RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Developments in Routing Security

Nathalie Trenaman | April 2019 |

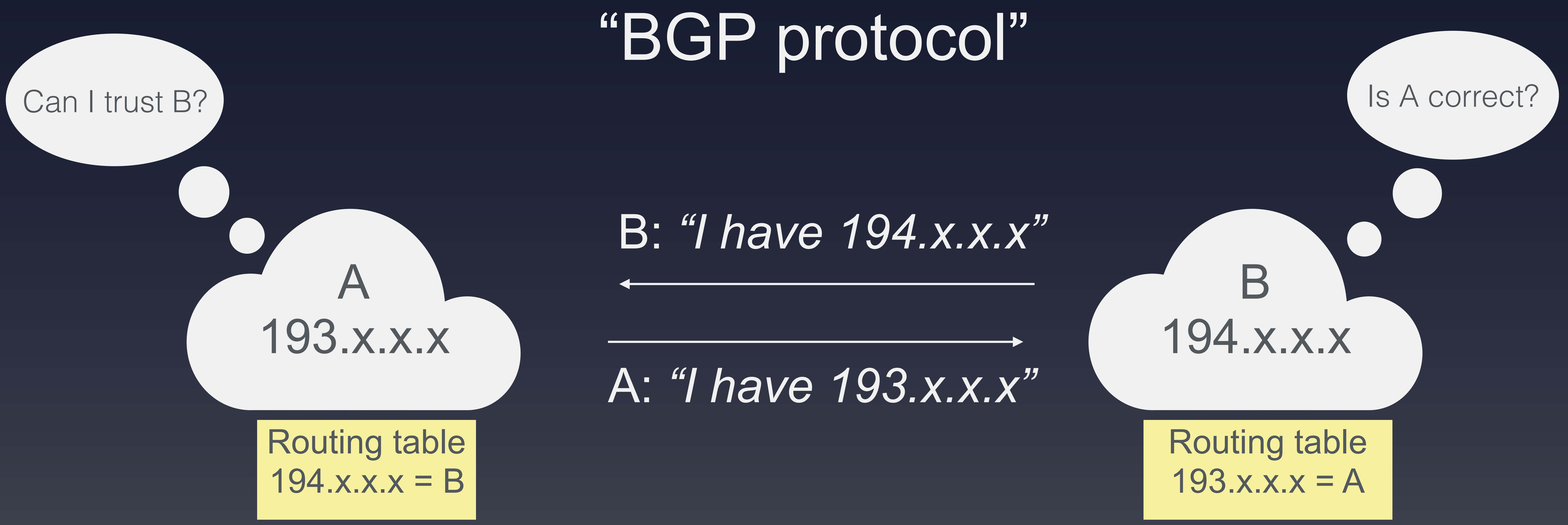
Who We Are

- 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 spaces

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, until recently, the only production-grade tool to do Origin Validation

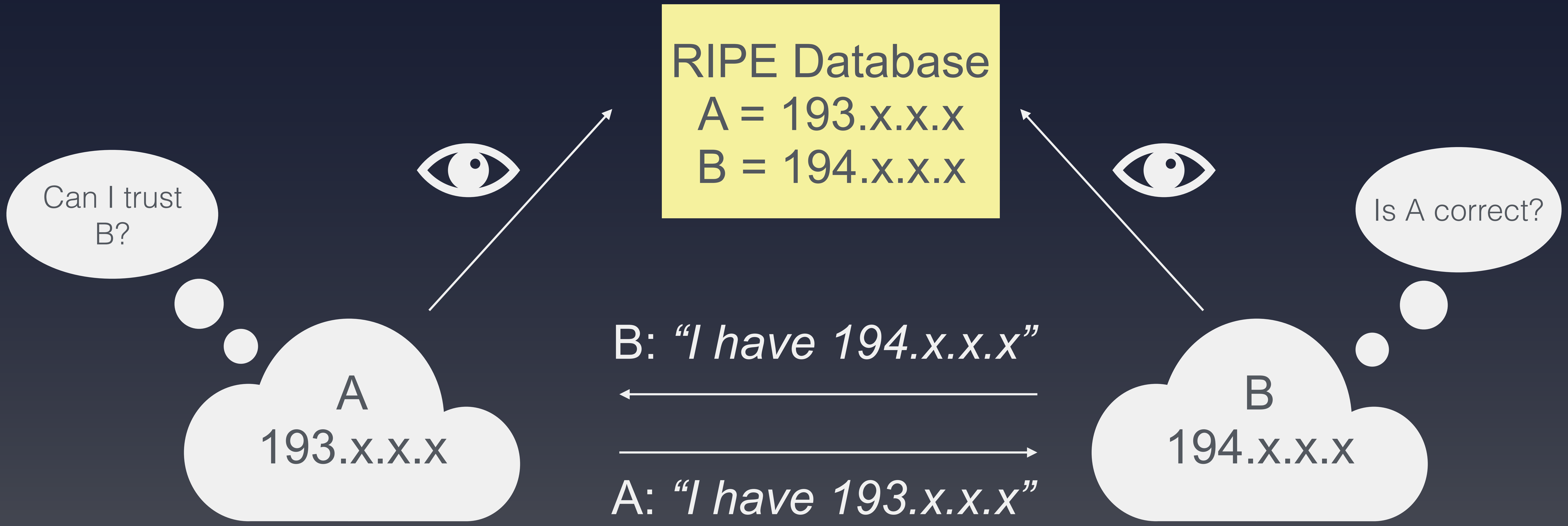
Routing on the Internet



“BGP protocol”

How to Secure Routing?

“Internet Routing Registry”



RIPE Database
A = 193.x.x.x
B = 194.x.x.x

Can I trust B?

Is A correct?

A
193.x.x.x

B
194.x.x.x

B: *“I have 194.x.x.x”*

A: *“I have 193.x.x.x”*

Internet Routing

- Border Gateway Protocol
  - BGPv4, 1994
- The problem remains
  - No built-in security in BGP Protocol

Accidents Happen

- Fat Fingers
  - 2 and 3 are really close on our keyboards…
- Policy violations (leaks)
  - Oops, we did not want this to go to the public Internet
  - Infamous incident with Pakistan Telecom and YouTube

Or Worse…

- **April 2018**
  - BGP and DNS hijack
  - Targeting MyEtherWallet
  - Unnoticed for 2 hours

Incidents Are Common

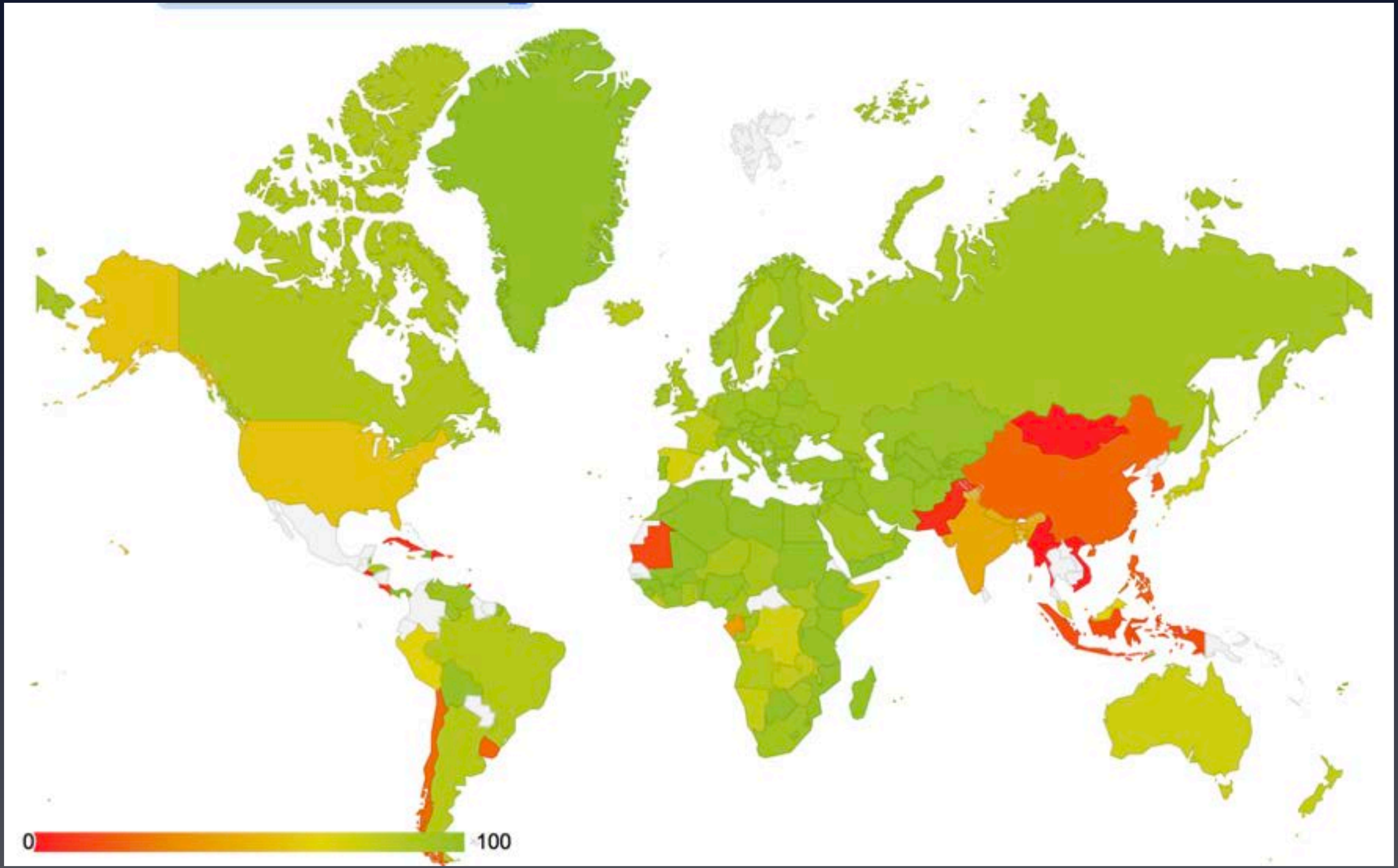
- **2018 Routing Security Review**
  - 12.6k incidents
  - 4.4% of all ASNs affected
  - 3k ASNs victims of at least one incident
  - 1.3k ASNs caused at least one incident

source: https://www.bgpstream.com/

Internet Routing Registry

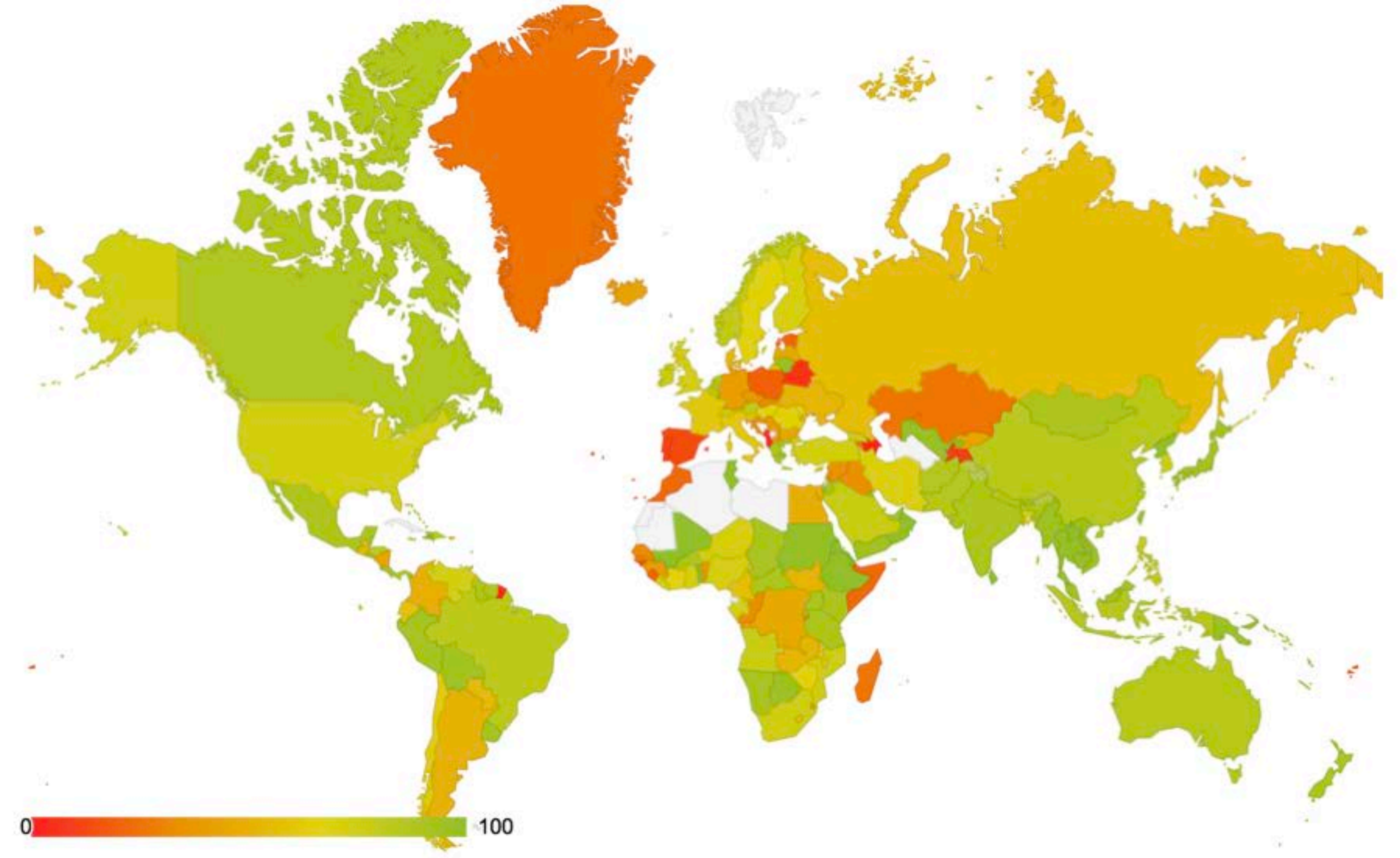
- Many exist, most widely used
  - RIPE Database
  - RADB
- Verification of holdership over resources
  - RIPE Database for RIPE region resources only
  - RADB allows paying customers to create any object
  - Lots of the other IRRs do not formally verify holdership

Accuracy - RIPE IRR



Accuracy - Valid announcements / covered announcements

Accuracy - RADB IRR



Accuracy - Valid announcements / covered announcements

Resource Public Key Infrastructure

- RPKI
  - Ties IP addresses and ASNs to public keys
  - Follows the hierarchy of the registry
- Authorised statements from resource holders
  - ASN X is authorised to announce my IP Prefix Y
  - Signed, holder of Y

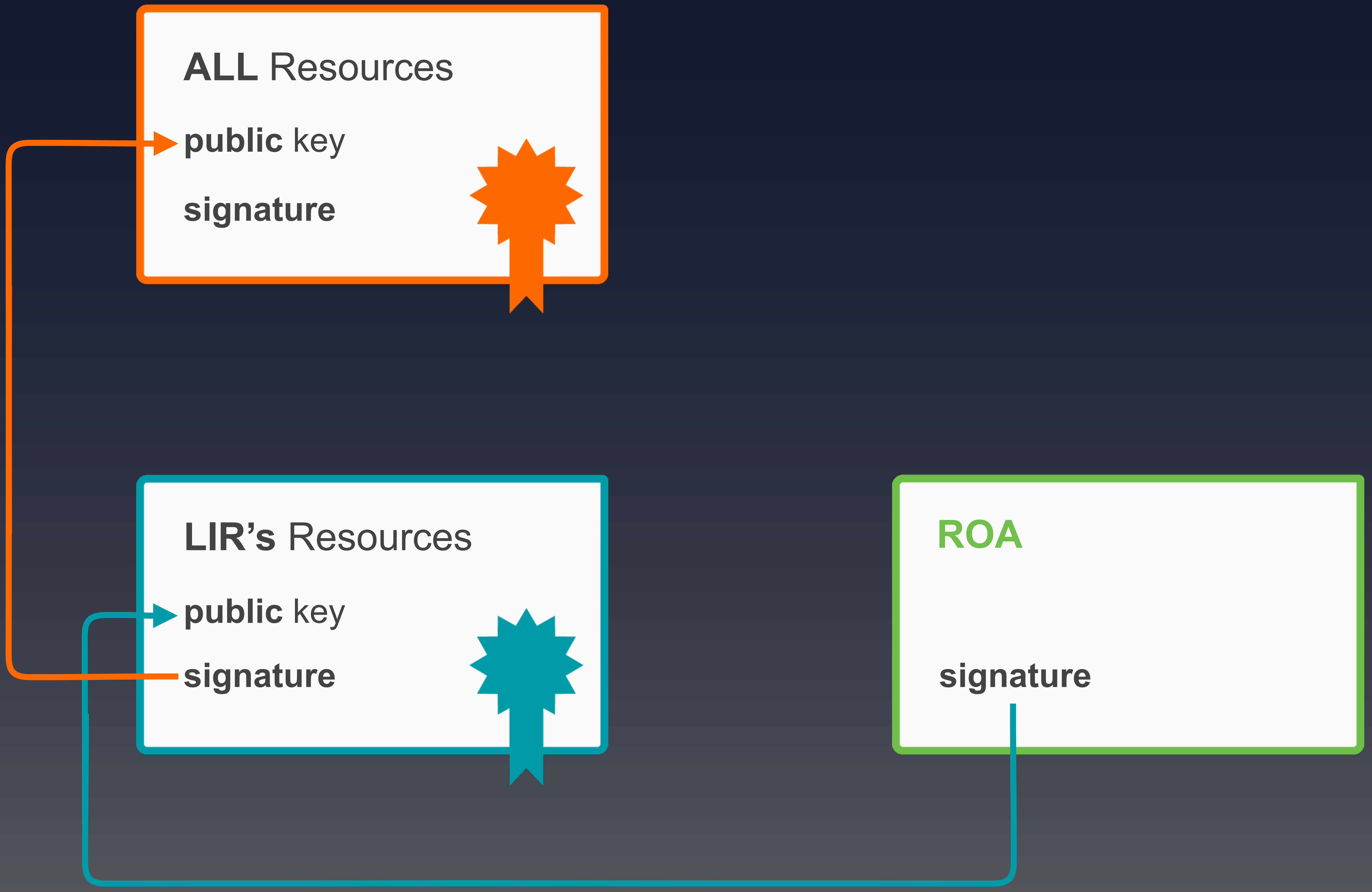
Resource Public Key Infrastructure

- Operated since 2008 by all RIRs
  - Community-driven standardisation (IETF)
  - IRR was not sufficient (incomplete, incorrect)
- Adds crypto-security to Internet Number Resources

Operators Are In Control

- We show member announcements
  - Member chooses to authorise or not
  - Does not need to worry about the crypto
  - It is there, but let the machines handle it…
- APNIC and LACNIC also have easy-to-use portals
  - Uptake and quality of data is a function of the interface

RPKI Chain of Trust



ALL Resources

public key

signature

LIR’s Resources

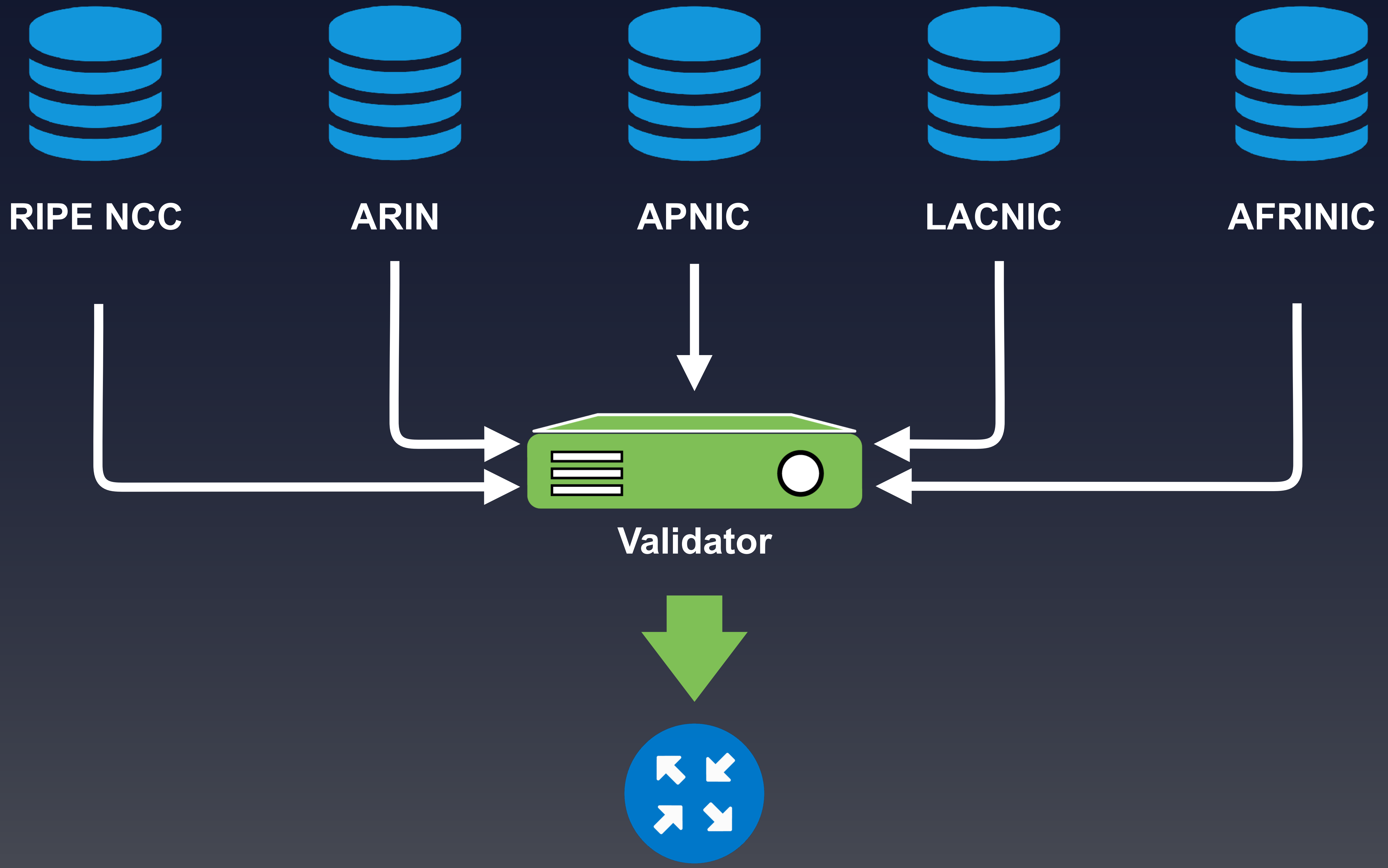
public key

signature

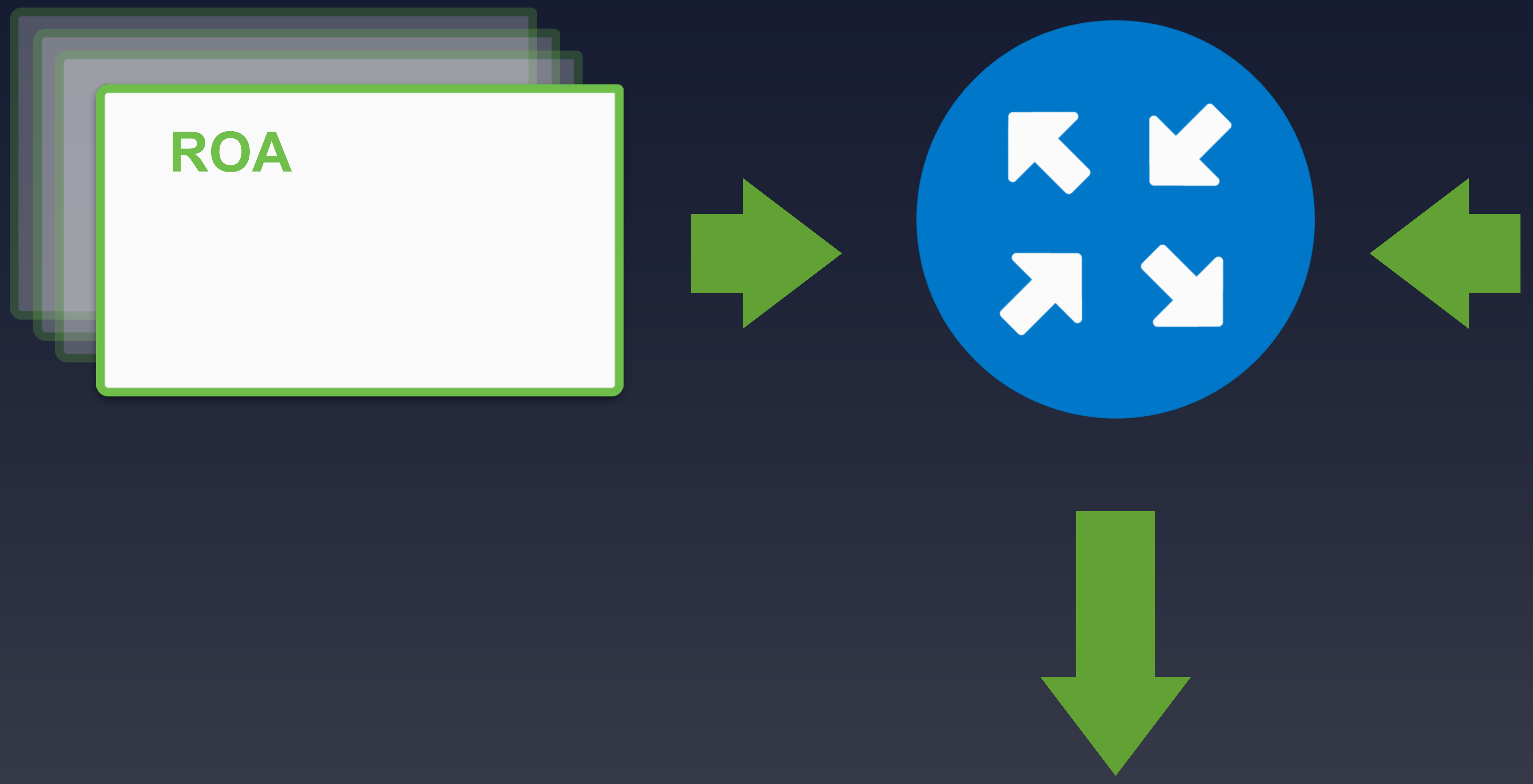
ROA

signature

Route Origin Validation



Route Origin Validation

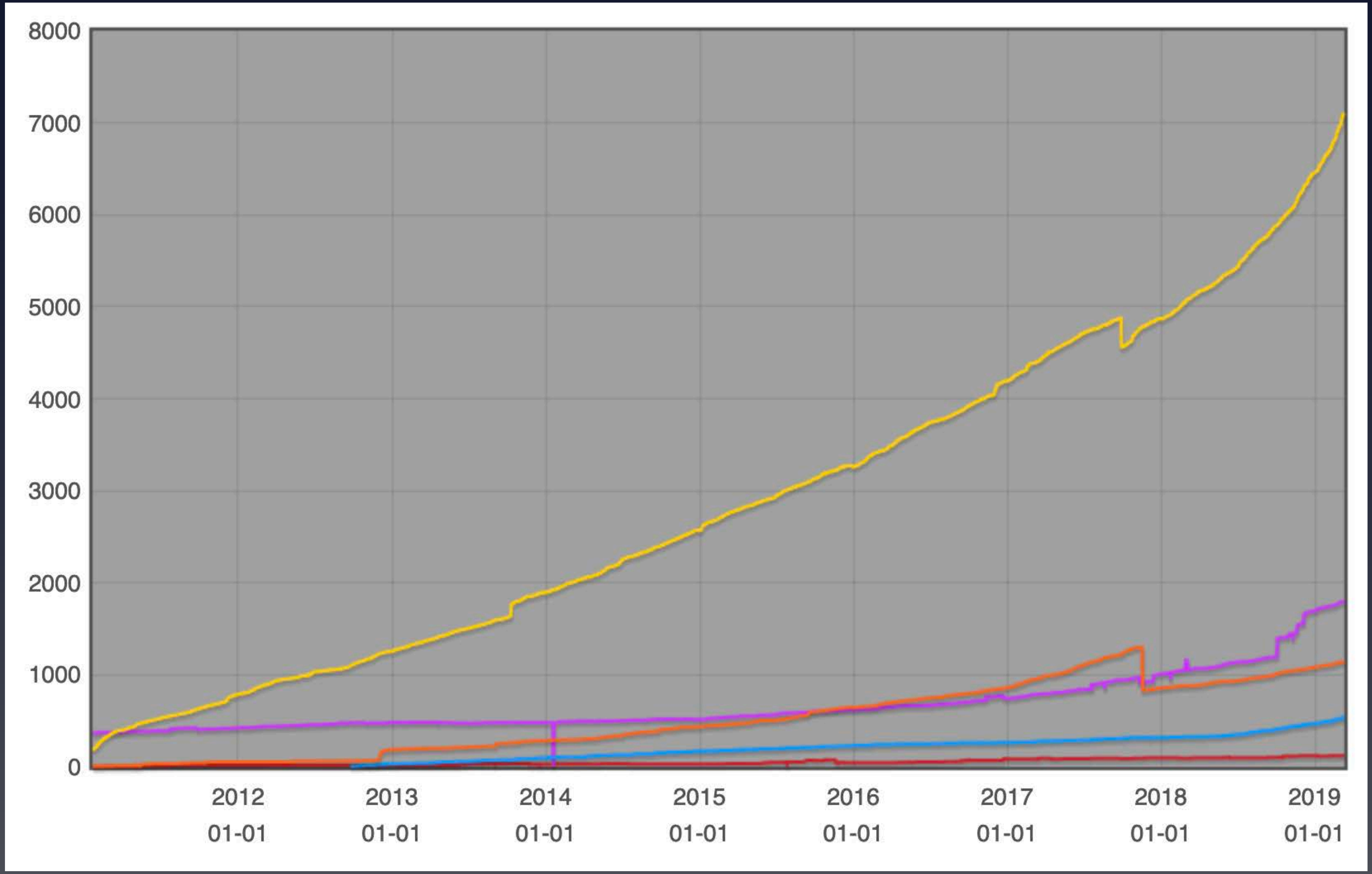


BGP Announcements

AS111	10.0.7.30/22
AS222	10.0.6.10/24
AS333	10.4.17.5/20
AS111	10.0.7.30/22
AS111	10.0.7.30/22
AS111	10.0.7.30/22

BETTER ROUTING DECISIONS

Number of Certificates



🟨 **RIPE NCC: 7100**

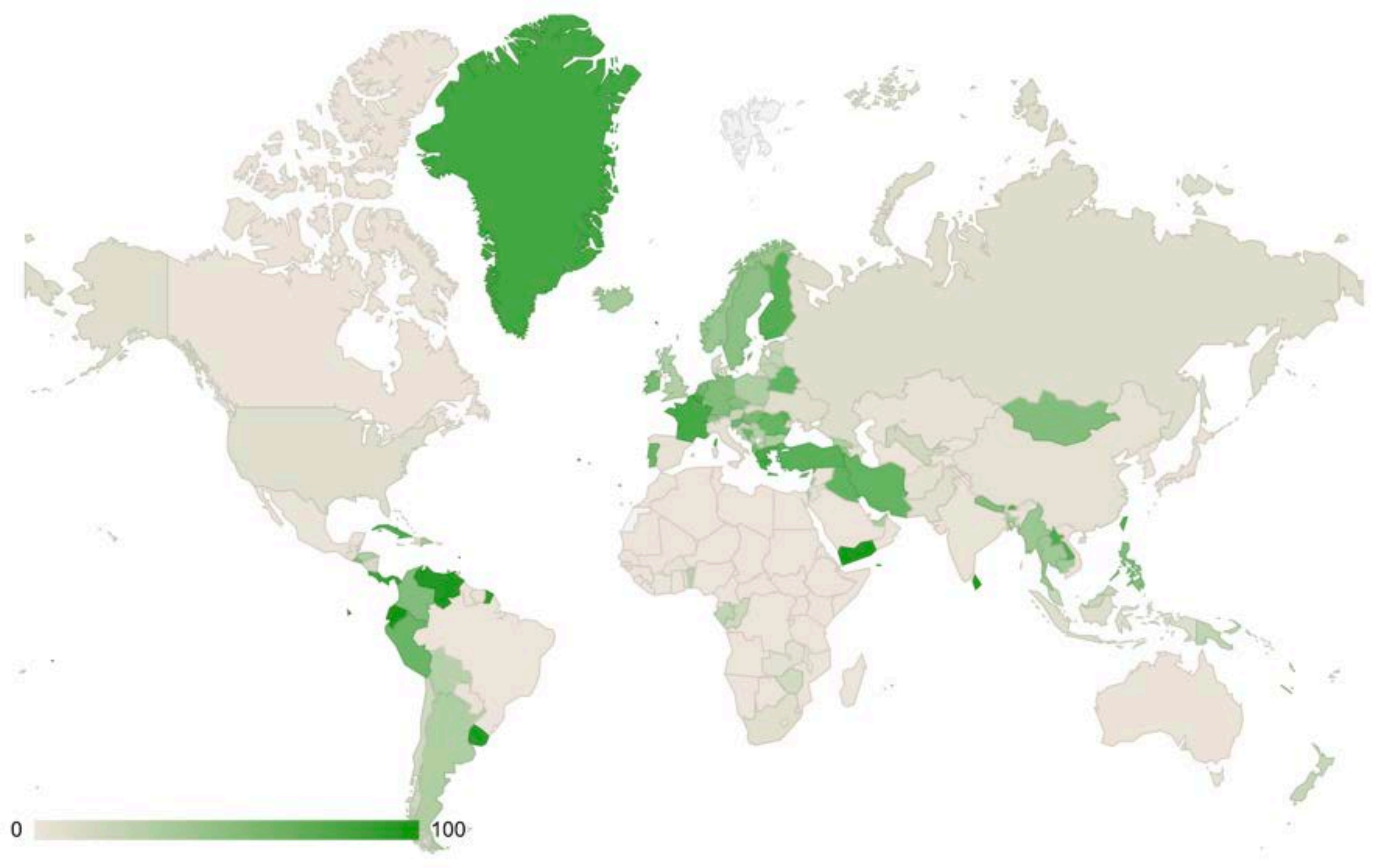
🟪 **APNIC: 1797**

🟧 **LACNIC: 1146**

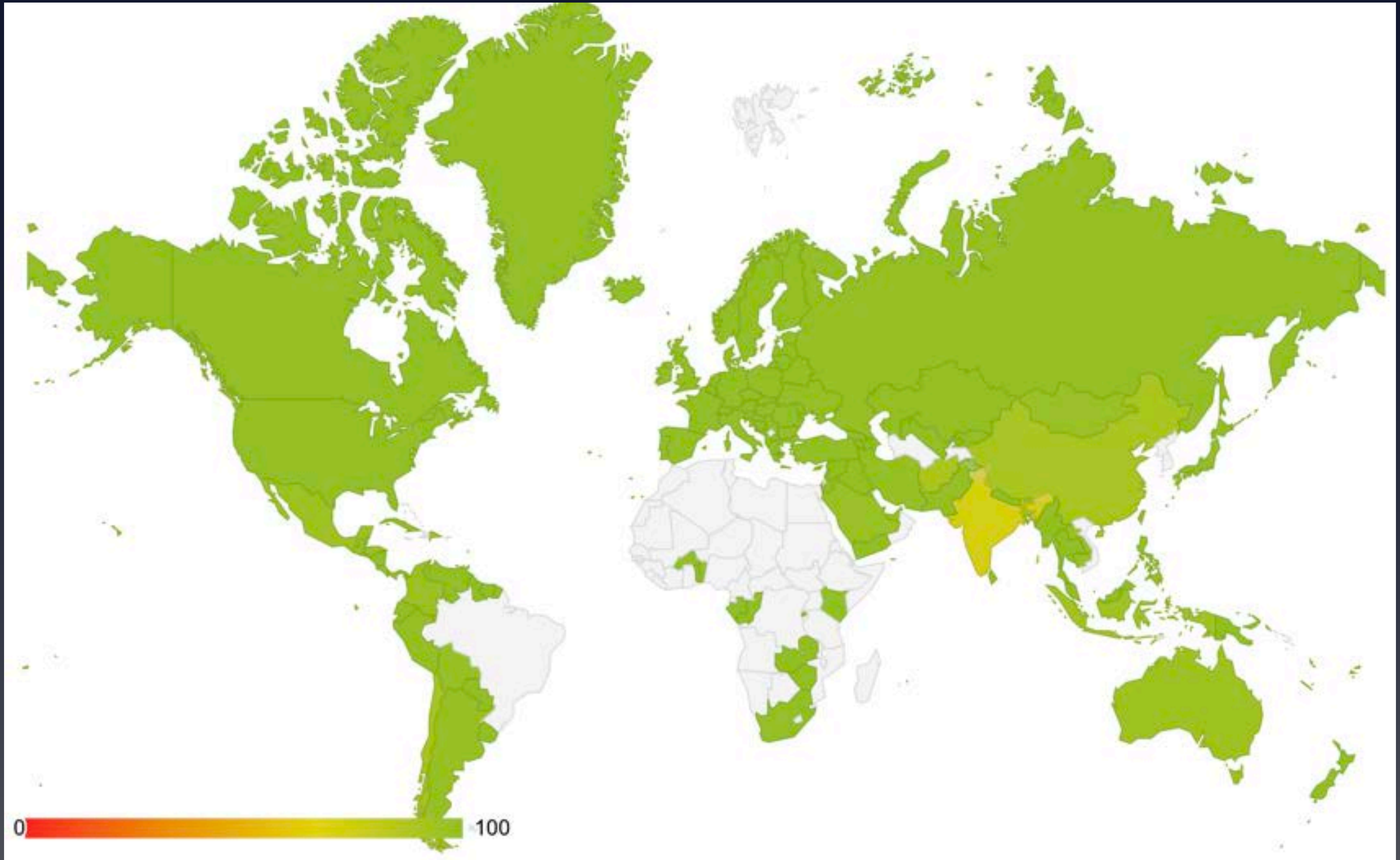
🟦 **ARIN: 538**

🟥 **AFRINIC: 123**

Coverage - RPKI (all RIRs)



Accuracy - RPKI (all RIRs)



IPv4 addresses in valid announcements / covered announcements

RPKI in some regional countries

Country	% Addreses	Accuracy
BY	**61,4%**	**100,0%**
GE	27,2%	100,0%
LV	20,8%	99,7%
LT	19,7%	100,0%
EE	17,1%	100,0%
UZ	12,9%	100,0%
RU	7,6%	99,8%
UA	7,4%	99,6%
KZ	2,35%	100,0%

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

Recommendations to Get Started

- Create your ROAs in the LIR Portal
- Pay attention to the Max Length attribute
- Download and run a Validator
- Check validation status manually, which routes are invalid?
- Set up monitoring, for example pmacct (link)

Invalid == Reject

- **What breaks if you reject invalid BGP announcements?**
  - “Not all vendors have full RPKI support, or bugs have been reported”
  - “Mostly nothing” -AT&T
  - “5 customer calls in 6 months, all resolved quickly” -Dutch medium ISP
  - “Customers appreciate a provider who takes security seriously” -Dutch medium ISP
  - “There are many invalids, but very little traffic is impacted” -very large cloud provider

Making the Difference

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

Questions

nathalie@ripe.net