RPKI Signed Checklists (RSCs)

What is an RSC?

- **R**PKI **S**igned **C**hecklist
- Defined in RFC 9323
- The specification provides for:
  - signing one or more arbitrary files using an RPKI certificate
  - packaging the signature, filenames, and hashes into an object (the **RSC** itself)
  - verifying the signature (i.e. “these files were signed by somebody with authority to route 192.0.2.0/24”)

Why is it useful?

- Arbitrary files can be signed
  - More flexible than existing RPKI functions
  - Supports ad hoc/people-driven processes
- No need to publish in a public repository
  - Associated business operations can remain private

Use cases

- BYOIP services
- Third-party databases
- Custom RPKI applications

BYOIP services

- Support use of RIR-delegated IP addresses for BGP announcements in cloud infrastructure
- RSCs can help to streamline the registration process

aws

Microsoft Azure

Third-party databases

- Acting as cross-RIR interfaces for specific use cases (e.g. peering)
- RSCs can be used to prove resource holdership

PeeringDB

Custom RPKI applications

- Define new object type and use RSCs for signing/packaging
- Useful for testing/prototyping, or for use within a closed group of participants
- No need to go through IETF process

Current status

- Specification published in November 2022
  - https://www.rfc-editor.org/rfc/rfc9323.txt
- Production code
  - https://www.rpki-client.org
- Proof-of-concept code
  - https://github.com/APNIC-net/rpki-rsc-demo
  - https://github.com/job/draft-rpki-checklists
  - https://github.com/benmaddison/rpkimancer
- APNIC implementing in Q2 of this year
  - In-principle support from other RIRs

2023

APRICOT

APNIC 55

MANILA, PHILIPPINES

20 February – 2 March 2023

#apricot2023