



Implementing RPKI-based  
origin validation one  
country at a time.

The Ecuadorian case study.

**IETF 89**

**LONDRES**

**MARCH 2014**

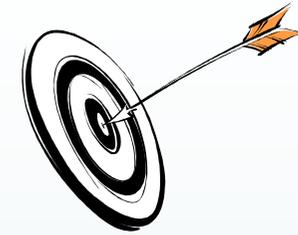
**Fabián Mejía**

# Why and who?

- ▶ BGP origin validation based on RPKI is in early stages of deployment. It is necessary to create a success story that brings enough value to both: network operators and resource holders.
- ▶ Multistakeholder Project: CISCO, LACNIC and APROVI.



# ABSTRACT



I-D: draft-fmejia-opsec-origin-a-country-00.txt

- One possible deployment strategy for BGP origin validation based on the Resource Public Key Infrastructure (RPKI) is the construction of islands of trust. This document describes the authors' experience deploying and maintaining a BGP origin validation island of trust in Ecuador.

The authors want comments from this WG.

# Roles



- ▶ **POLICER NETWORK:** NAP.EC ([www.nap.ec](http://www.nap.ec)). IXP in Ecuador (UIO and GYE). Mandatory multilateral routing policy. AEPROVI manages the NAP.EC infrastructure.



- ▶ **RESOURCE HOLDERS:** a number of holders, including organizations like ISP, content providers, universities, .ec domain and root servers administrators. Local and foreign organizations.

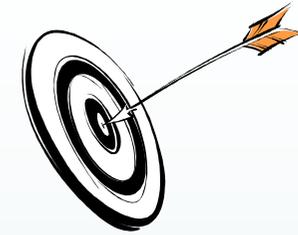


- ▶ **RPKI CAs AND REPOSITORY:** The LACNIC-hosted RPKI CA model was used for this project.



- ▶ **TECHNICAL SUPPORT:** To involve trained people and train new ones is very important. Cisco and LACNIC staff collaborated.

# Objective



- ▶ "Deploy RPKI-based BGP origin validation in NAP.EC's route servers. For the success of the project, 80% of the Ecuadorian prefixes (both IPv4 and IPv6) received by those routers should have a valid origin."
- ▶ NAP.EC - GYE was taken as reference (because NAP.EC - UIO had non-Ecuadorian prefixes announced).

# Planning

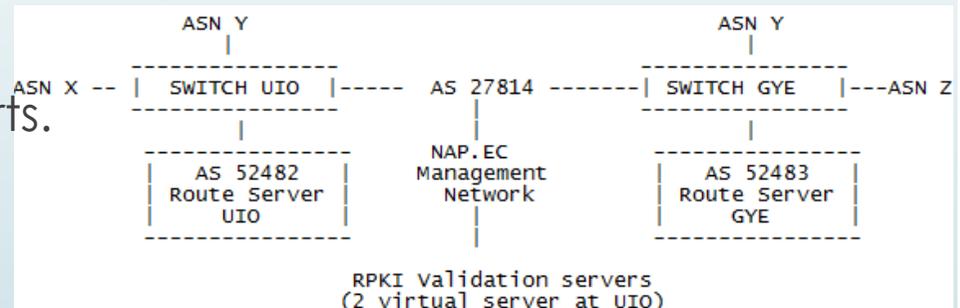


- ▶ Discussion points:
  1. RPKI-based origin validation support in the route-servers equipments
  2. How to deploy a RPKI cache into the Network
  3. How to populate the RPKI database with the correct and necessary information
  4. Action to take with NotFound and Invalid prefixes
- ▶ About 3: It was decided to organize an event with two objectives: training and RPKI object signing.
- ▶ Communication strategy should not be overlooked.

# Deployment

## RPKI Validation servers

- ▶ Two VMs running GNU Linux.
- ▶ VMs are within management AS and access to Internet and both NAP.EC locations (UIO , GYE).
- ▶ Each VM runs 2 validating software: from RIPE and rpknet project.
- ▶ Different service ports.



## Origin validation setting

- ▶ At the beginning, no action: marking each prefix with a BGP community based on its RPKI origin state.
- ▶ Some months later: dropping Invalid prefixes and setting a lower local preference for NotFound prefixes.

# Training and RPKI signing event

- ▶ Key planning activity: to create the list of participants and to make sure that at least one participant per network had the authentication credentials to create its RPKI signed objects.
- ▶ Target community: Ecuadorian organizations that had received IP resources from LACNIC until mid-2013.
- ▶ The attendance represented around 80% of the target prefixes.
- ▶ Two days event. Theoretical and practical training.
- ▶ Time slots to sign RPKI objects: at the end of the first day and during the second day.
- ▶ Feedback before closing the event: applying an acceptable policy in order do not waste the successful effort.



# Outcome and post-event activities



- ▶ Ecuadorian prefixes with RPKI origin state as Valid:
  - ❑ Less 1% before the event.
  - ❑ Less than 20% at the start of the second day,
  - ❑ Around 80% at the end of the event.
  - ❑ Almost 100% a few days after the event, after to contact some non-attending organizations.
- ▶ After, some communication activities were performed.
- ▶ Overall, management has been simple and without major problems.

# Lessons learned and best practices



- Implementation support needs to be verified in all target platforms.
- The resource holders community need RPKI-based origin validation training.
- Two days event is a better practice. The participants may not be confident about their skills at the end of the first day or may need further authorization.
- Initial work to have the "right people" in the room is a key to success.
- Operators are less conservative than original though by organizers.
- When a new ISP wants to join NAP.EC, it receives information about RPKI-based origin validation and it is invited to create its ROAs.
- The event was a great opportunity to assemble the local community.
- Post event communication needs to be discussed ahead of time.

# IMPACT – LAC REGION

**JULY 2013**

RIR	Total	Valid	Invalid	Unknown	RPKI Adoption Rate
LACNIC	56294 (100%)	5561 (9.88%)	1184 (2.1%)	49549 (88.02%)	11.98%

**OCTOBER 2013**

RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
LACNIC	61506 (100%)	11336 (18.43%)	1109 (1.8%)	49061 (79.77%)	91.09%	20.23%

Fuente: <http://rpki.surfnet.nl/perrir.html>

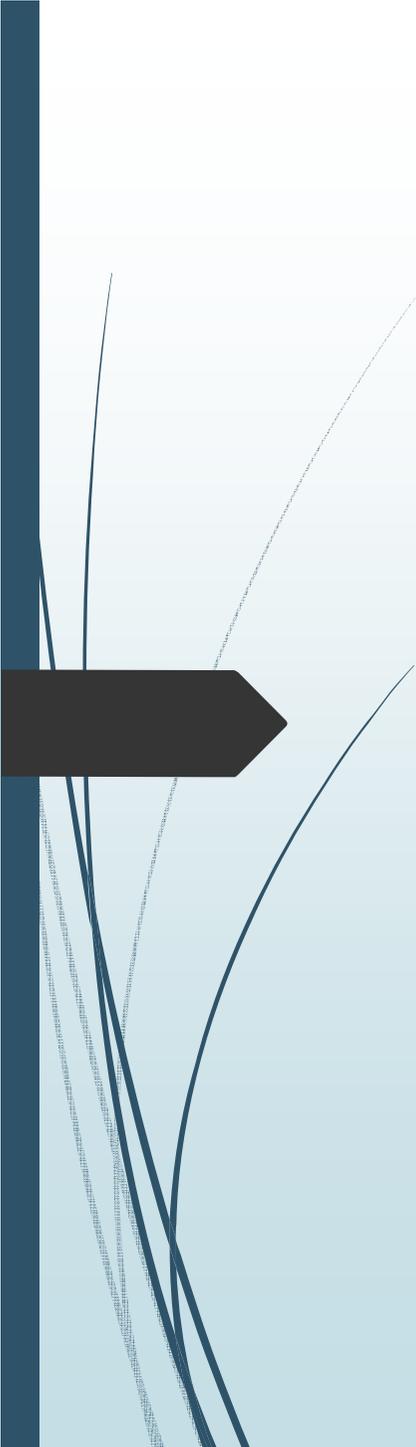
# IMPACT – COMPARATIVE

OCTOBER 2013

10 records per page Search:

RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
AFRINIC	11281 (100%)	41 (0.36%)	42 (0.37%)	11198 (99.26%)	49.4%	0.74%
APNIC	118423 (100%)	162 (0.14%)	236 (0.2%)	118025 (99.66%)	40.7%	0.34%
ARIN	186884 (100%)	649 (0.35%)	91 (0.05%)	186144 (99.6%)	87.7%	0.4%
LACNIC	61506 (100%)	11336 (18.43%)	1109 (1.8%)	49061 (79.77%)	91.09%	20.23%
RIPE NCC	131666 (100%)	7515 (5.71%)	1133 (0.86%)	123018 (93.43%)	86.9%	6.57%

Fuente: <http://rpki.surfnet.nl/perrir.html>



# Thanks

Fabián Mejía  
NAP.EC Administrator  
[fabian@aprovi.org.ec](mailto:fabian@aprovi.org.ec)