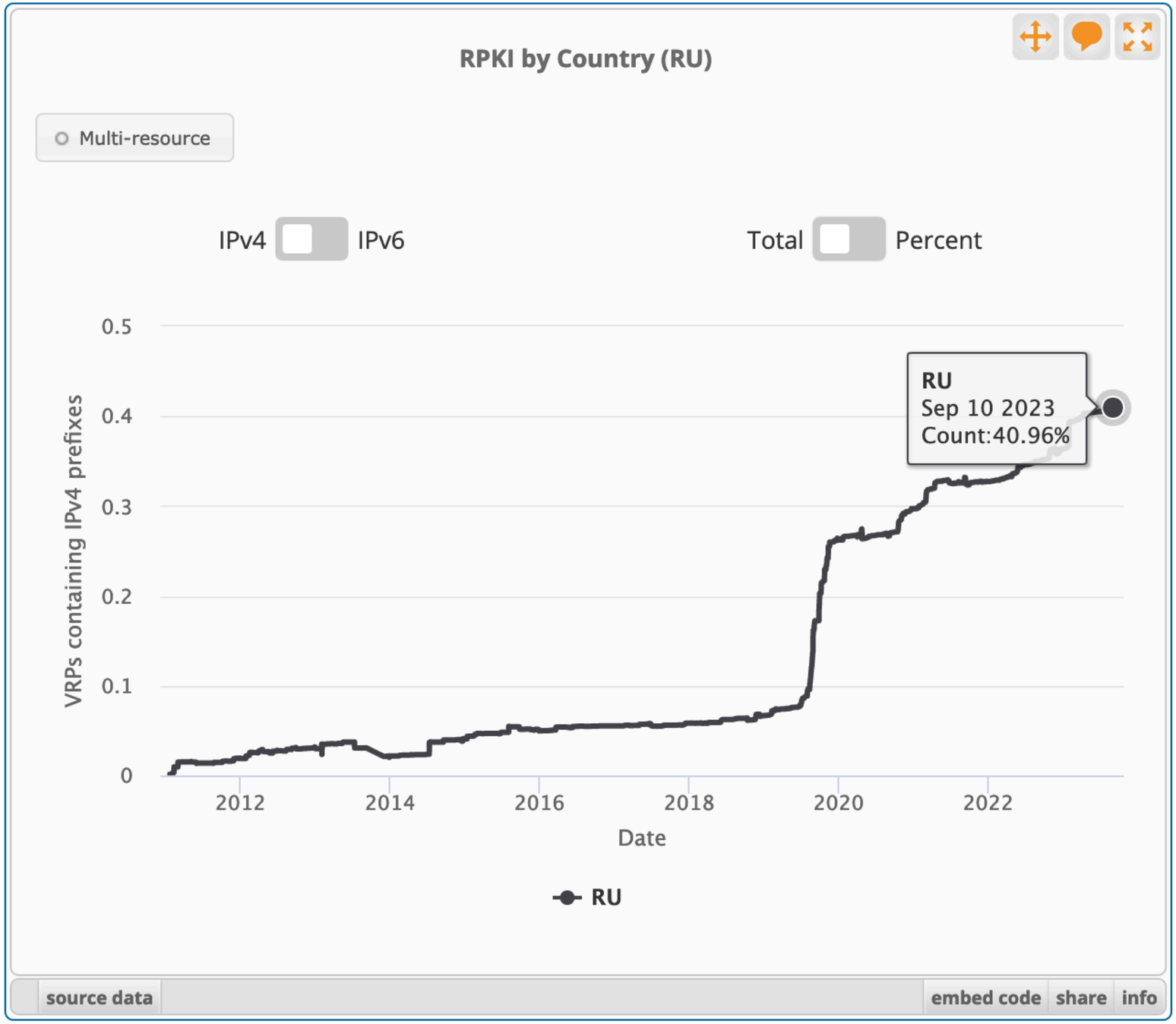
ROA data by Country (%)

Click here for a zoomable map

☐ Remember current choice for 7 days

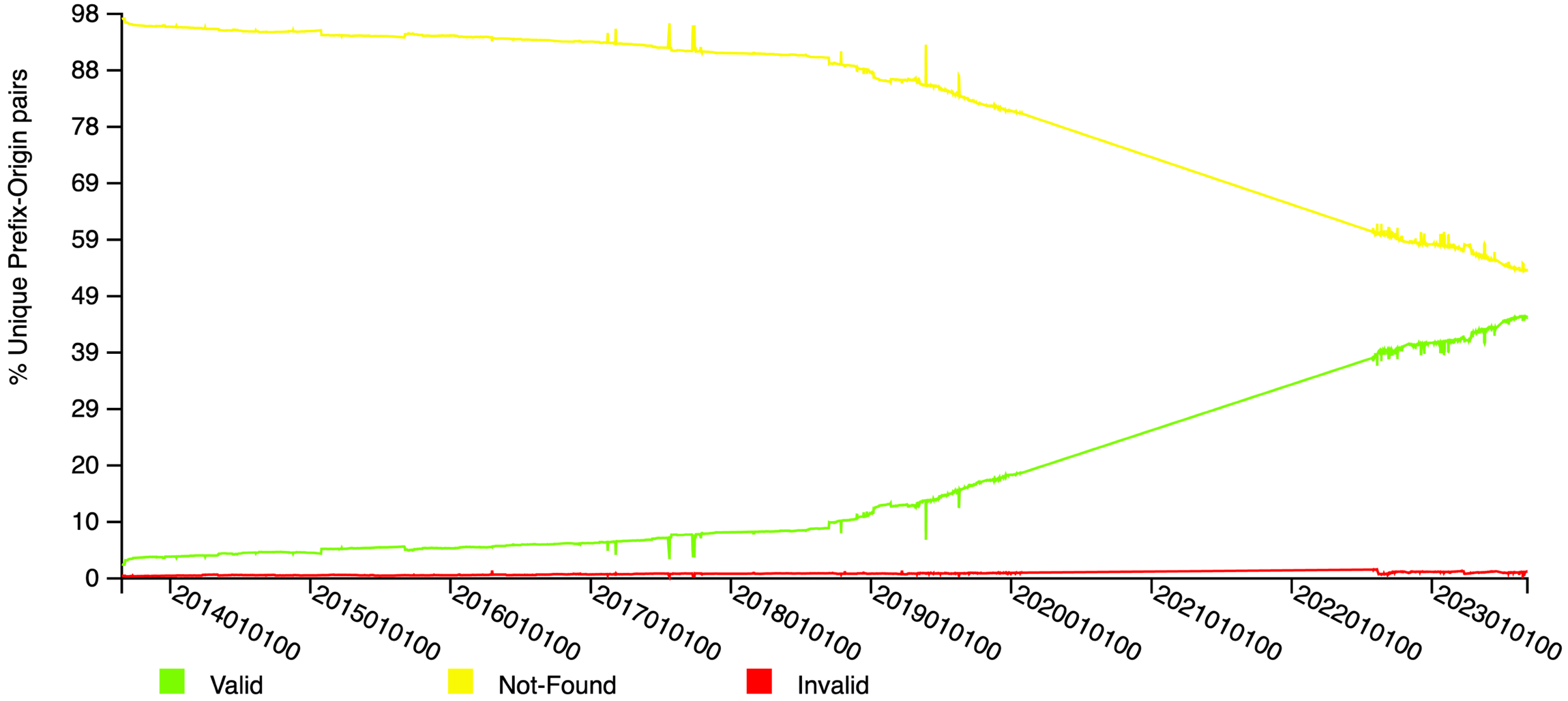


https://stats.labs.apnic.net/roas



https://stat.ripe.net/ui2013/RU#tabId=routing

RPKI-ROV History of Unique Prefix-Origin Pairs (IPv4)



NIST RPKI Monitor: RPKI-ROV Analysis **Protocol:** IPv4 **RIR:** All

https://rpki-monitor.antd.nist.gov/

Actions RIPE NCC / What's next: policy related

- **From RIPE NCC 2022-2026 strategy: https://ftp.ripe.net/ripe/docs/ripe-774.pdf**
  - 3.1 Secure internet number resources by developing and operating a resilient, externally auditable, and secure resource certification Trust Anchor
  - 3.3 Support the growth of the Internet through promoting the use of best practices for Internet Resources and standards such as IPv6 and RPKI
- **This includes a focus on training of members and others: Routing Security courses and -certification**
  - https://academy.ripe.net/ (free online courses) and https://learning.ripe.net (physical and webinars)
- **Outreach: organise and host workshop at Internet Governance Forum 2023: https://www.intgovforum.org/en/content/igf-2023-ws-339-increasing-routing-security-globally-through-cooperation**

Actions RIPE NCC / What's next: technically

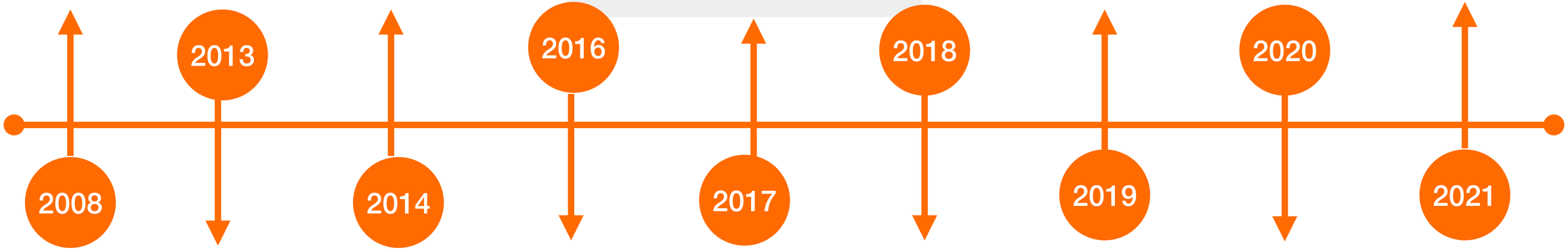
- **ASPA ('Autonomous System Provider Authorization') support based on RPKI —> path validation**
  - Standard not finalised yet within IETF - once RFC published we intend to offer the feature to members
- **RIPE NCC's RPKI infrastructure: improving security, audit and ISAE 3000 certification**
  - Upgrades, planning migration to a new online HSM later this year
  - Regular two year penetration tests for our software and once performed Red-team test (overall security exercise)
  - RIPE NCC designed RPKI tailored control framework (ISAE 3000): gap analysis completed, now further developing documentation and implementing controls to prepare for first certification audit end 2023 / early 2024

Questions

TLDCON RPKI
Bonus slides

1 min.

A few notable BGP related incidents from recent years



Pakistan Telecom hijacked YouTube

STE hijacked many prefixes including US DoD, YouTube, Level 3, Akamai…

Google, Apple, FB, Microsoft, Riot Games prefixes were hijacked

Taiwan Network Information Center Public DNS in Taiwan was hijacked

AS55410 (Vodafone Idea) hijacked almost 40k prefixes, belonging to 4k+ ASNs in 164 countries.

Ukranian Telco (Vega) hijacked BT prefixes

AWS Route Leak

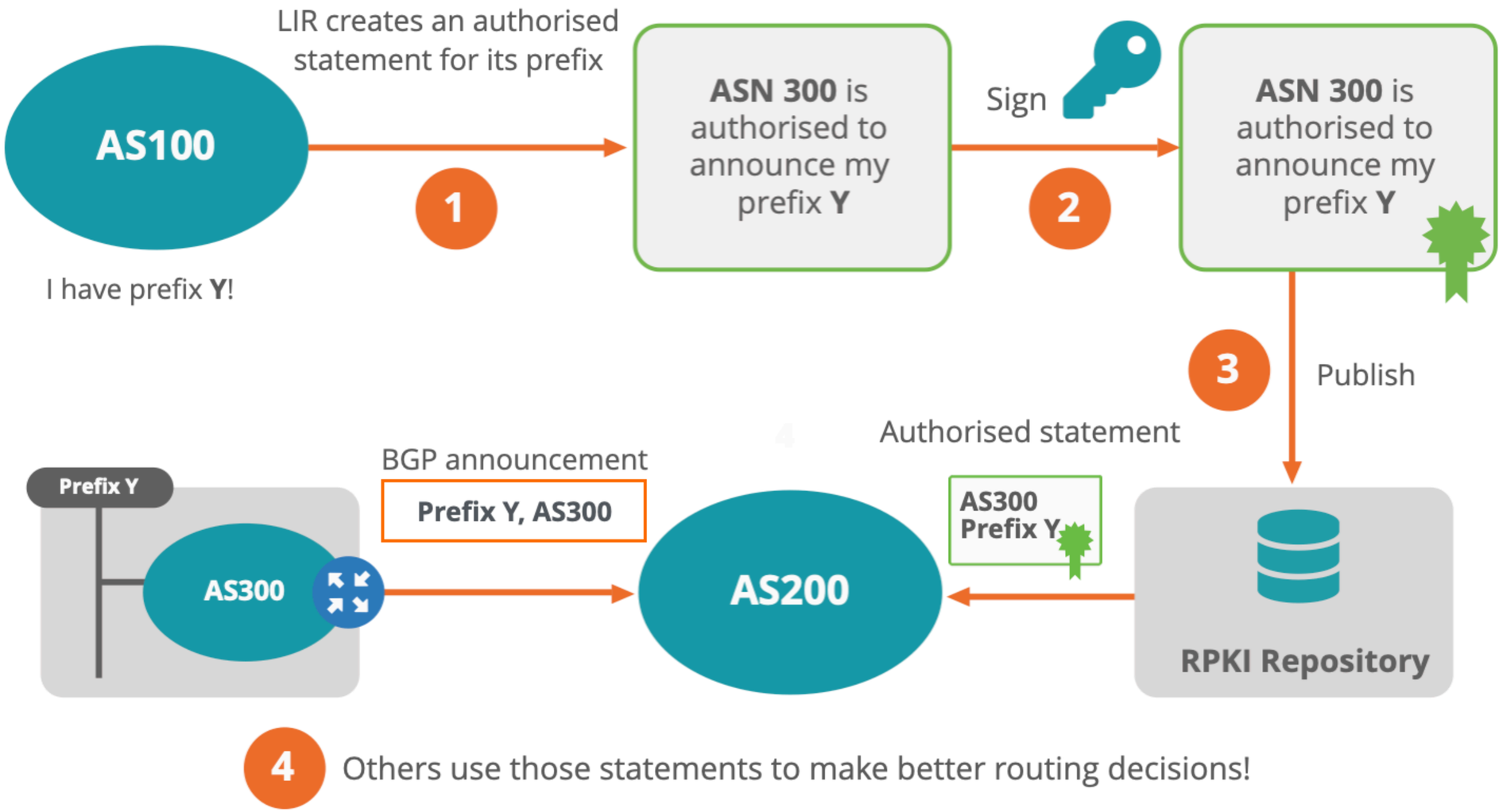
Amazon Route 53 Hijack myetherwallet.com cryptocurrency hijack

Google Prefix Leak

Telstra hijacked 500 prefixes

>8k BGP prefixes hijacked, affected companies such as Amazon, Akamai, Alibaba

How does RPKI work?



How is RPKI different than the IRR system?

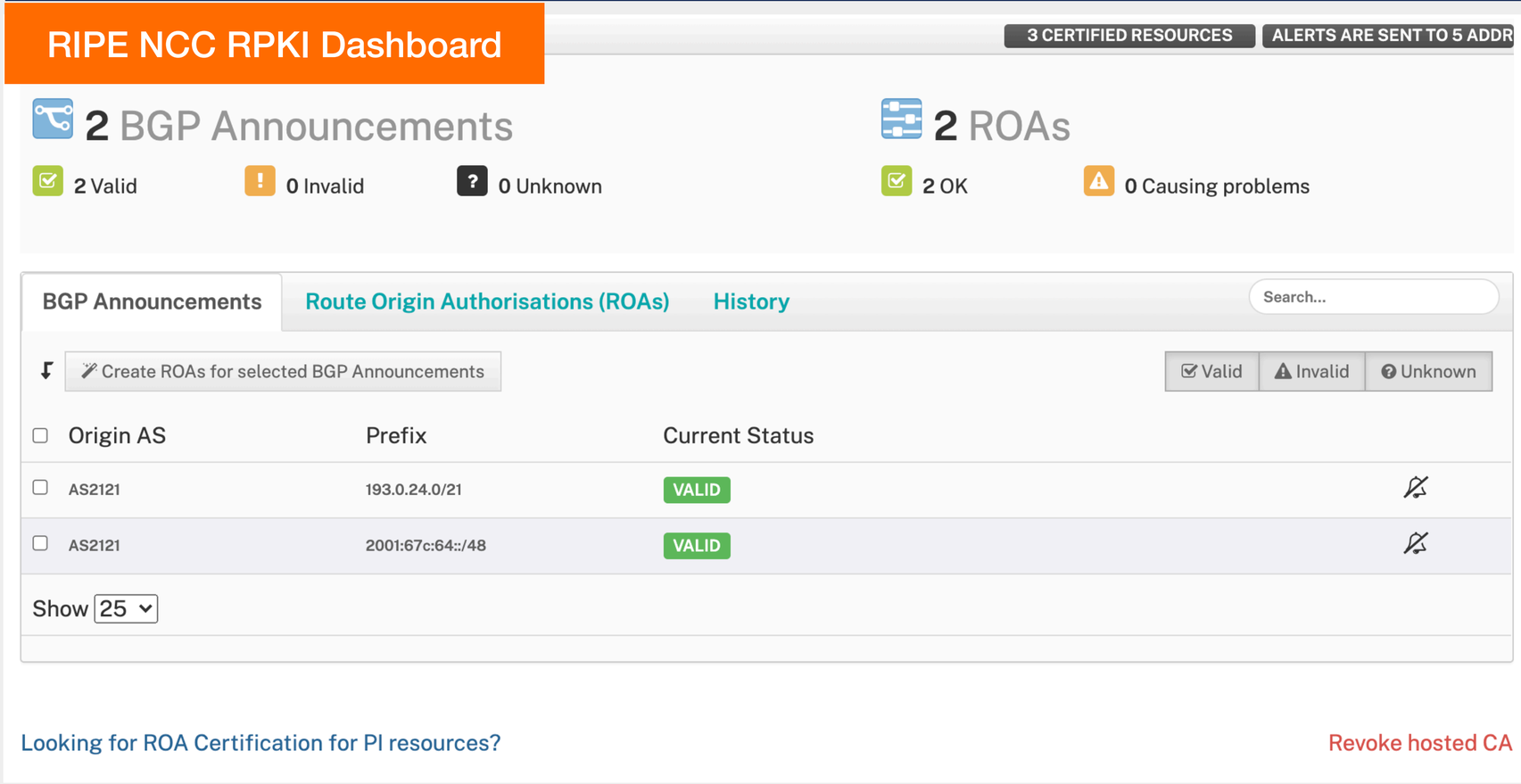
- **RPKI is based on the RIRs (= five globally) as Trust Anchors**
  - RIRs have control over the accuracy of registered data

- **Cryptography is used to verify the holdership**
  - Provides data you can trust

RPKI, SIGNING

Create ROAs for your prefixes in the RPKI system

RIPE NCC RPKI Dashboard

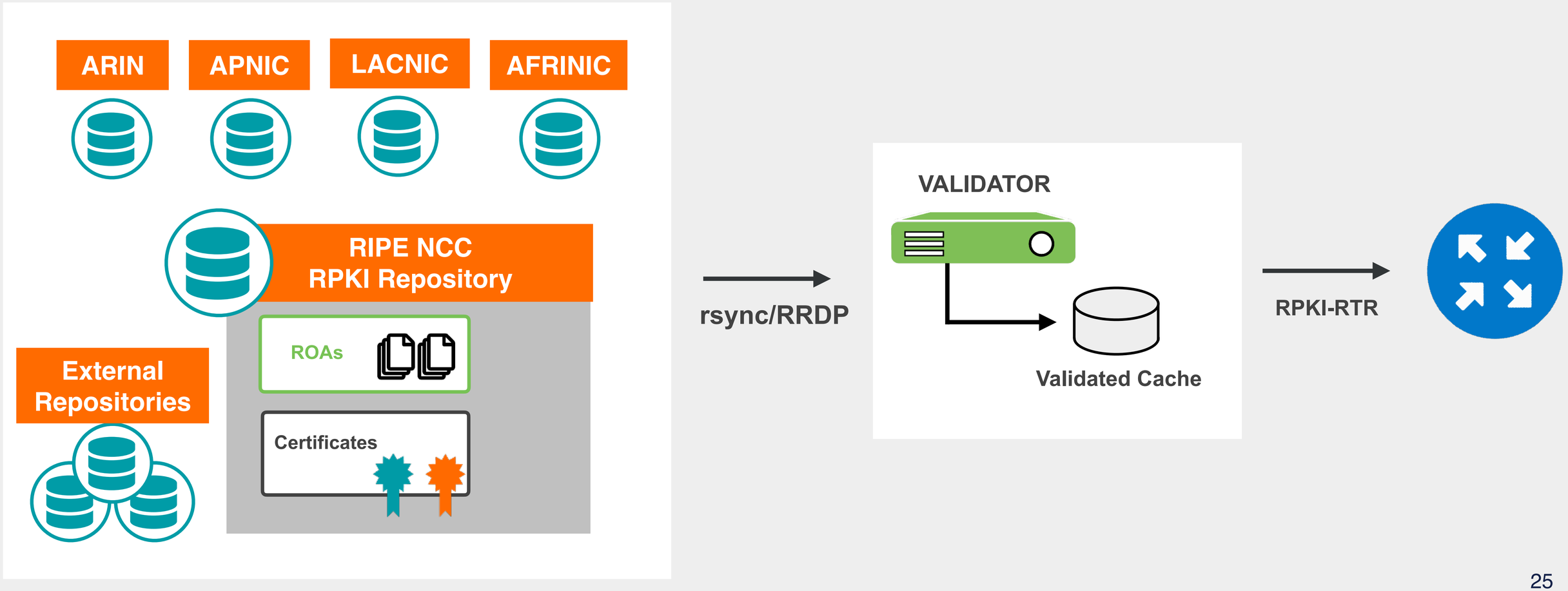


Publication

RIPE NCC RPKI Repository

RPKI, VALIDATION

Verify information provided by others



RPKI Test Dashboard

https://localcert.ripe.net/#/rpki

- You can create test ROAs for your BGP announcements
- It doesn’t affect your network
- It’s just a test dashboard
- You need to sign in with your RIPE NCC Access account

What to do - suggested steps at the technical level

1. Check prefixes before announcing

2. Register your routing information in IRRs

3. Filter BGP routes from your peers, customers and upstreams

4. Implement BGP filters based on verifiable information (Internet Routing Registry, RPKI)

Some factors limiting adoption of routing security

- Implementing routing security is non-trivial.
- Incidents have not been a major threat.
- Collective action problem: Methods require many parties to work together, with limited direct benefit.
- Limited robust data over time on the scope and scale of routing incidents.