



**RIPE NCC**

RIPE NETWORK COORDINATION CENTRE

# Developments in Routing Security

Oleg Muravskiy

4 June 2019 | ENOG 16

# Who We Are



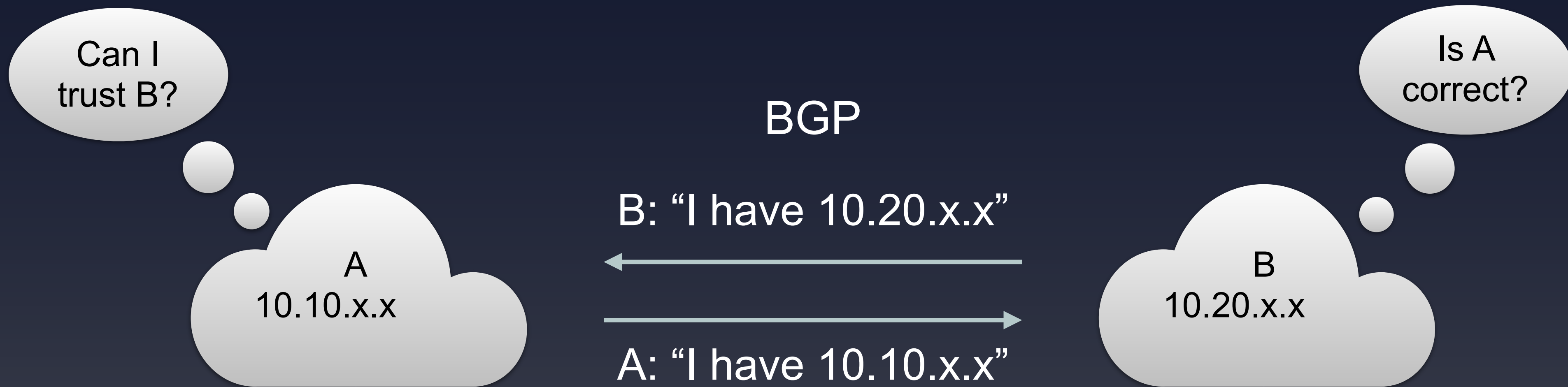
- **We manage IP and ASN allocations in Europe, the Middle East and parts of Central Asia**
  - Ensure unique holdership
  - Document holdership in the RIPE Database (whois)
  - Enable operators to document use of their address space

# Routing Security is in Our DNA



- In 1994, RIPE-181 was the first document published that used a common language to describe routing policies
- We co-developed standards for IRR and RPKI
- We are one of the five RPKI Trust Anchors
- Our Validator tool was the first tool to do Origin Validation

# Routing on the Internet



# Incidents Are Common



- **2017 Routing Security Review by the Internet Society**
  - 14k incidents
  - 10% of all ASes affected
    - 3k ASNs victims of at least one incident
    - 1.5k ASNs caused at least one incident

# Or Worse...

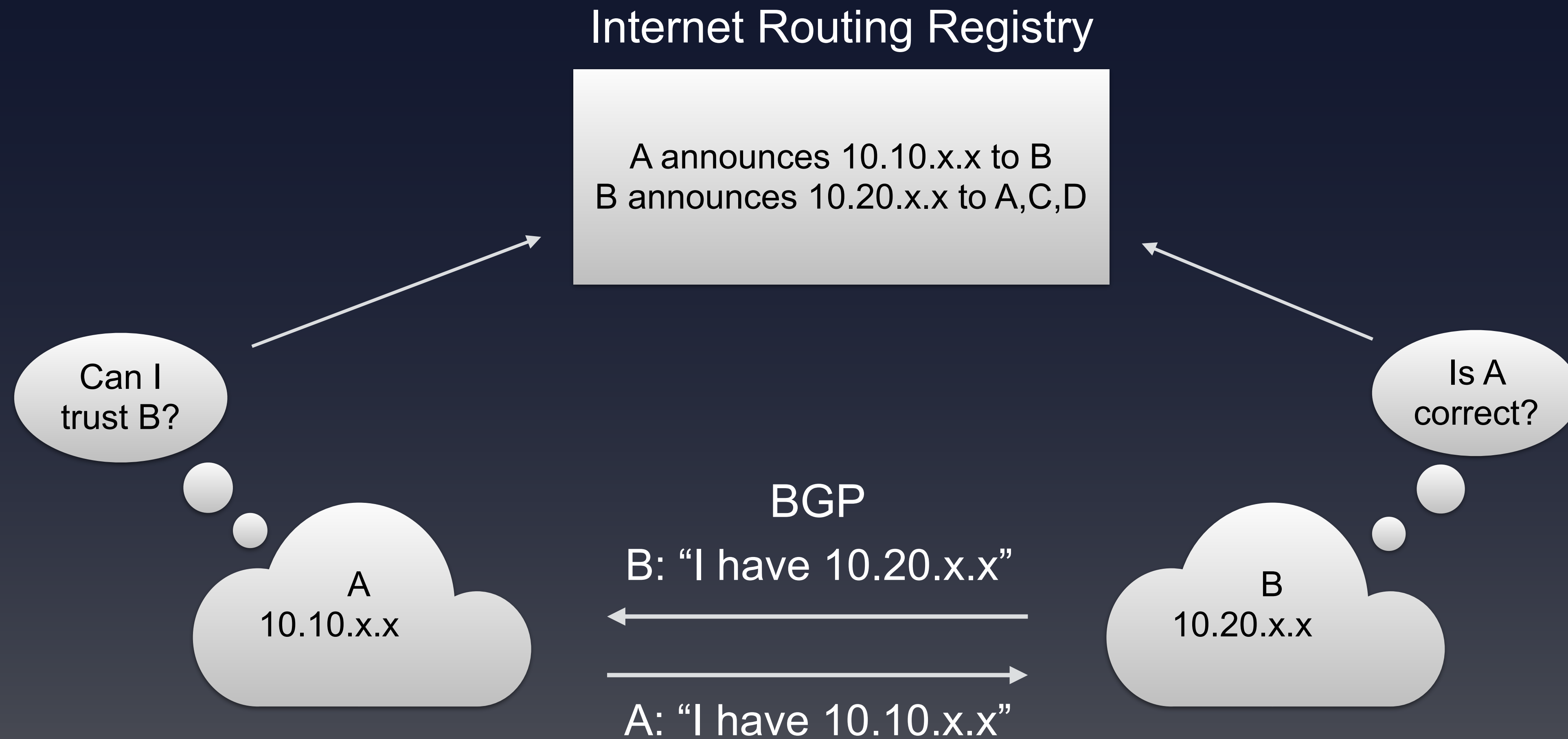


- April 2018
  - BGP and DNS hijack targeting Amazon and MyEtherWallet.com
- August 2018
  - Same technique used against several payment systems





# How to Secure Routing?



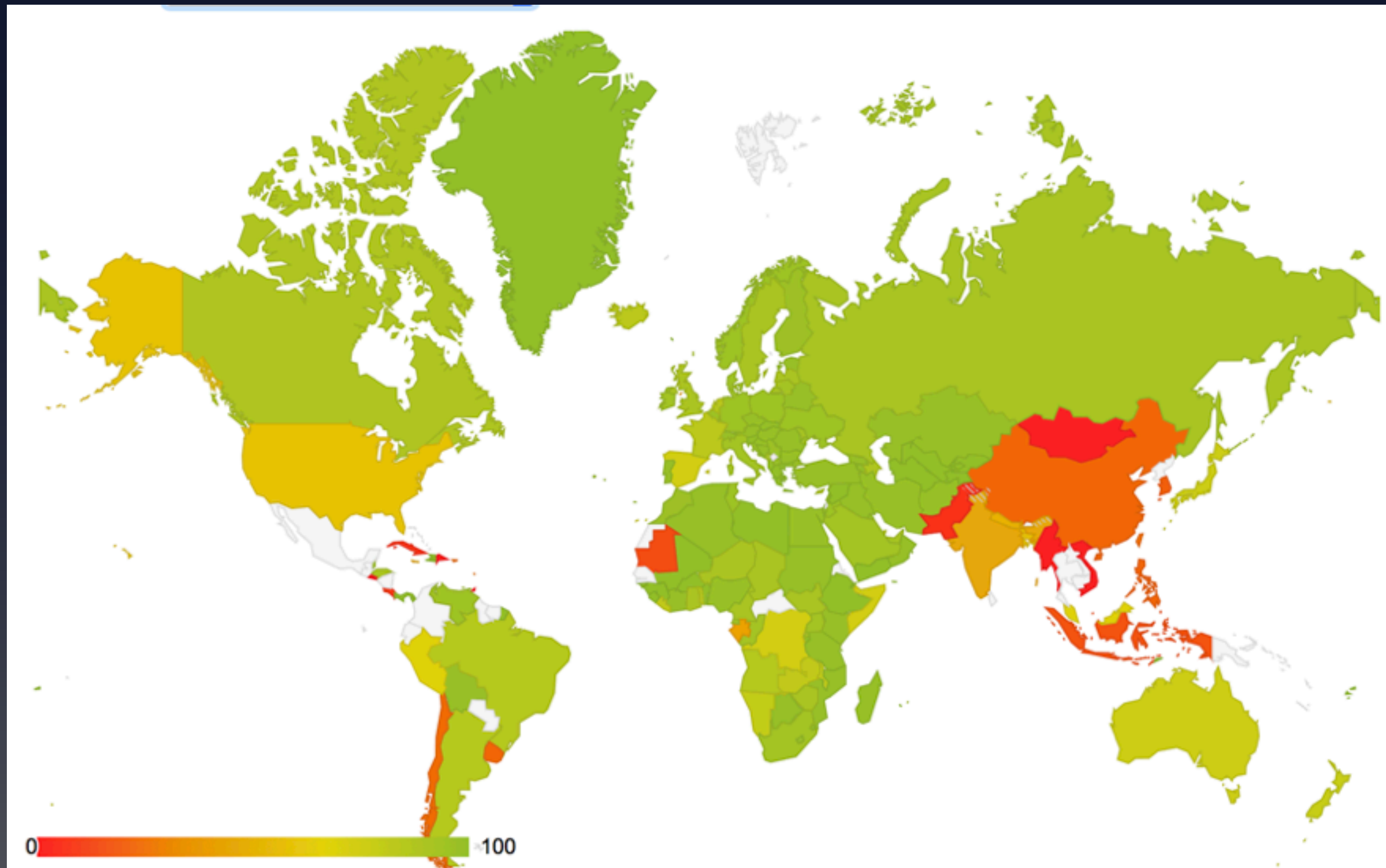
# Internet Routing Registry (IRR)



- IRRs exist for many years
- RIPE DB, NTTCOM, RADB, ALTDB, ARIN IRR, BBOI, BELL, LEVEL3, RGNET, TC, CANARIE, ...
- But their accuracy is not great
  - The RIPE Database verifies holdership for the RIPE region resources only
  - The RADB allows paying customers to create any object
  - Many IRRs do not formally verify holdership

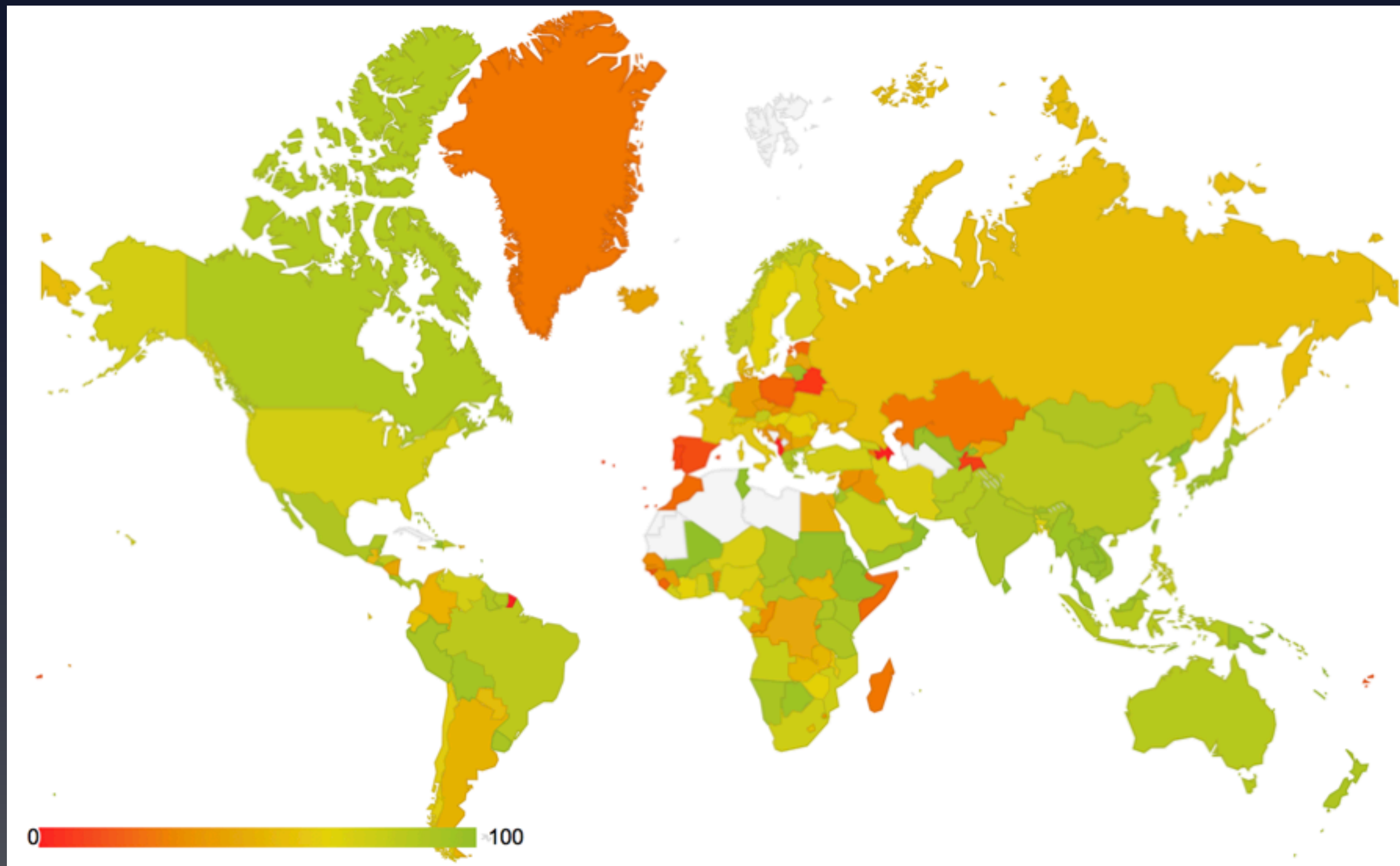


# Accuracy – RIPE DB IRR



Valid announcements / covered announcements

# Accuracy – RADB IRR



Valid announcements / covered announcements

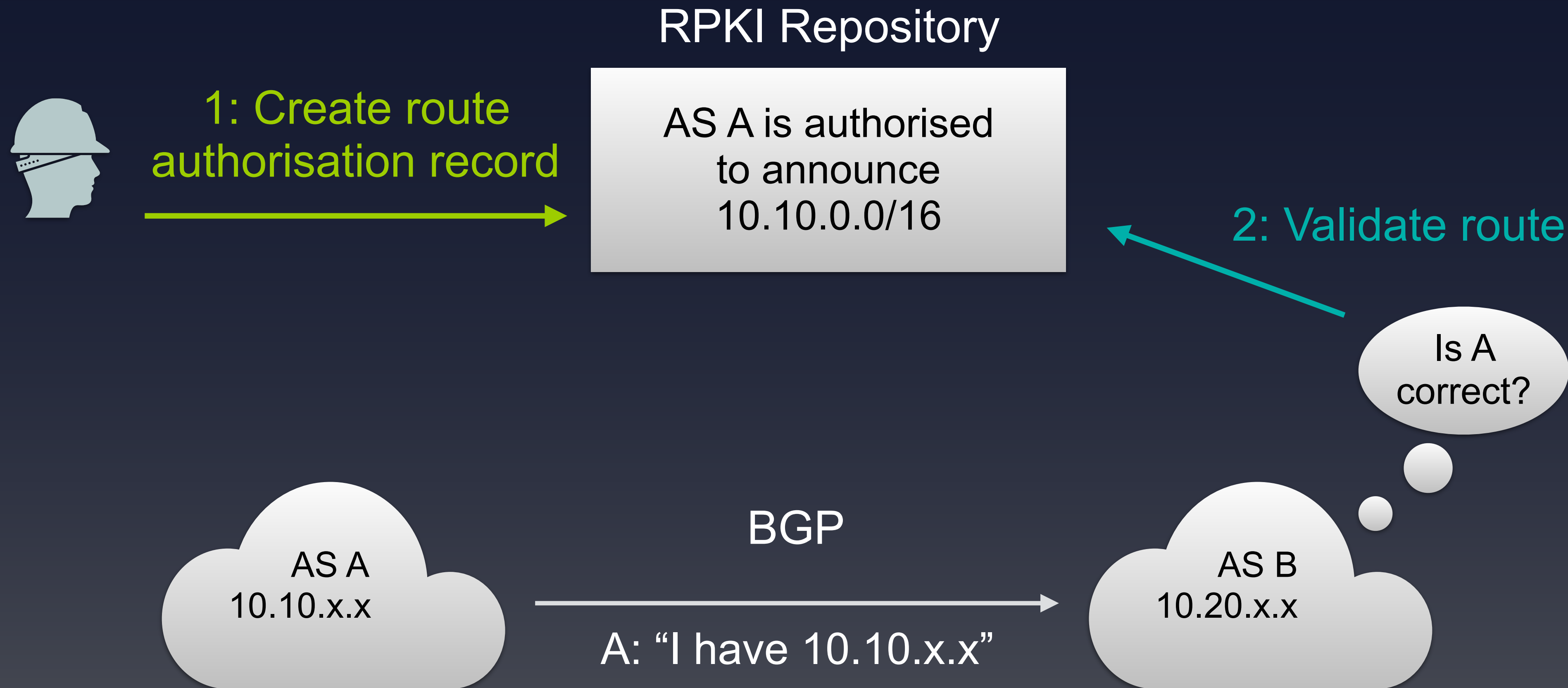
# Resource Public Key Infrastructure (RPKI)



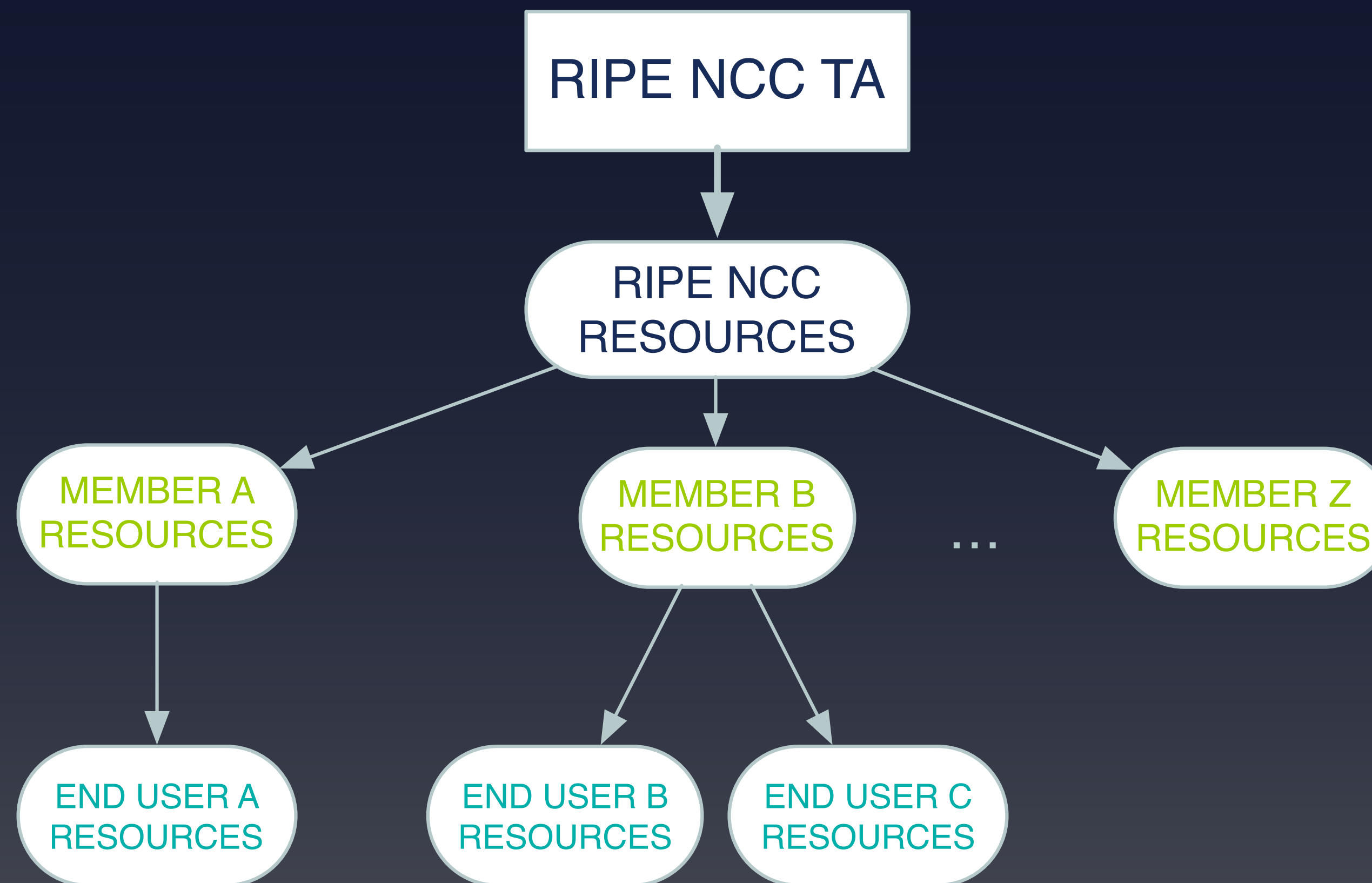
- **Ties IP addresses and ASNs to digital certificates (X.509)**
- **Digitally sign statements from resource holders**
  - AS X is authorised to announce my IP prefix Y
  - Signed by the holder of Y
- **Operated since 2011 by all RIRs**
- **Supported by IETF standards**



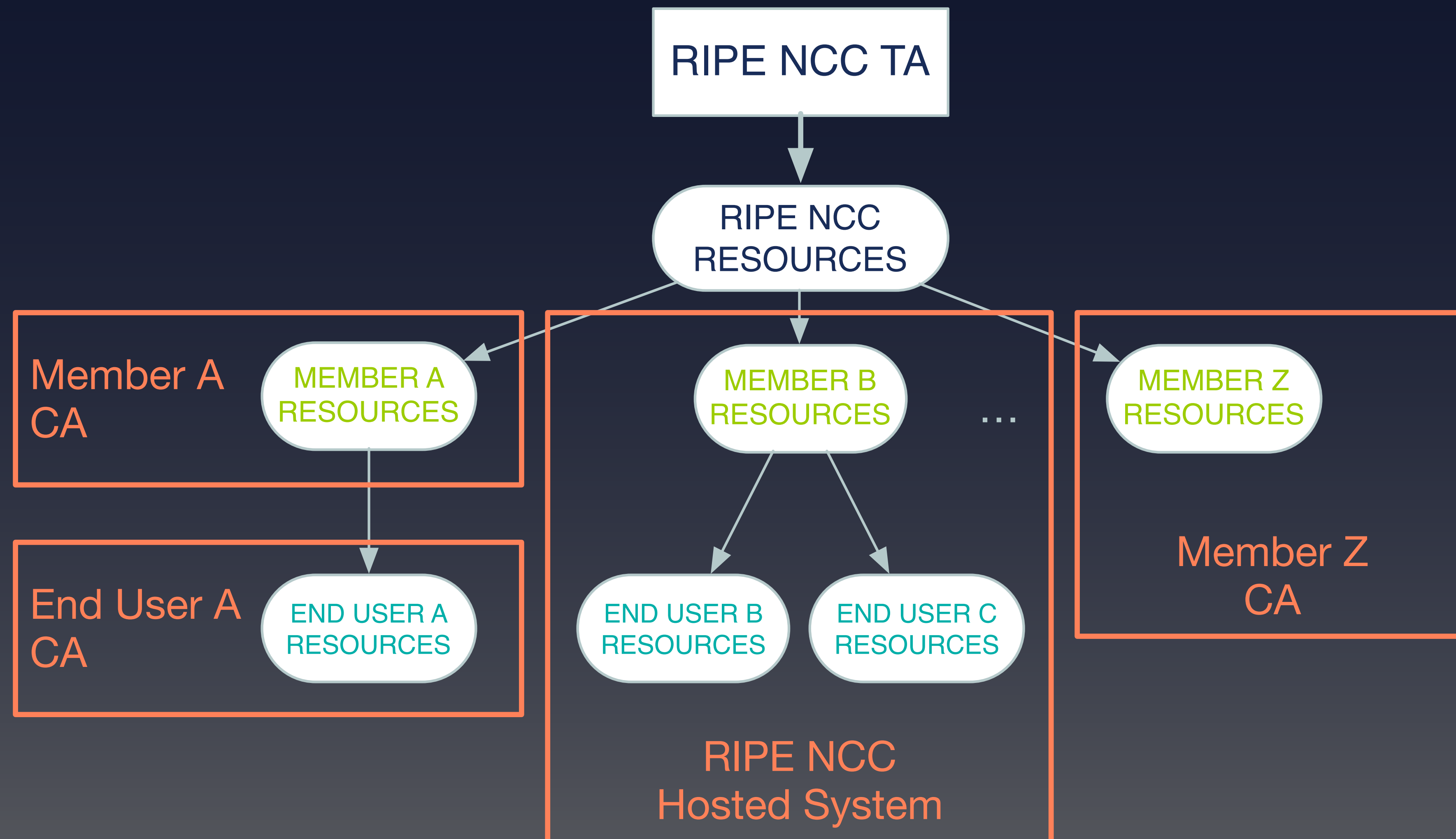
# RPKI Needs Two Actions



# Creating RPKI Objects: Certificate Hierarchy



# Creating RPKI Objects: Hosted vs Non-Hosted





# Creating RPKI Objects: Running Non-Hosted CA



- **Install RPKI CA software**
  - Dragon Research Labs, [rpki.net](http://rpki.net) RPKI toolkit
  - NLnet Labs Krill
- **Enable non-hosted CA on LIR Portal**
- **Setup connection with RIPE NCC CA**

# Enable Non-Hosted CA on the LIR Portal



The screenshot shows the RIPE NCC LIR Portal at the URL <https://my.ripe.net/#/provisioning>. The page title is "Create a Certificate Authority". The main content area displays the "RIPE NCC Certification Service Terms and Conditions" and the "Introduction" section. Below the terms, there is a section titled "Article 1 – Definitions" and a "Type of Certificate Authority" section with two radio buttons: "Hosted" and "Non-Hosted". The "Non-Hosted" option is selected. At the bottom of the form, there is a button labeled "I accept. Create my Certificate Authority". A large blue arrow points from the "Resources" menu item in the left sidebar to the "Non-Hosted" radio button.

RIPE NCC  
RIPE NETWORK COORDINATION CENTRE

RIPE Database (Whois) Website

Search the content of this website

Manage IPs and ASNs > Analyse > Participate > Get Support > Publications > About Us >

You are here: Home > Manage IPs and ASNs > LIR Portal

You are editing

My Account >

Resources >

My Resources

Sponsored Resources

Request Resources

Request Transfer

IPv4 Transfer Listing Service

[RPKI Dashboard](#)

RIPE Database >

Create a Certificate Authority

RIPE NCC Certification Service Terms and Conditions

Introduction

This document will stipulate the Terms and Conditions for the RIPE NCC Certification Service. The RIPE NCC Certification Service is based on Internet Engineering Task Force (IETF) standards, in particular RFC3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC3779, "X.509 Extensions for IP Addresses and AS Identifiers", and the "Certificate Policy (CP) for the Resource PKI (RPKI)".

Article 1 – Definitions

In the Terms and Conditions, the following terms shall be understood to have the meanings assigned to them

Type of Certificate Authority

☐ Hosted

☒ Non-Hosted

By clicking on 'I accept' below you confirm that that you have read, understood and agree to the [RIPE NCC Certification Service Terms and Conditions](#).

[I accept. Create my Certificate Authority](#)

f t in YouTube

Home | Sitemap | Contact Us | Service Announcements | Privacy Statement | Legal | Cookies | Copyright Statement | Term of Service

# Setup Connection With the RIPE NCC CA



A screenshot of the RIPE NCC website's provisioning interface. The browser address bar shows 'https://my.ripe.net/#/provisioning/non-hosted'. The page header includes the RIPE NCC logo and a search bar. A navigation menu at the top contains links like 'Manage IPs and ASNs', 'Analyse', 'Participate', 'Get Support', 'Publications', and 'About Us'. The main content area is titled 'Create a Certificate Authority' and prompts the user to 'Please upload the identity xml file generated on your client.' with a 'Choose file' button and an 'Upload' button. A sidebar on the left lists various resources and account management options. The footer contains social media icons and a list of links including 'Home', 'Sitemap', 'Contact Us', 'Service Announcements', 'Privacy Statement', 'Legal', 'Cookies', 'Copyright Statement', and 'Term of Service'.

# Setup Connection With the RIPE NCC CA



Browser address bar: <https://my.ripe.net/#/rpki>

RIPE NCC  
RIPE NETWORK COORDINATION CENTRE

RIPE Database (Whois) Website

Search the content of this website

Manage IPs and ASNs > Analyse > Participate > Get Support > Publications > About Us >

You are here: [Home](#) > [Manage IPs and ASNs](#) > LIR Portal

You are editing

My Account >

Resources ▾

- My Resources
- Sponsored Resources
- Request Resources
- Request Transfer
- IPv4 Transfer Listing Service
- [RPKI Dashboard](#)

RIPE Database >

## Non-Hosted Certificate Authority

A valid client identity certificate was uploaded ✓

[Download this server's identity xml file \(used to configure your local Certificate Authority\)](#)

Revoke your current non-hosted Certificate Authority from this server so that you can re-initialise a new instance (can not be undone):

Revoke

f t in YouTube

Home | Sitemap | Contact Us | Service Announcements | Privacy Statement | Legal | Cookies | Copyright Statement | Term of Service

# Creating RPKI Objects: Running non-Hosted CA



- **Install RPKI CA software**
  - [Dragon Research Labs rpki.net RPKI toolkit](#)
  - [NLnet Labs Krill](#)
- **Enable non-hosted CA on LIR Portal**
- **Setup connection with RIPE NCC CA**
- **Generate your resource certificate and get it signed**
- **Create your ROA objects**
- **Publish your resource certificate and ROA objects in your RPKI repository**
- **Keep re-publishing your objects (every 24 hours) (from another AS)**



# Creating RPKI Objects: Using Hosted CA



- **Enable Hosted CA on the LIR Portal**
- **Create your ROA objects**



# Create Your ROA Objects in a Hosted CA



Manage IPs and ASNs > Analyse > Participate > Get Support > Publications > About Us >

You are here: [Home](#) > [Manage IPs and ASNs](#) > LIR Portal

You are editing:

My Account

Resources

- My Resources
- Sponsored Resources
- Request Resources
- Request Transfer
- IPv4 Transfer Listing Service
- [RPKI Dashboard](#)

RIPE Database

## RPKI Dashboard

9 CERTIFIED RESOURCES NO ALERT EMAIL CONFIGURED

### 41 BGP Announcements

4 Valid 1 Invalid 36 Unknown

### 4 ROAs

3 OK 1 Causing problems

[BGP Announcements](#) [Route Origin Authorisations \(ROAs\)](#) [History](#)

☐ Create ROAs for selected BGP Announcements ☒ Valid ☐ Invalid ☐ Unknown

<input type="checkbox"/>	Origin AS	Prefix	Current Status	
<input type="checkbox"/>	AS12654	2001:7fb:fe01::/48	UNKNOWN	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	AS12654	2001:7fb:fe0c::/48	UNKNOWN	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	AS12654	2001:7fb:fe0f::/48	UNKNOWN	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	AS12654	2001:7fb:ff00::/48	UNKNOWN	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	AS12654	2001:7fb:ff01::/48	UNKNOWN	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	AS12654	2001:7fb:ff02::/48	UNKNOWN	<input type="checkbox"/> <input type="checkbox"/>

# Create Your ROA Objects in a Hosted CA



Manage IPs and ASNs > Analyse > Participate > Get Support > Publications > About Us >

You are here: [Home](#) > [Manage IPs and ASNs](#) > LIR Portal

You are editing

My Account >

Resources ▾

- My Resources
- Sponsored Resources
- Request Resources
- Request Transfer
- IPv4 Transfer Listing Service
- [RPKI Dashboard](#)

RIPE Database >

## RPKI Dashboard

36 CERTIFIED RESOURCES NO ALERT EMAIL CONFIGURED

BGP Announcements

ROAs

☒ Valid

☐ Invalid

☐ Unknown

☒ OK

☐ Causing problems

BGP Announcements

Route Origin Authorisations (ROAs)

History

Search...

There are currently no ROAs to be shown.

☐ AS number

Prefix

Most specific length allowed

Affects

Show

25

of 0 items

Tour



# Creating RPKI Objects: Using Hosted CA



- Enable Hosted CA on LIR Portal
- Create your ROA objects
- **We will publish your objects in our RPKI repository**
- **We will keep your objects up-to-date**

45 seconds  
(if you know your  
RIPE NCC Access  
password)

# Hosted CA for PI End-Users



- By default RPKI for PI resources is managed by the sponsoring LIR
- Your sponsoring LIR could make you a maintainer of an inetnum object for your resources in RIPE DB
- Then you could link your RIPE NCC Access account to that maintainer
- ...and enable your own RPKI CA
- Documentation

# Hosted CA for PI End-Users



Your account

Your organisation  
Linked maintainers

Authenticate

https://portal.ripe.net/rpki-enduser

RIPE NCC  
RIPE NETWORK COORDINATION CENTRE

RIPE Database (Whois) Website

Search the content of this website

o.leg@ripe.net

Manage IPs and ASNs > Analyse > Participate > Get Support > Publications > About Us >

Home > Manage IPs and ASNs > Documentation for Resource Management > Resource Certification (RPKI) > Enable RPKI for End User Resources

### Resource Certification (RPKI) for End User Resources

Enter organisation or prefix:

ORG-NCC1-RIPE / RIPE Network Coordination Center

**Maintainers**

- RIPE-NCC-RIS-MNT

**Resources**

Password for RIPE-NCC-RIS-MNT Associate

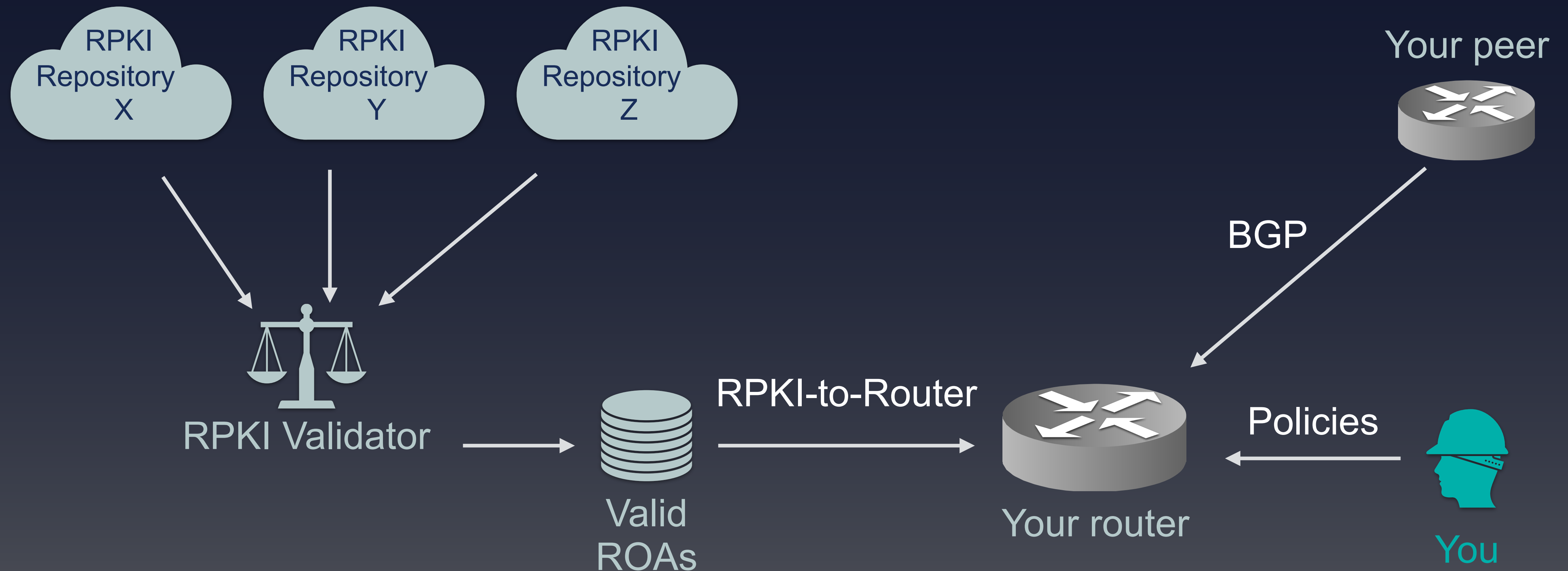
Continue to RPKI



# Routing validation



# Validating Route Announcements

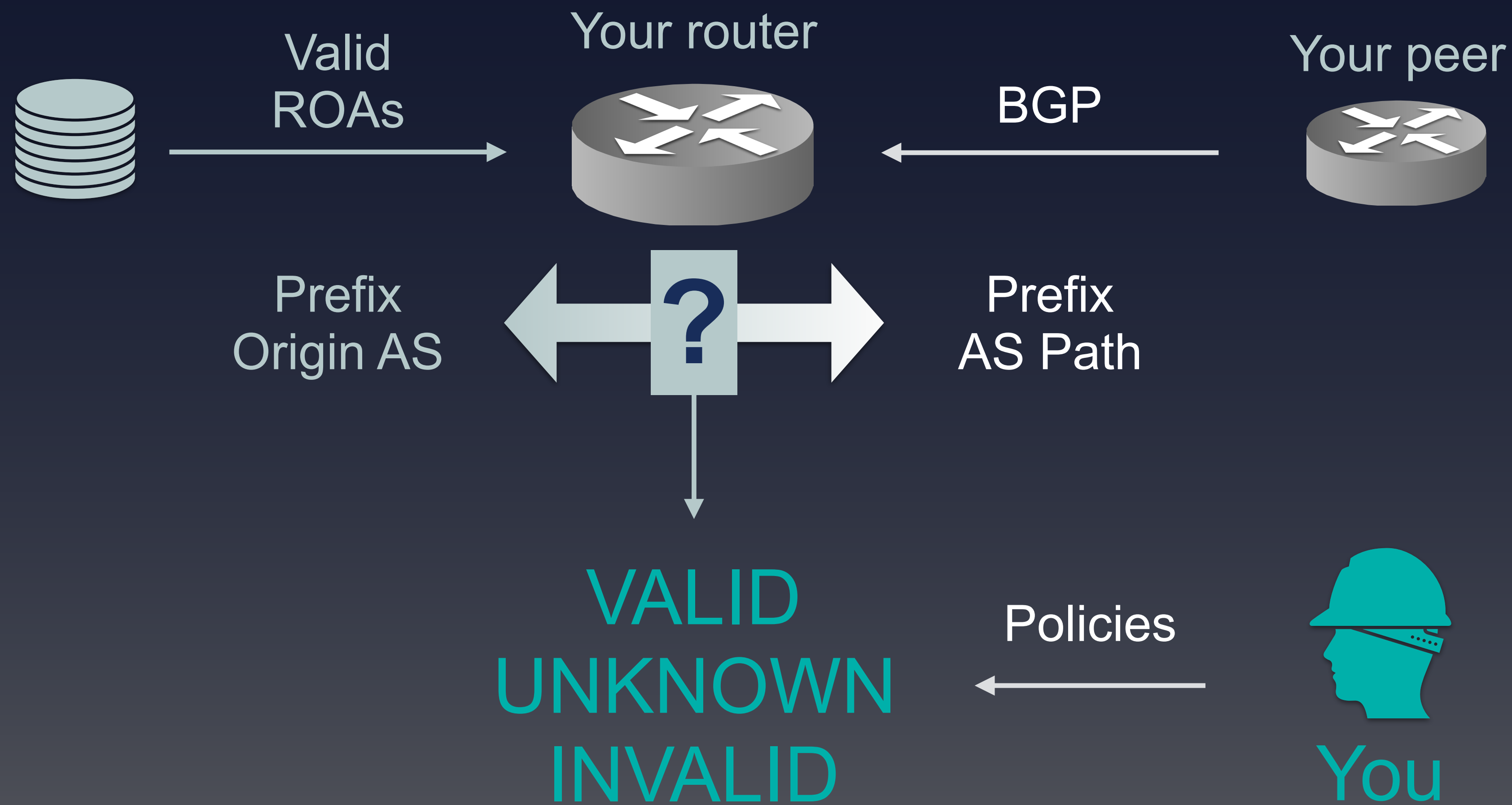


# RPKI Validators



- **RIPE NCC RPKI Validator**
  - Version 2
  - Version 3
- **Dragon Research Labs rpki.net RPKI toolkit**
- **NLnet Labs Routinator**
- **Cloudflare's OctoRPKI**

# Validating Route Announcements



# Validating Route Announcements: Policies



- Prefer **VALID** over others
- Prefer **UNKNOWN** over **INVALID**
- Drop **INVALID**?

# Invalid == reject ?



- **What breaks if you reject invalids?**
  - **“Mostly nothing” – AT&T**
  - **“5 customer calls in 6 months, all resolved quickly” – medium Dutch ISP**
  - **“Customers appreciate a provider who takes security seriously” – medium Dutch ISP**
  - **“There are many invalids, but very little traffic is impacted” – very large cloud provider**

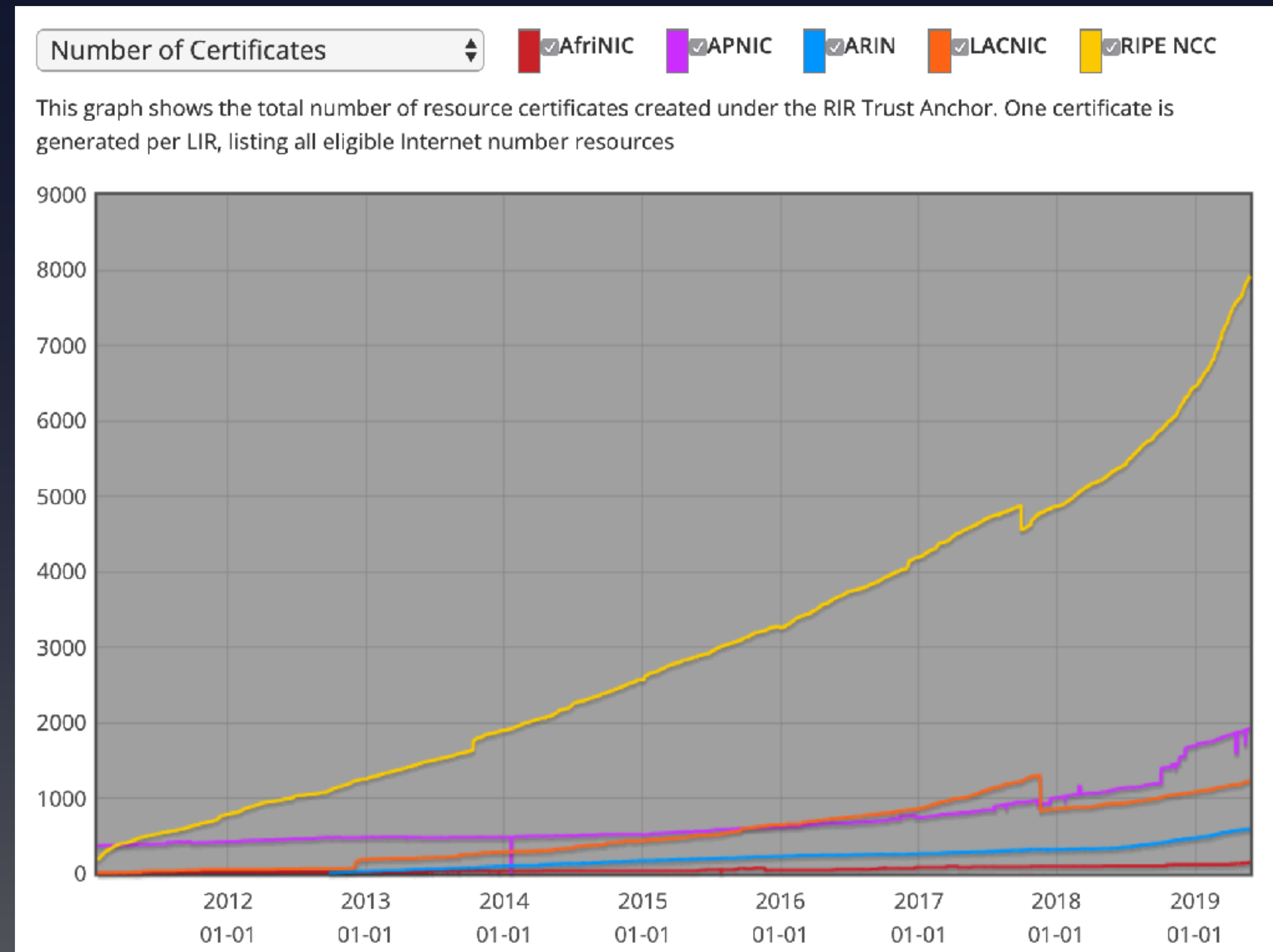
# Origin Validation vs. Path Validation



- **ROA-based validation covers only part of the problem**
- **BGPsec could solve it, but can't**
- **Autonomous System Provider Authorization (ASPA)**
  - **Work in progress**
- **Don't wait, start now**

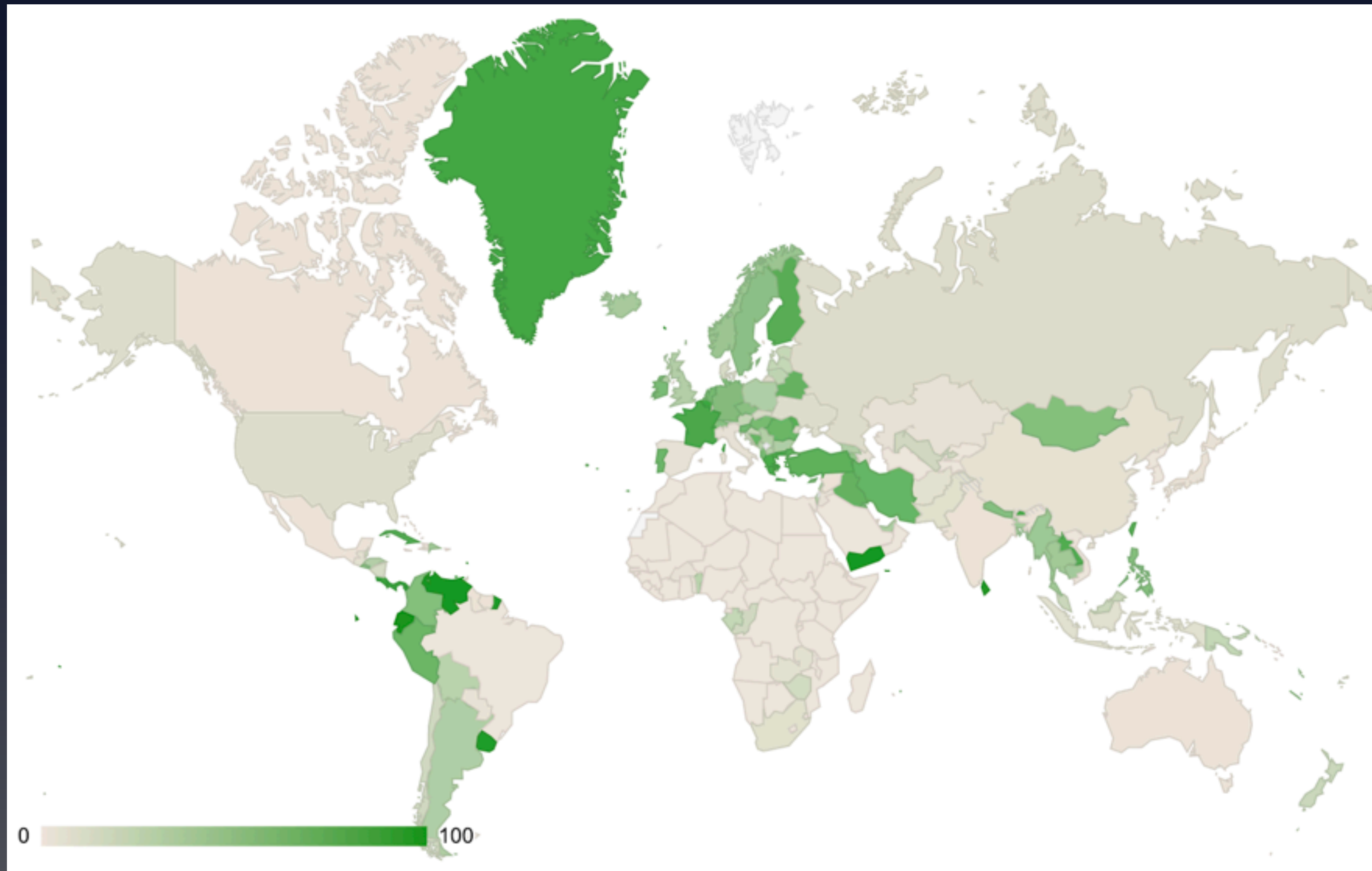


# Number of Certificates



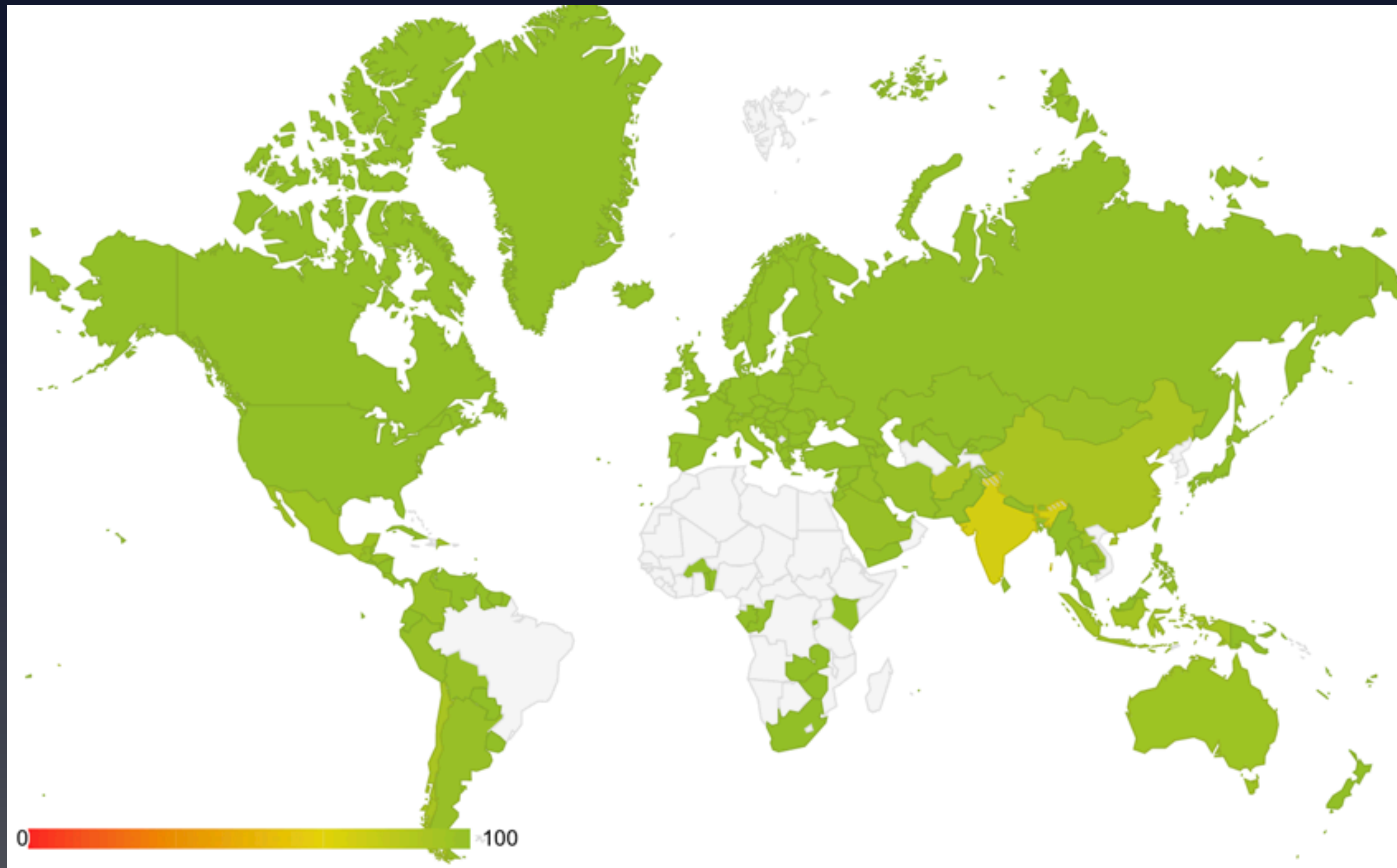
<https://certification-stats.ripe.net/>

# Coverage – RPKI (all RIRs)



<https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html>

# Accuracy – RPKI (all RIRs)



<https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html>



# RPKI in some regional countries



Country	ROA Coverage	ROA Accuracy
AM	42,83%	100%
AZ	3,25%	100%
BY	61,37%	100%
EE	19,2%	100%
GE	27,25%	100%
KG	7,05%	100%
KZ	2,35%	100%
LT	20,37%	100%
LV	24,34%	99,76%
MD	65,57%	100%
RU	7,8%	99,83%
IR	67,22%	99,15%
TR	66,91%	99,48%
TM	1,82%	100%
TJ	0%	—
UA	7,69%	99,59%
UZ	24,31%	100%

<https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html>

# Yesterday's ROA signing result



Prefix Overview (185.229.108.0/22)

Reload this widget by entering a resource here

Routing information (RIS)

- ☒ Is visible as exact match
- ☒ No more/less-specific prefixes are visible

This prefix is announced by:

AS205143 - RPKI Status: "CLOUD9 - Cloud 9 Ltd."

RIR information:

Resource	RIR	Status	Registration	Country
185.229.108.0/22	RIPE NCC	ALLOCATED	2017-10-31	GE

Show IANA Registry Information

Showing results for 185.229.108.0/22 as of 2019-06-04 00:00:00 UTC

source data embed code permalink info

# RPKI Filtering at IXPs



- **Analysis by Job Snijders / Samer Abdel-Hafez / Marty Strong: <http://peering.exposed/>**
- **9 out of top 10 IXPs already filtering**
- **Of all analysed IXPs: 68 filtering, 12 not filtering, 55 unknown**
- **Only 3 IXPs from ENOG region**

# Recommendations



- **Create Your ROAs**
  - “my network becomes safer if you implement both signing and validation”
  - Pay attention to the Max Length
- **Download a Validator, or two**
- **Check validation status manually, which routes are invalid?**
- **Set up monitoring, for example pmacct**



# Making the Difference



- **Is routing security on your agenda?**
- **Initiate the conversation with providers and colleagues**
- **Are you leading by example?**



# Questions



Email address  
@Twitter handle

---

**What can we do better for you?**

Tell us and you could win an iPad!

[www.ripe.net/survey](http://www.ripe.net/survey)

