

# Cleaning up your RPKI invalids

Elly Tawhai  
PacNOG 31  
elly@apnic.net

# What is RPKI?

A robust security framework for verifying the association between **resource holders** and their **Internet number resources**.



# Route Origin Authorization

What is contained in a ROA?

- The AS number you have authorized
- The prefix that is being originated from it
- The most specific prefix (maximum length) that the AS may announce

For example: "ISP 4 permits AS65551 to originate a route for the prefix 198.51.100.0/24"



# Route Origin Validation

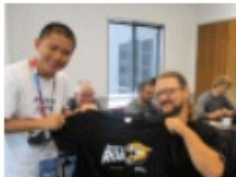
- **Valid**
  - The prefix (prefix length) and AS pair found in the database
- **Invalid**
  - Prefix is found, but origin-AS is wrong, OR
  - The prefix length is longer than the maximum length

# Route Origin Validation

NAME	TYPE	DETAILS	STATUS ▲
Lumen	transit	signed + filtering	safe
Arelion (Formally Telia)	transit	signed + filtering	safe
Cogent	transit	signed + filtering	safe
NTT	transit	signed + filtering	safe
Hurricane Electric	transit	signed + filtering	safe
GTT	transit	signed + filtering	safe
TATA	transit	signed + filtering	safe
PCCW	transit	signed + filtering	safe
RETN	transit	partially signed + filtering	safe
Orange	transit	signed + filtering	safe
Telefonica/Telixius	transit	signed + filtering	safe
Comcast	ISP	signed + filtering	safe
Liberty Global	transit	signed + filtering	safe
Cloudflare	cloud	signed + filtering	safe
Microsoft	cloud	signed + filtering	safe
Amazon	cloud	signed + filtering	safe
Netflix	cloud	signed + filtering	safe
Wikimedia Foundation	cloud	signed + filtering	safe
Scaleway	cloud	signed + filtering	safe
Telstra International	transit	signed	partially safe
AT&T	ISP	signed + filtering peers only	partially safe
Google	cloud	signed	partially safe
DigitalOcean	cloud	filtering peers only	partially safe

<https://isbgpsafeyet.com/>

# RPKI invalids



## Rise of the invalids

By Tashi Phuntsho on 10 Apr 2020



## RPKI invalids are not going away

By Md Abdul Awal on 16 Jul 2021



## Solo effort to clean up RPKI invalids across a region

By Peter Peele on 26 Jul 2021

# RPKI invalids

Validation result	IPv4 count
Invalid origin ASN	305
Invalid origin ASN and Max Length	138
Invalid Max Length	1333

Routeviews collector SG and Routunator

# RPKI invalids in Vanuatu

Validation result	IPv4 count
Invalid origin ASN	-
Invalid origin ASN and Max Length	-
Invalid Max Length	1



# RPKI invalids

Origin ASN	AS Name	Economy	No. of invalid routes
AS9249	VUTELECOM-AS01-VU-APC	VU	1

# ROA Prevalidation

### Add new ✕

**Prefix**

**Origin AS**

**Max length**

**ROA**  Enabled (ROAs will be created for this route)

**Whois**  Enabled (Whois route objects will be created for this route)  
 Define Whois route attributes

**Options**  Notify additional contacts

# ROA Prevalidation

- Validate changes submitted via MyAPNIC to ensure that they won't cause problems in BGP
- Allows Members to override if necessary

**Pending Queue** ×

**⚠ BGP validation warning:** If the requested changes are made, the following BGP announcements will become "not found" or/and "invalid".  
Are you sure you want to commit these changes?

BGP Prefix	BGP Origin AS	Current RPKI Status	New RPKI Status
202.125.96.0/24	AS45192	VALID	INVALID

Previous **1** Next

Back Yes, commit changes

# Routing status alerts in DASH

## Overview of inconsistencies

Total inconsistencies found

3

Status of ROAs and route objects as seen in BGP:

● ROA mismatches

3

[View prefixes](#) ▾

● Route object mismatches

0

## Routing status for my prefixes

Show 20 entries ▾

Search by prefix or ASN 🔍

Filter by:  ROA issues  Route object issues



Prefix ▾	BGP Route ▾	Origin AS ▾	ROA ▾	Route Object ▾
103.21.244.0/22	103.21.244.0/24	AS13335	● Mismatch <a href="#">+ info</a>	● Not Published
103.21.244.0/22	103.21.244.14/32	AS11708	● Mismatch <a href="#">+ info</a>	● Not Published
103.21.244.0/22	103.21.244.15/32	AS11708	● Mismatch <a href="#">+ info</a>	● Not Published

<https://dash.apnic.net/>

# Routing status alerts in DASH

## ROA mismatch for 103.21.244.0/24



**Reason:** The prefix length seen in BGP does not match with the ROA maxlength.

Length in **BGP**: /24      Scope in **ROA** ⓘ : /23 - /23 (103.21.244.0/23 - AS0)

### Required actions:

- If you did not expect a route with this length, review your routing configuration to evaluate if there is a misconfiguration or a BGP prefix hijack. [Learn more about BGP hijacking.](#) ▼
- If you did not expect this max length, review the ROAs for this prefix.

Close

# ROA alert filters in DASH

### Create alert

Define filter >

Define trigger >

Define action >

Name alert >

**Filter**

Select trigger filter type (Prefix or Origin AS):

Prefix     Origin AS

**Prefix**

- Any prefix announced by my Origin ASes
- All prefixes delegated to my account
- Select individual prefixes

Next

### Create alert

Define filter >

Define trigger >

Define notification >

Name alert >

**Filter**

Select trigger filter type (Prefix or Origin AS):

Prefix     Origin AS

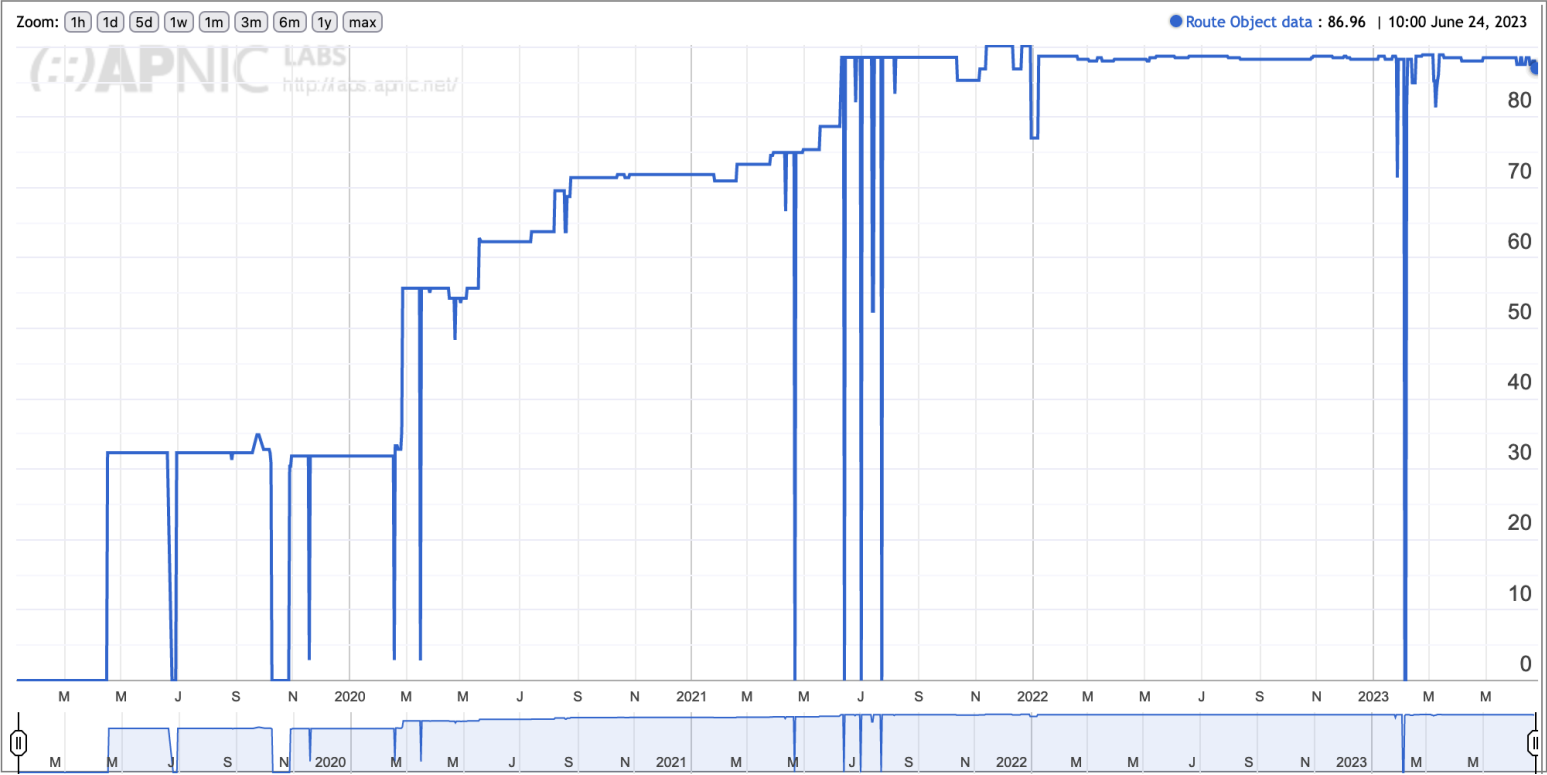
**Origin AS**

- All Origin AS delegated to my account.
- Select individual Origin ASes.

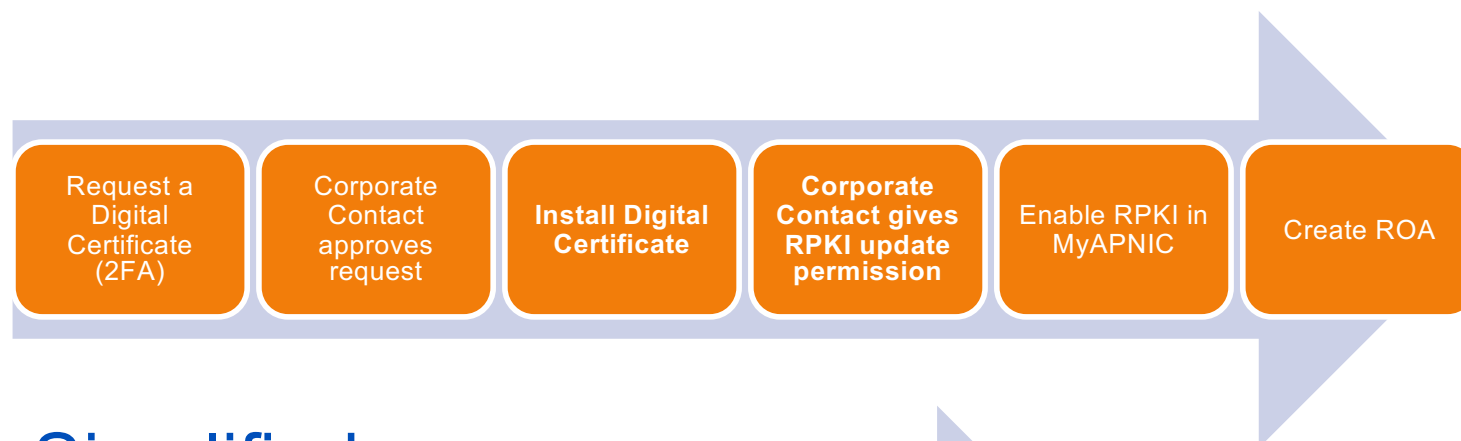
Next

# ROA coverage – Vanuatu

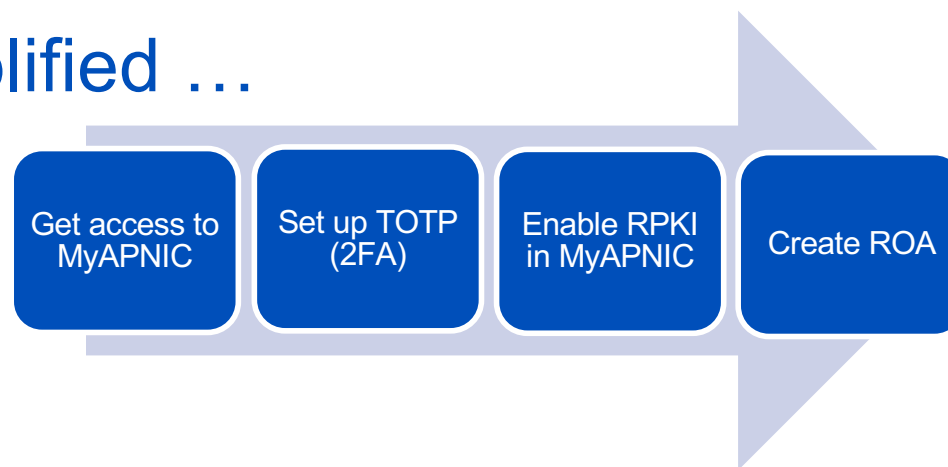
Display: Addresses (Advertised ROA-Valid Advertised Addresses), IPv4, Percent (of Total)



# Access to RPKI



## Simplified ...





# Questions?