RIPE NCC RPKI Operations Update

Tim Bruijnzeels | 22 May 2024 | RIPE 88

A New UI?

- Why?

  - Improve sub-optimal processes: staging ROAs, alerts, etc

  - Improve maintainability

  - Add support for new RPKI object types more easily

- How?

  - UX interviews with users at RIPE 87

  - Implementation is happening right now!

  - Beta test starting soon! Volunteers wanted!

For Example: Pending Changes

Review and apply ✕

Staged ROAs

Origin AS	Prefix	Max Length
AS2121	193.0.24.0/21	21

📢 **Affected announcements**

Origin AS	Prefix	Current status	New status
AS2121	193.0.24.0/21	☐ Unknown	→ ☑ Valid

Apply now | To pending changes

Review and apply ✕

Staged ROAs

Origin AS	Prefix	Max Length
AS2121	2001:67c:64::/48	48

📢 **Affected announcements**

Origin AS	Prefix	Current status	New status
AS2121	2001:67c:64::/48	☐ Unknown	→ ☑ Valid

Apply now is not available when you have pending changes | To pending changes

BGP Announcements: 2	ROAs: 2	Pending changes: 2

Staged ROAs

✓ Apply All | ↺ Discard All

Origin AS	Prefix	Max Length		
AS2121	193.0.24.0/21	21	✎ Edit	↺ Discard
AS2121	2001:67c:64::/48	48	✎ Edit	↺ Discard

Affected Announcements

Origin AS	Prefix	Current State	Future State
AS2121	193.0.24.0/21	☐ Unknown	→ ☑ Valid
AS2121	2001:67c:64::/48	☐ Unknown	→ ☑ Valid
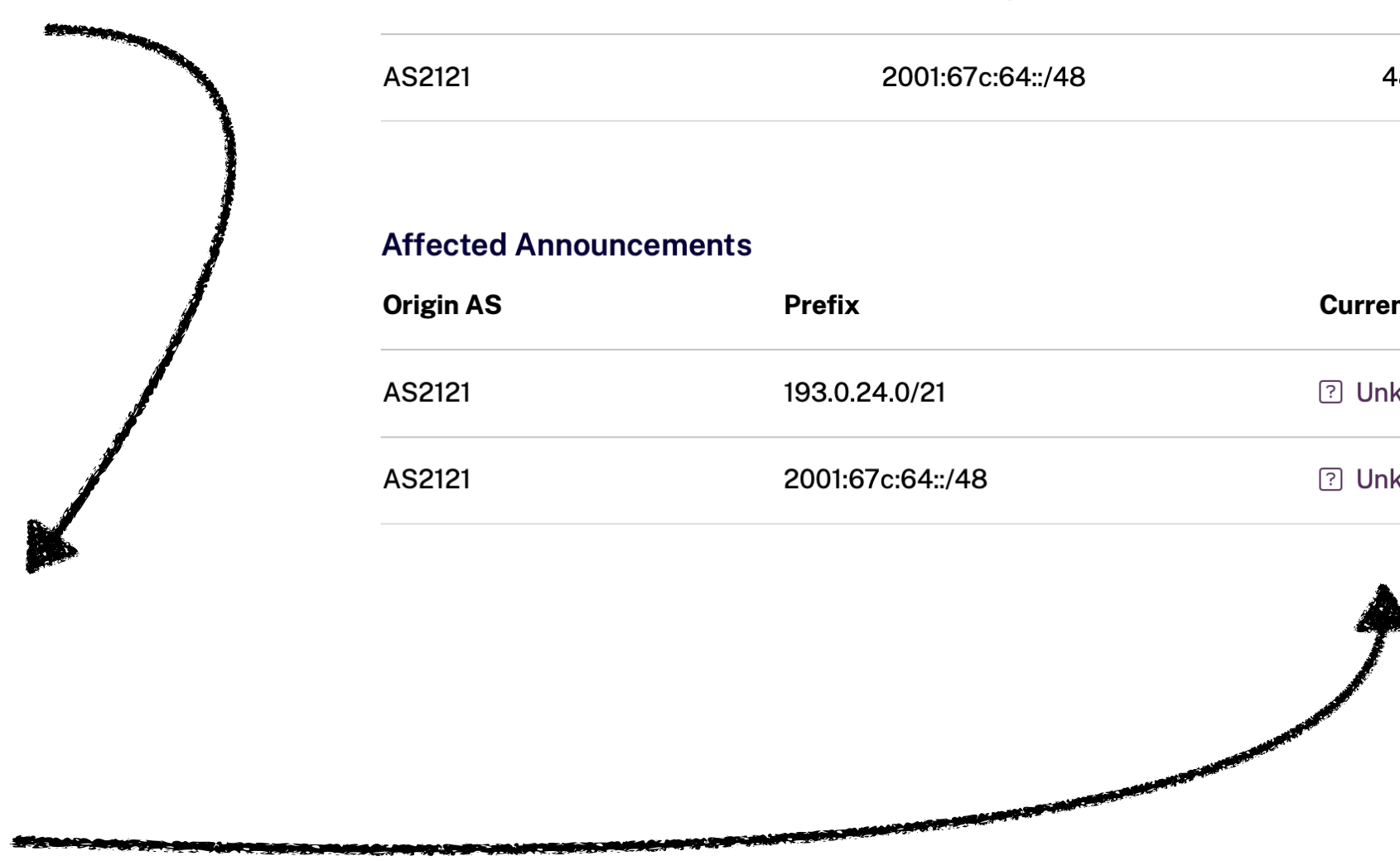
Future Functionality

- New RPKI object types

  - ASPA (API/UI, pending IETF last call)

  - Resource Signed Checklists (API)

  - BGPSec router certificates (API)

- Faster BGP information

  - Current BGP information is up to eight hours old

- IRR integration

  - Automatically create route objects?

ASPA… in one minute

- AS holders declare providers

  - Helps detect route leaks

  - Makes path spoofing attacks on ROV (much) harder

- More information

  - RPKI Usability 2024 at SEE12

  - Presentation by Ben Maddison at AfPIF2023

  - IETF verification draft and proof of correctness

- Currently available in the test environment (API only)

Hardware Security Modules (HSM)

- Used to keep private keys secure

- Replaced HSM hardware for the online system

- Replaced Trust Anchor laptop (using USB based HSM)

ISAE3000

- Support auditors and InfoSec

- Formalise Business Continuity Plan

  - Clearly documented outage scenarios and mitigations

- Improved database backup strategy

  - Reduced data loss in case to <1 hour

- Updated Certification Practice Statement

  - In particular: improved description of the offline Trust Anchor signing sessions

NRO RPKI Program

- Aimed at providing a **more consistent RPKI service for the global Internet community**

- Started in 2024

  - Sofía Silva Berenguer, RPKI Program Manager - NRO

  - Representatives of each RIR

  - Regular (online) meetings

- Read more

  - https://labs.ripe.net/author/sofia_silva_berenguer/improving-rir-alignment-in-the-rpki-space/

  - https://www.nro.net/technical-coordination/security/certification/#rpki_program

NRO RPKI Program

- What are the **main barriers or obstacles** for RPKI adoption that could be solved (or at least improved!) through better **coordination and collaboration** among the RIRs?

- Do you have ideas of initiatives we should consider?

- Let us know!

  - Talk to us

  - Discuss in the routing working group

  - Or email Sofia directly at rpki_program@nro.net

NRO RPKI Program

- Key Objectives

  - Definition of what a single global RPKI system looks like

  - Better understanding and improved transparency of robustness

  - Enhanced security consistency

  - Engage with the global technical community

- Short term (2024)

  - Establish and document status quo at each RIR

  - Cooperate on proposals

  - Follow-up work items likely in 2025

Questions ?

tbruijnzeels@ripe.net