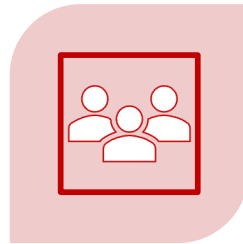# A more consistent RPKI service for the global Internet community

Sofía Silva Berenguer
RPKI Program Manager - NRO
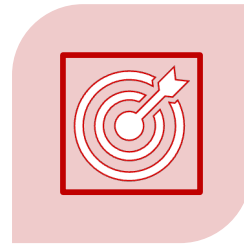
Agenda

PROGRAM INTRO

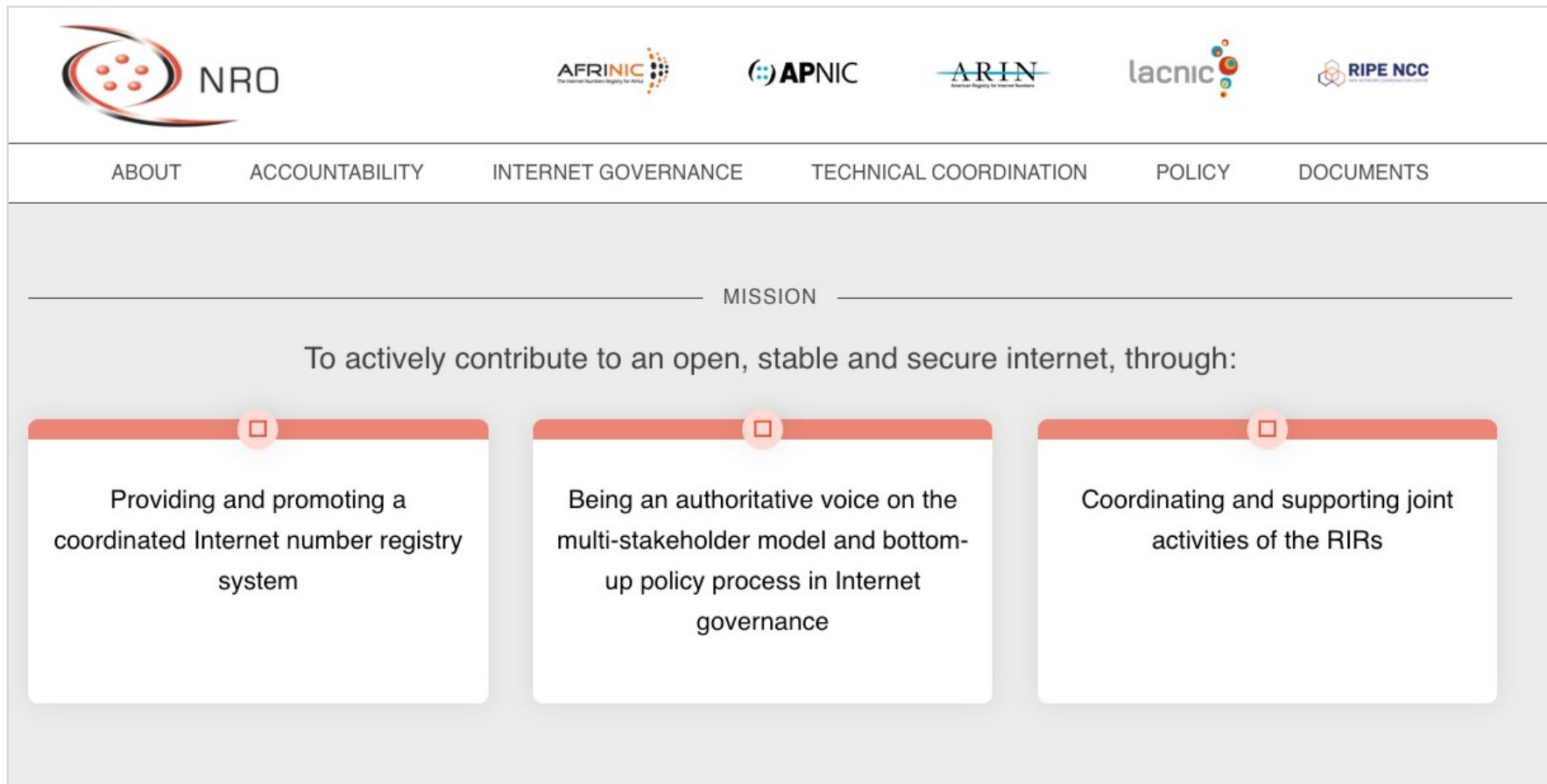PROGRAM TEAM

WHAT DO WE WANT TO ACHIEVE?

LEARN MORE AND GET IN TOUCH

What's the NRO?

Number Resource Organization

NRО | AFRINIC | APNIC | ARIN | lacnic | RIPE NCC

ABOUT   ACCOUNTABILITY   INTERNET GOVERNANCE   TECHNICAL COORDINATION   POLICY   DOCUMENTS

—— MISSION ——

To actively contribute to an open, stable and secure internet, through:

Providing and promoting a coordinated Internet number registry system

Being an authoritative voice on the multi-stakeholder model and bottom-up policy process in Internet governance

Coordinating and supporting joint activities of the RIRs

Why is RPKI important?

- RPKI = Resource Public Key Infrastructure
- Was developed to help secure global routing through **resource certificates and ROAs**
  - **Resource certificate** = Verifiable digital statement that an Internet number resource has been registered by an RIR to a holder
  - **ROA** = Route Origin Authorization, verifiable digital statement created by the resource holder to state that a given IP prefix will be originated by a specific Autonomous System

- Routers doing **Route Origin Validation** can then verify the BGP announcements they receive and make informed decisions to enhance their routing security.

Why is this program important?

- Current diversity/inconsistency among RIRs
  - Differences in RPKI related services being offered - Hosted/delegated, ROAs, AS0, etc
  - Integrations (or lack of) between RPKI and IRR services

MANRS

ABOUT   PROGRAMS

Common ROA Management Requirements and Security Standards for Operators of RPKI Services (ORS)

RIR and NIR Interactions
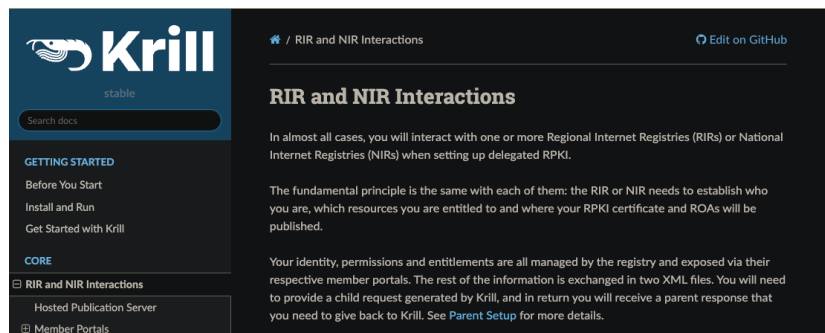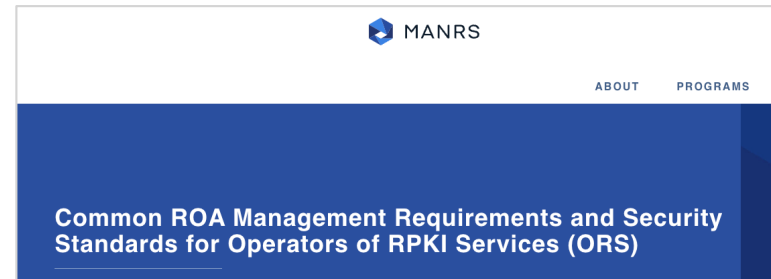
Annex I. Compliance Status of the top-level ORSs (as of July 2021)

Registry	Index		ARIN	APNIC	LACNIC	AFRINIC	RIPE
ROA Certificate	1a	Auto Renewal of a ROA	NO	YES	YES	NO	YES
	1b	Standard Validity	825d 10yr	1yr	1yr	10yr	2yr
	1c	Alerting on expiration or renewal	YES	NO	NO	NO	NO
ROA Certificate	2a	API for ROA Management	YES	NO	NO	NO	YES
	2b	API Security	NO	NO	NO	NO	NO
Infrastructure Reliability	3a	Service health Status	YES	NO	NO	NO	NO
	3b	Service health degradation notification	YES	NO	NO	NO	NO
ROA Validation	4a	Invalid subnet validation	NO	NO	NO	NO	NO
	4b	ASN change validation	NO	NO	NO	NO	NO

Sources:
https://krill.docs.nlnetlabs.nl/en/stable/parent-interactions.html
https://manrs.org/resources/common-roa-management-requirements-and-security-standards-for-operators-of-rpki-services-ors/

Are those differences hindering the adoption of RPKI?

Program Intro

NRO Strategic Review Process

- Agreement to work toward providing a robust, coordinated and secure RPKI service

The NRO RPKI Program was created

- Purpose: "**To provide a more consistent and uniformly secure, resilient and reliable RPKI service**"
- Removing barriers for RPKI adoption currently experienced by network operators who create RPKI objects through multiple RIRs.

Program Team

The **NRO EC**, as the executive sponsor of the program, with a role of strategic goal prioritisation, approval and funding.

The NRO **RPKI Program Manager**, with a role of operational direction, oversight and support

The **RPKI Steering Group**, which includes RPKI experts from the five RIRs and has a role of specific direction and advise related to agreed objectives
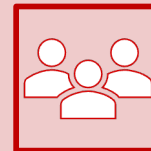
Other RIR **RPKI Subject Matter Experts** (SMEs) and consultative groups, with a role of goal delivery and execution

RPKI Steering Group

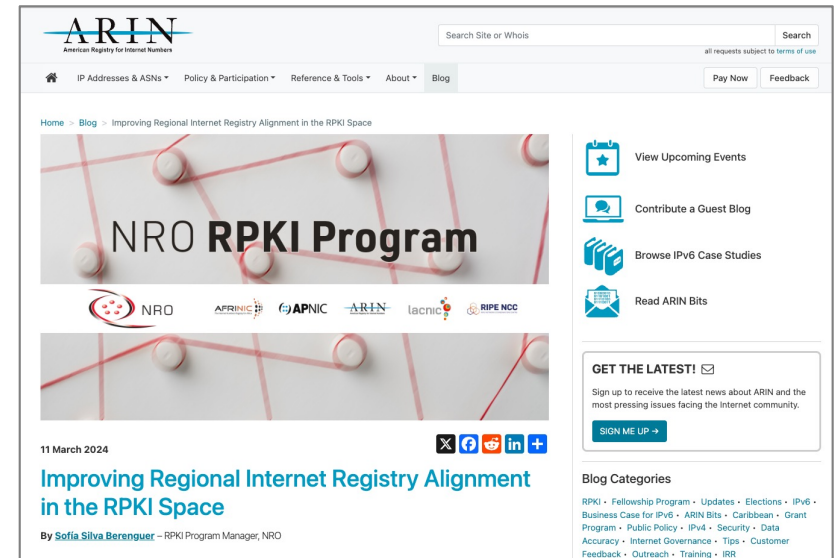| Name	Title	RIR
Yogesh Chadee	Head of Value Added Services	AFRINIC
Anton Strydom	Director, Engineering	APNIC
Tom Harrison	Product and Delivery Manager – Registry Product	APNIC
Mark Kosters	Chief Technology Officer	ARIN
Brad Gorman	Senior Product Owner, Routing Security	ARIN
Carlos Martinez Cagnazzo	Chief Technology Officer	LACNIC
Jorge Cano	Senior Software Architect	LACNIC
Felipe Victolla Silveira	Chief Technology Officer	RIPE NCC
Tim Bruijnzeels	Principal Engineer RPKI	RIPE NCC

What do we want to achieve?

- Purpose: "To provide a more consistent and uniformly secure, resilient and reliable RPKI service"

- More specifically, we want to achieve the following **outcomes**:
  - Definition of what a **single global RPKI system** looks like.
  - Better **understanding** and improved **transparency of the robustness** of the RPKI system
  - **Enhanced security consistency** of the RPKI system across the different RIRs
  - The technical community is kept **informed and engaged** throughout the program, and their **concerns are addressed in a coordinated way**.

Different aspects of consistency

- Consistency across RIRs:
  - In services/features offered
  - In mechanism to manage ROAs (create, read, update and delete)
  - In terms of robustness of the system

- What other aspects of consistency do you think we should consider?

Do you want to know more?

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

- Read our blog series:
  - https://www.arin.net/blog/2024/03/11/improving-rir-alignment-rpki/
  - https://www.arin.net/blog/2024/05/15/nro-rpki-program-series-2/

We want to hear from you!

- 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?

- Please share them sending an email to **rpki_program@nro.net**

THANKS FOR YOUR ATTENTION!