RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Developments in Routing Security

Oleg Muravskiy

4 June 2019 | ENOG 16

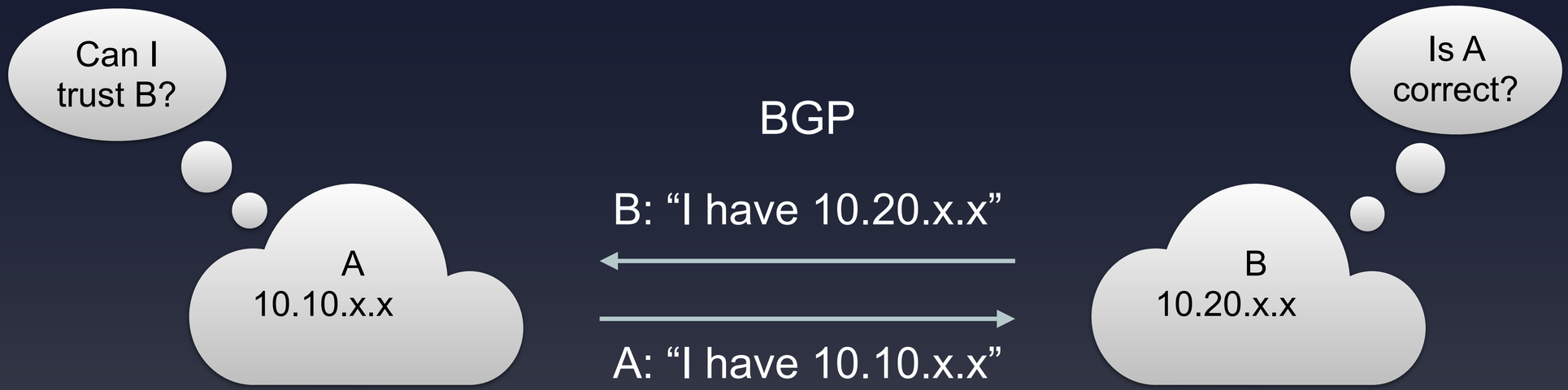
Who We Are

- **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



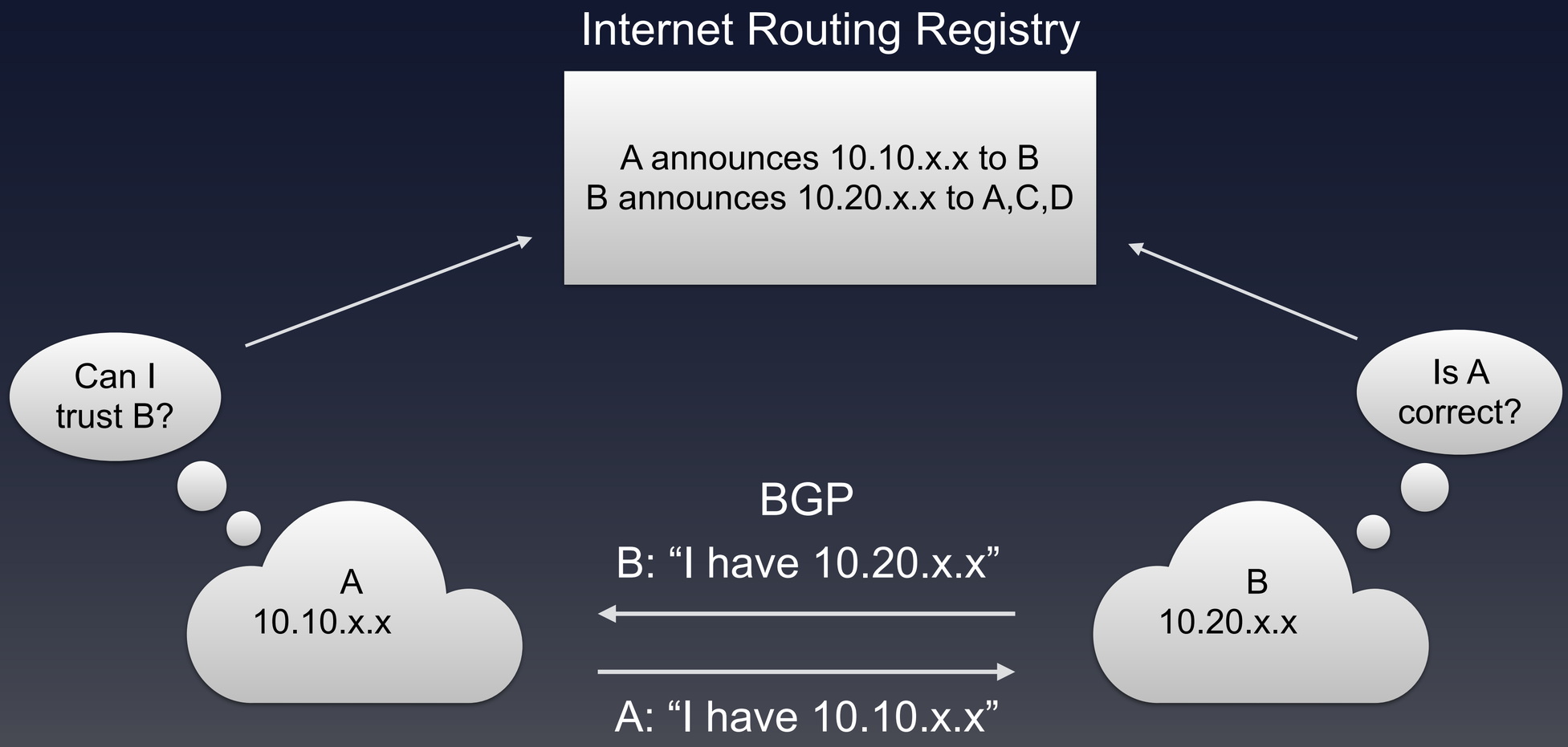
Incidents Are Common

- 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

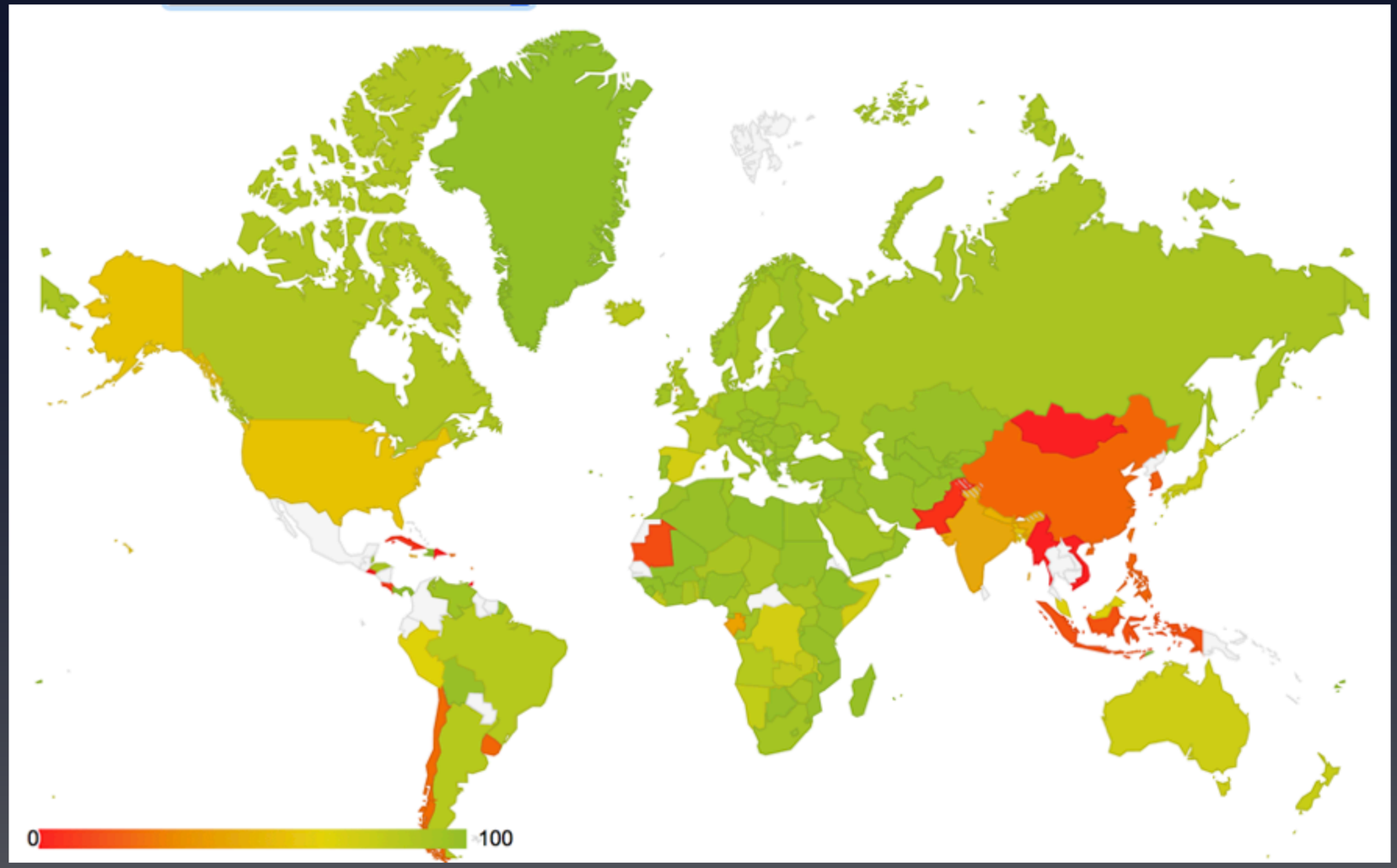
How to Secure Routing?



Internet Routing Registry (IRR)

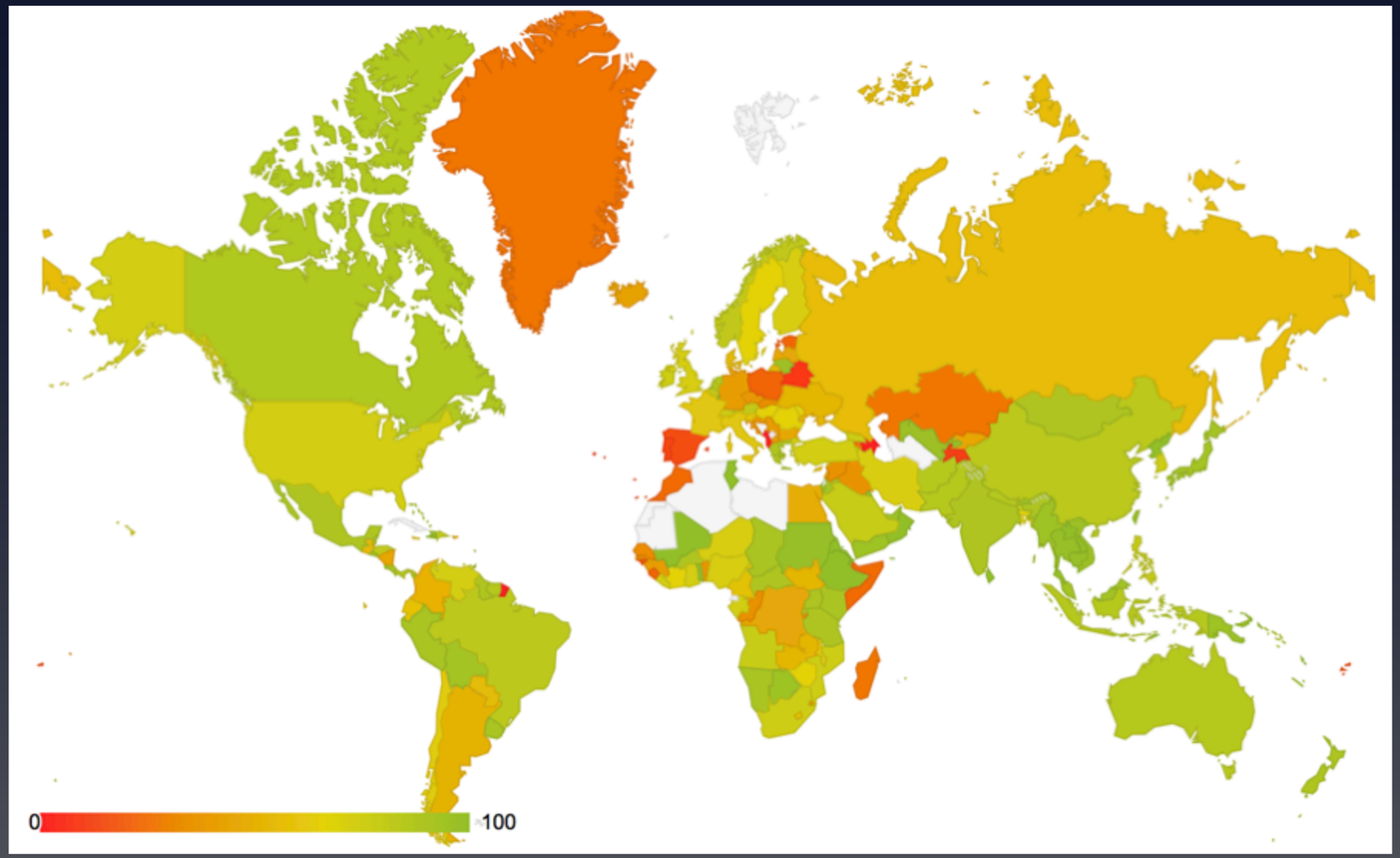
- **IRRs exist for many years**
- **RIPE DB, NTTCOM, RADB, ALTDB, ARIN IRR, BBOI, BELL, LEVEL3, RGNET, TC, CANARIE, …**
- **But their accuracy is not great**
  - The RIPE Database verifies holdership for the RIPE region resources only
  - The RADB allows paying customers to create any object
  - Many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

1: Create route authorisation record

RPKI Repository

AS A is authorised to announce 10.10.0.0/16

2: Validate route

Is A correct?

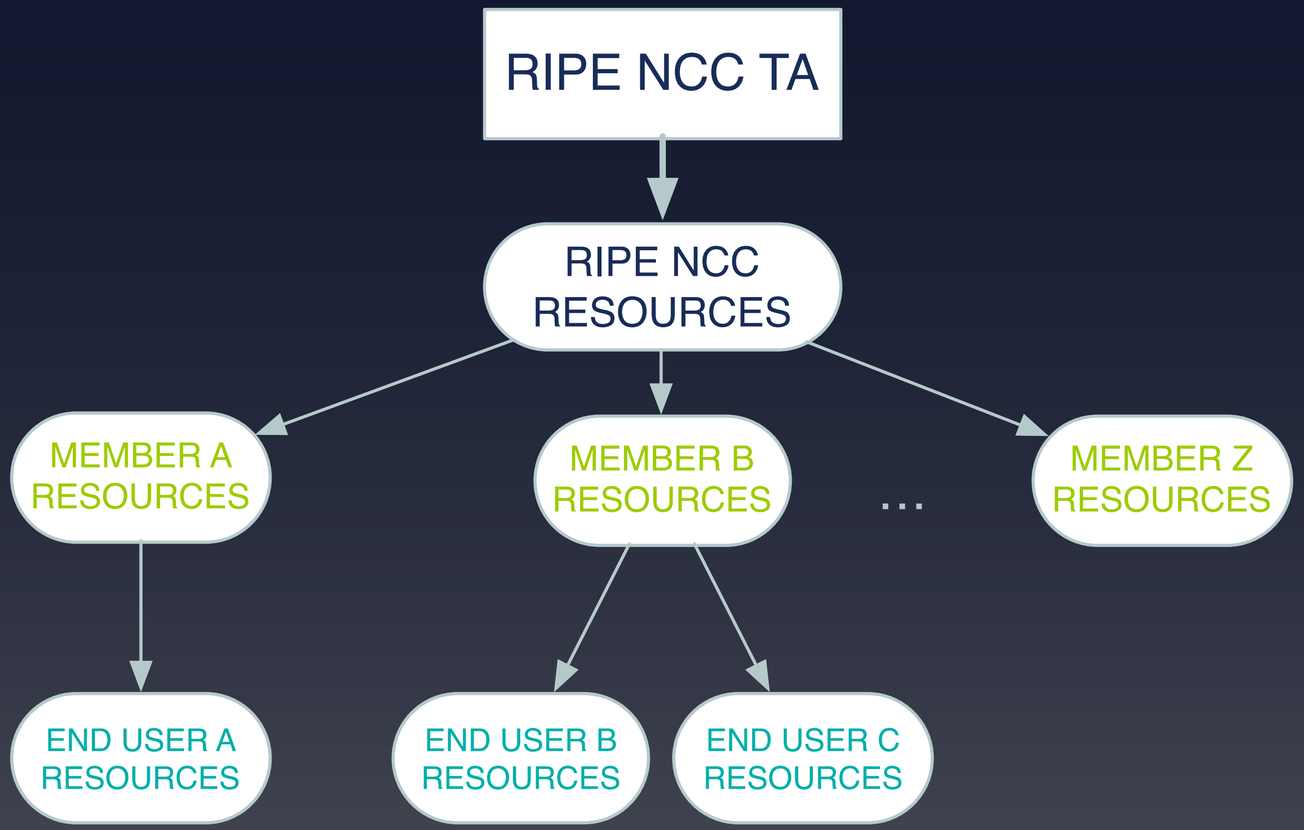
AS A
10.10.x.x

BGP

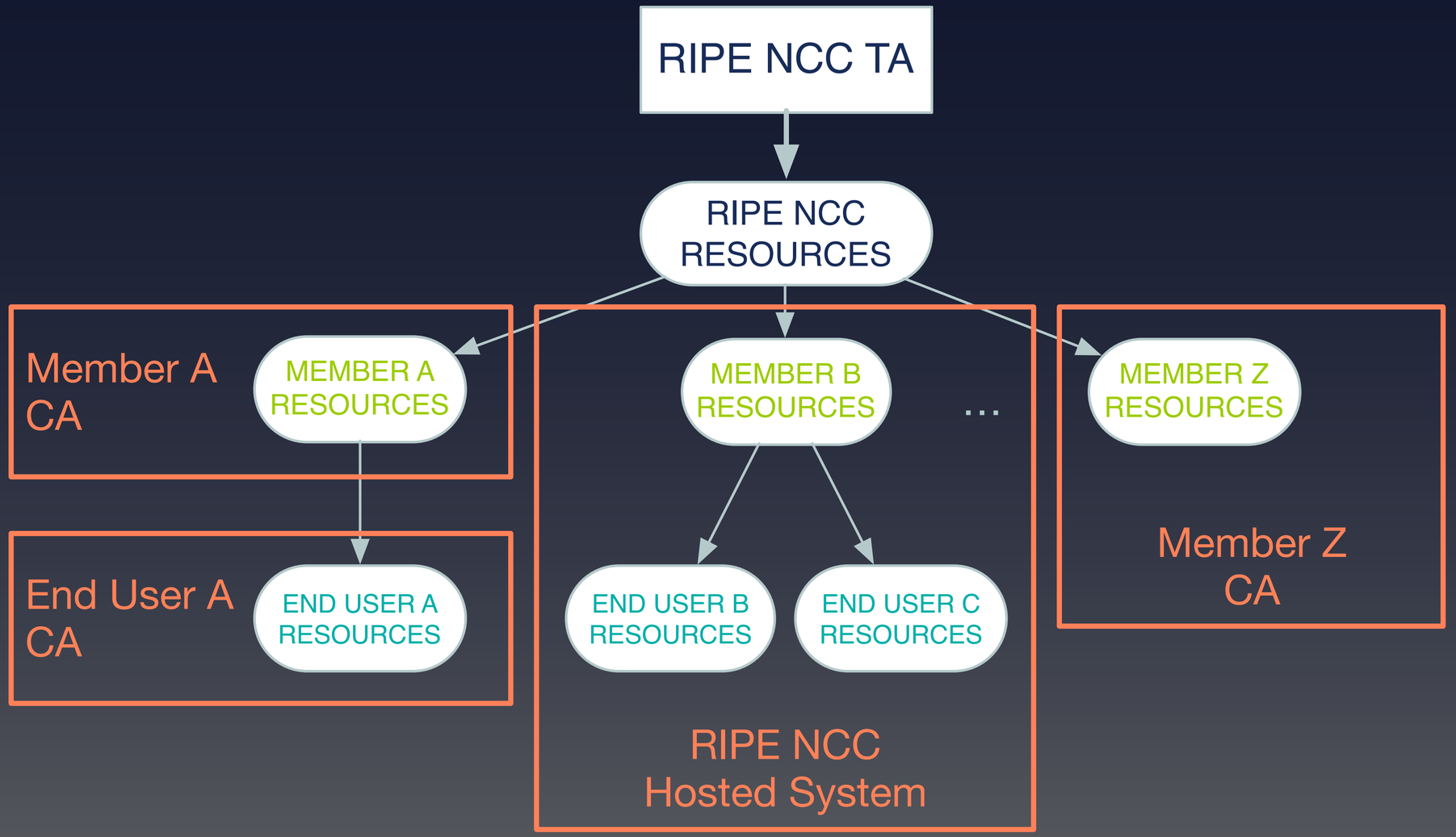
A: “I have 10.10.x.x”

AS B
10.20.x.x

Creating RPKI Objects: Certificate Hierarchy



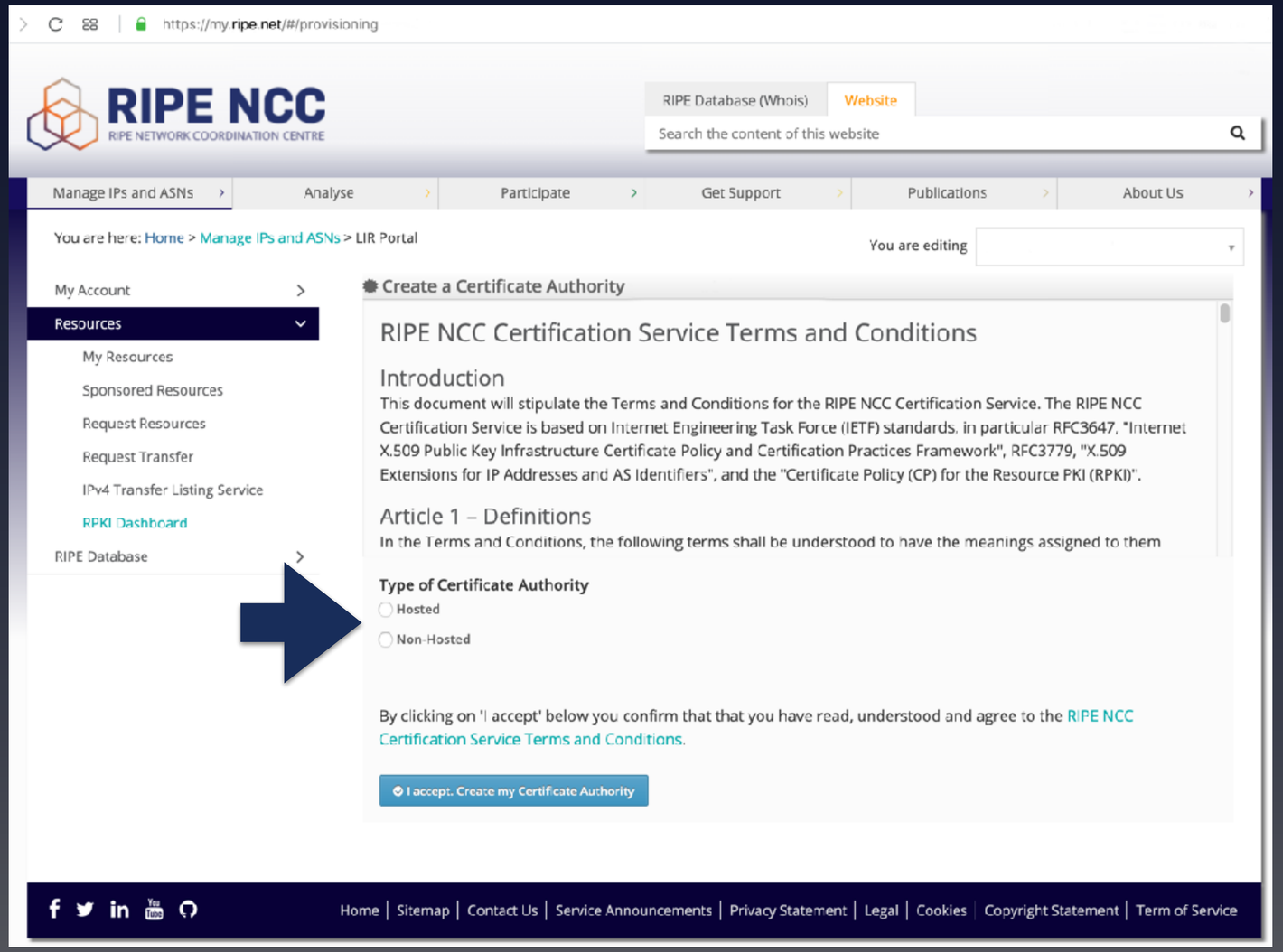
Creating RPKI Objects: Hosted vs Non-Hosted



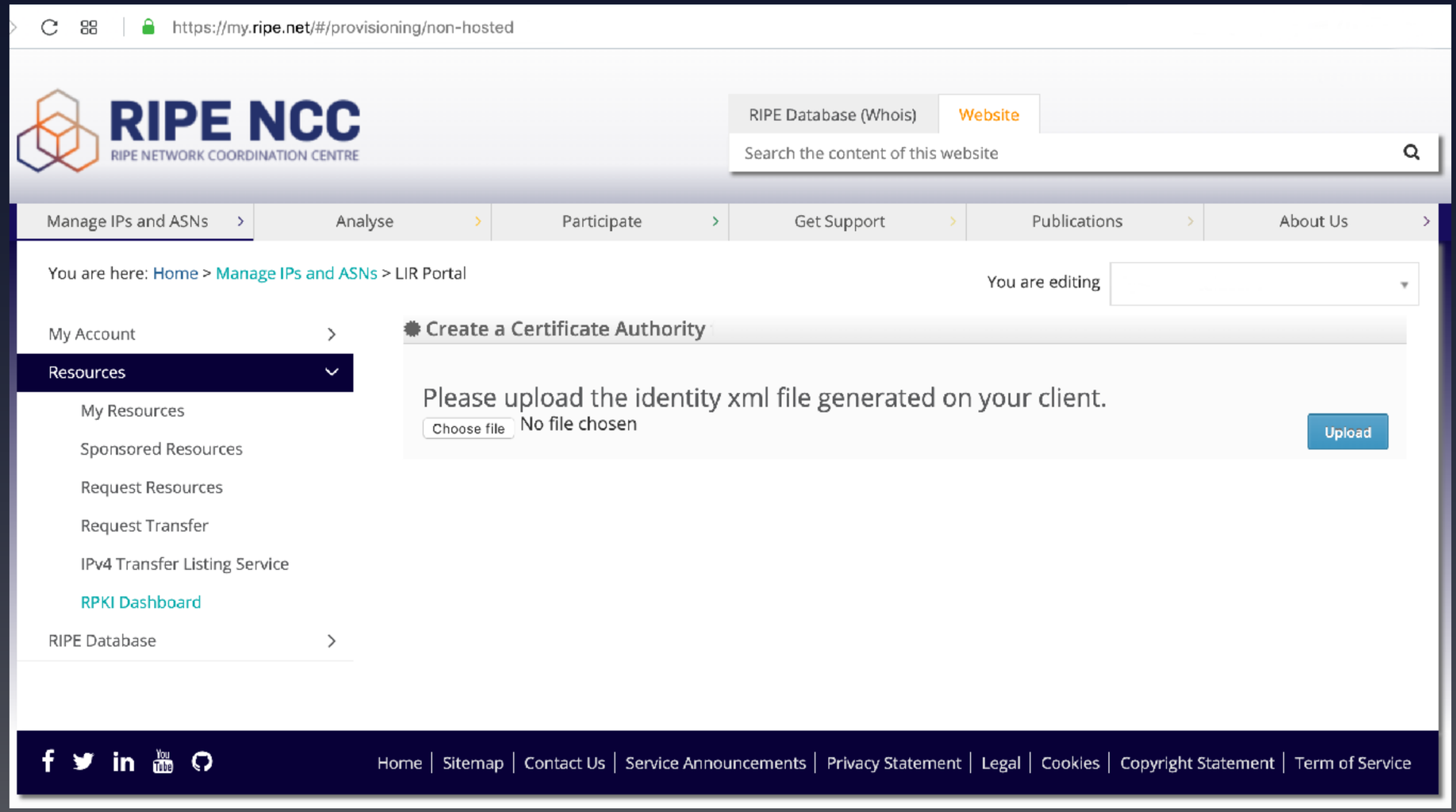
Creating RPKI Objects: Running Non-Hosted CA

- **Install RPKI CA software**
  - Dragon Research Labs, rpki.net RPKI toolkit
  - NLnet Labs Krill
- **Enable non-hosted CA on LIR Portal**
- **Setup connection with RIPE NCC CA**

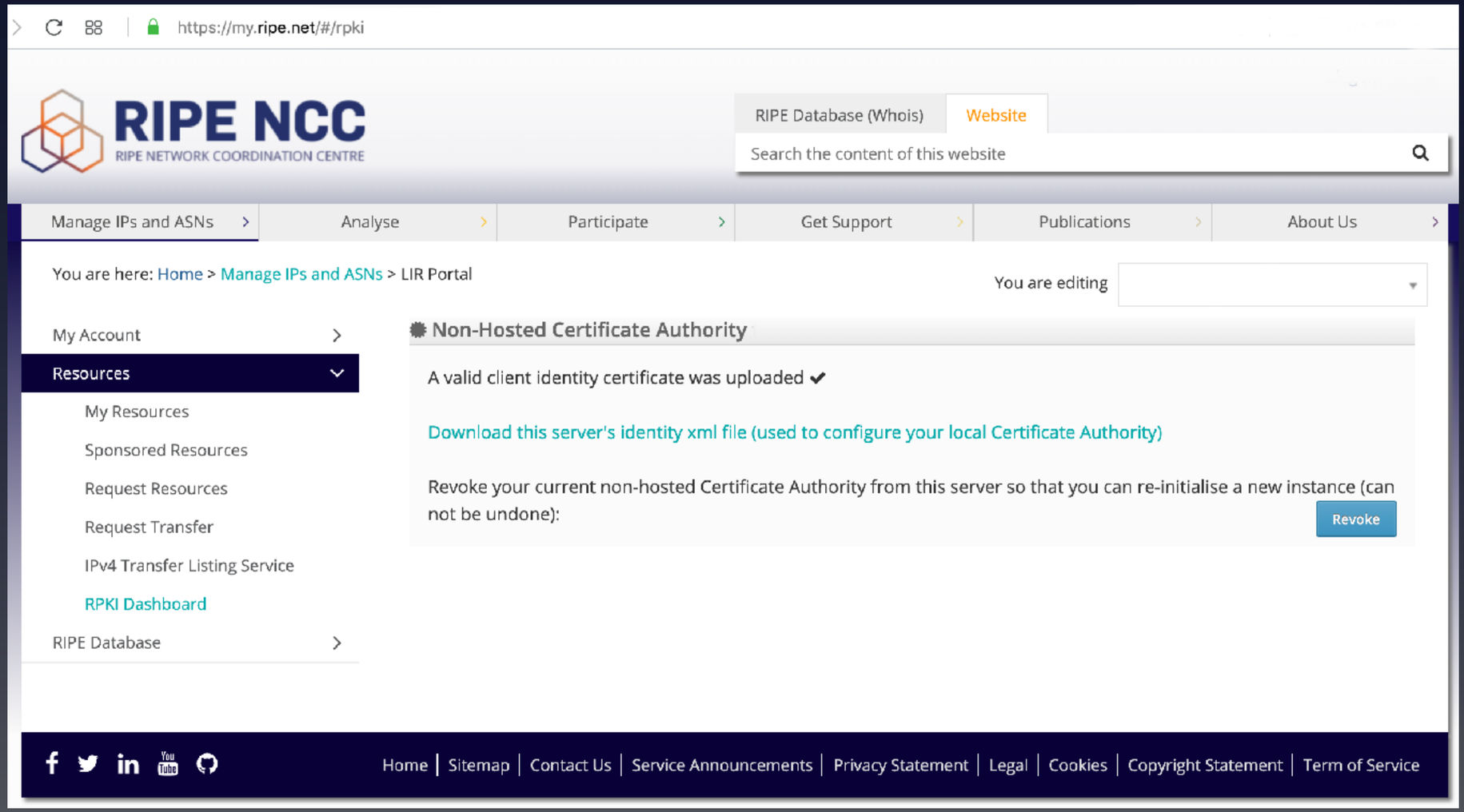
Enable Non-Hosted CA on the LIR Portal



Setup Connection With the RIPE NCC CA



Setup Connection With the RIPE NCC CA



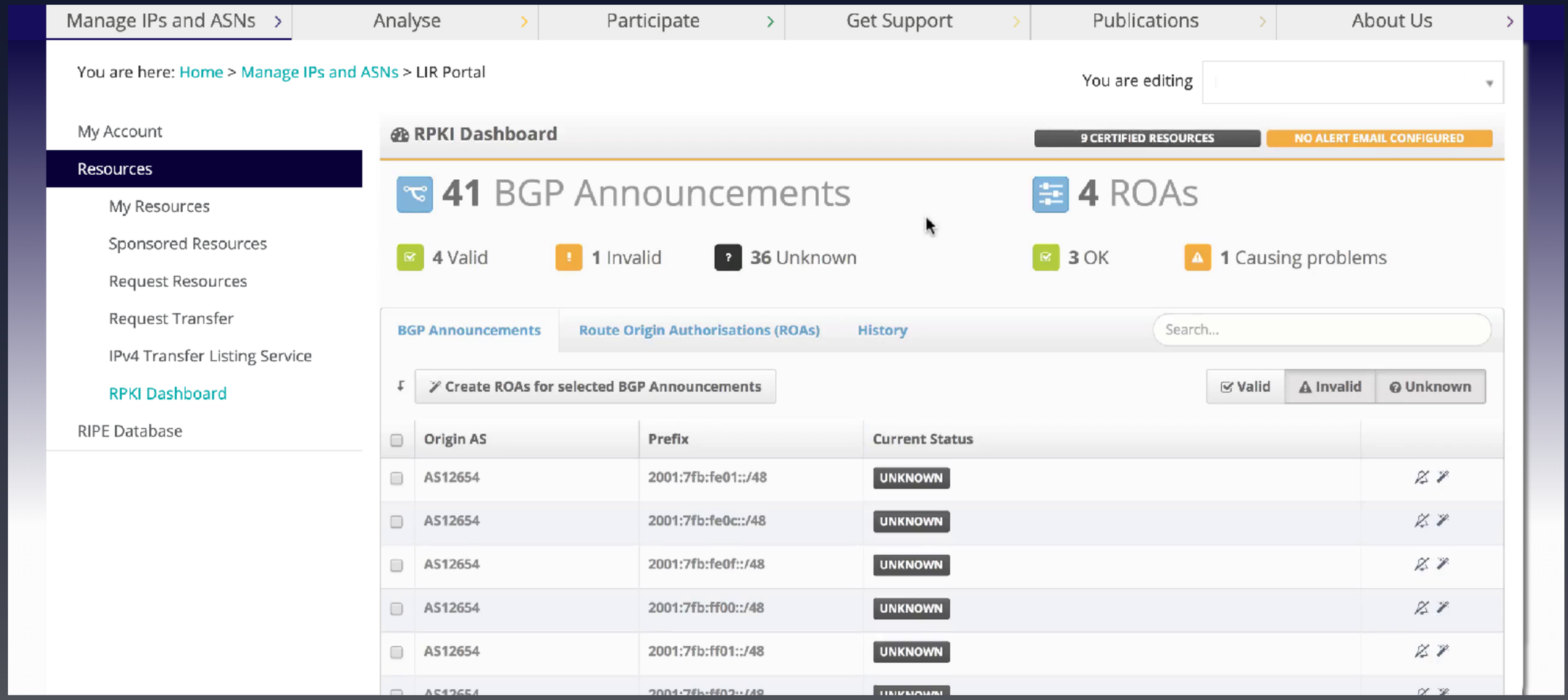
Creating RPKI Objects: Running non-Hosted CA

- **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)**

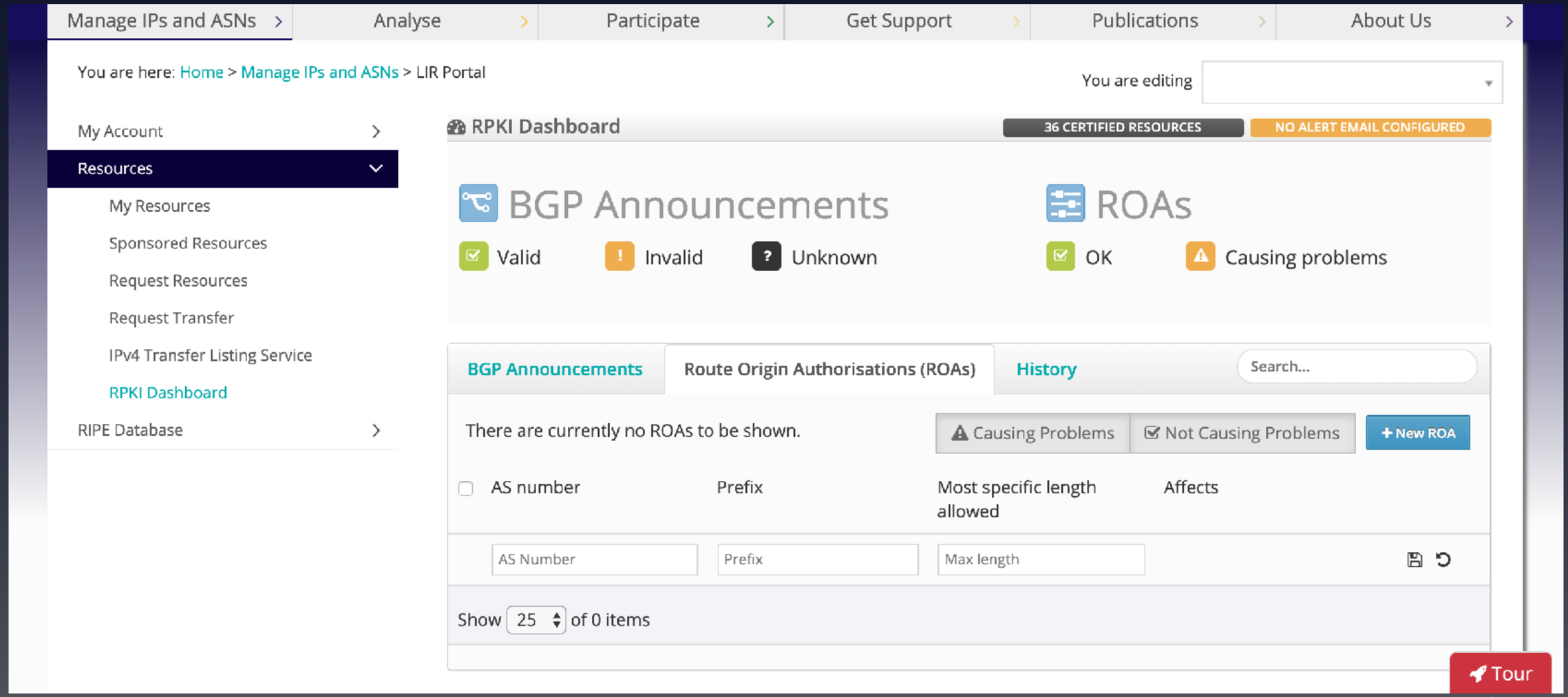
Creating RPKI Objects: Using Hosted CA

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

Create Your ROA Objects in a Hosted CA



Create Your ROA Objects in a Hosted CA



https://youtu.be/gLwHp12wOGw

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

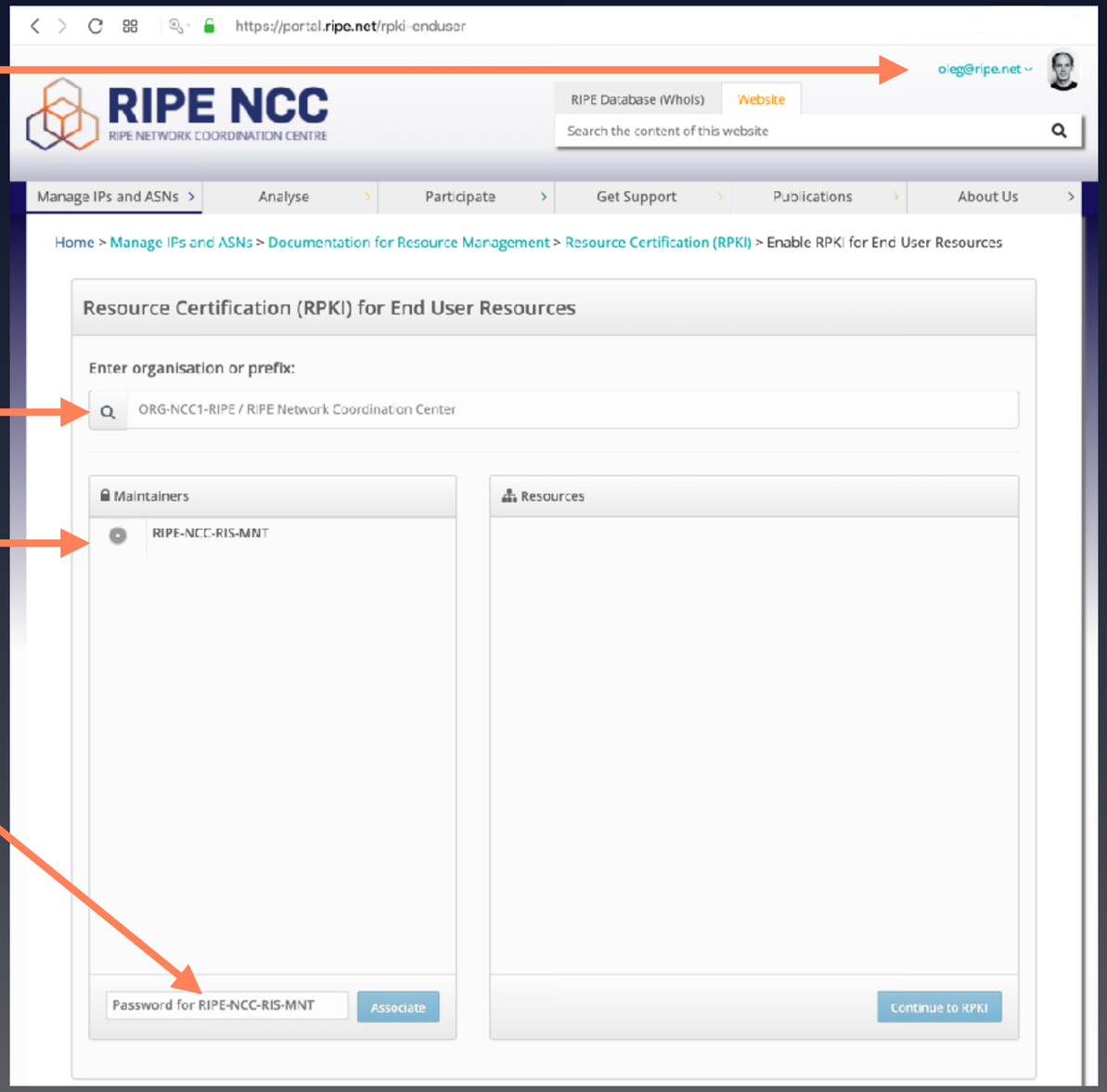
Hosted CA for PI End-Users

Your account

Your organisation

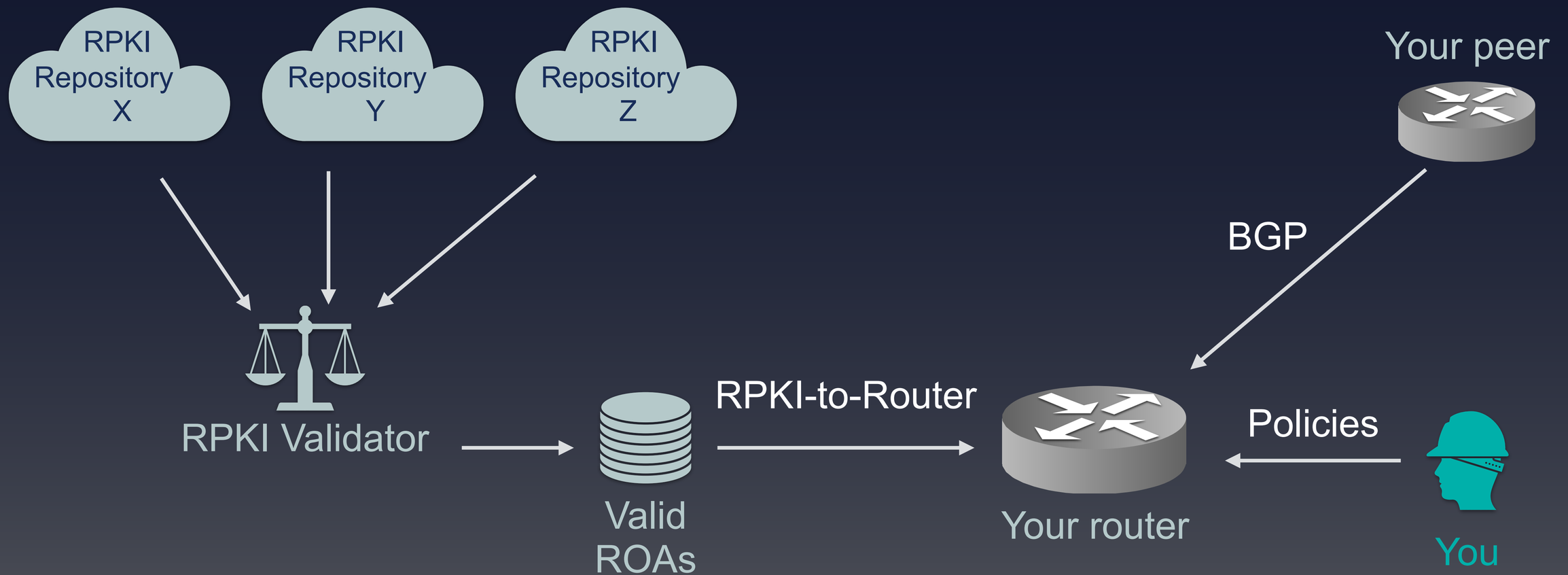
Linked maintainers

Authenticate



Routing validation

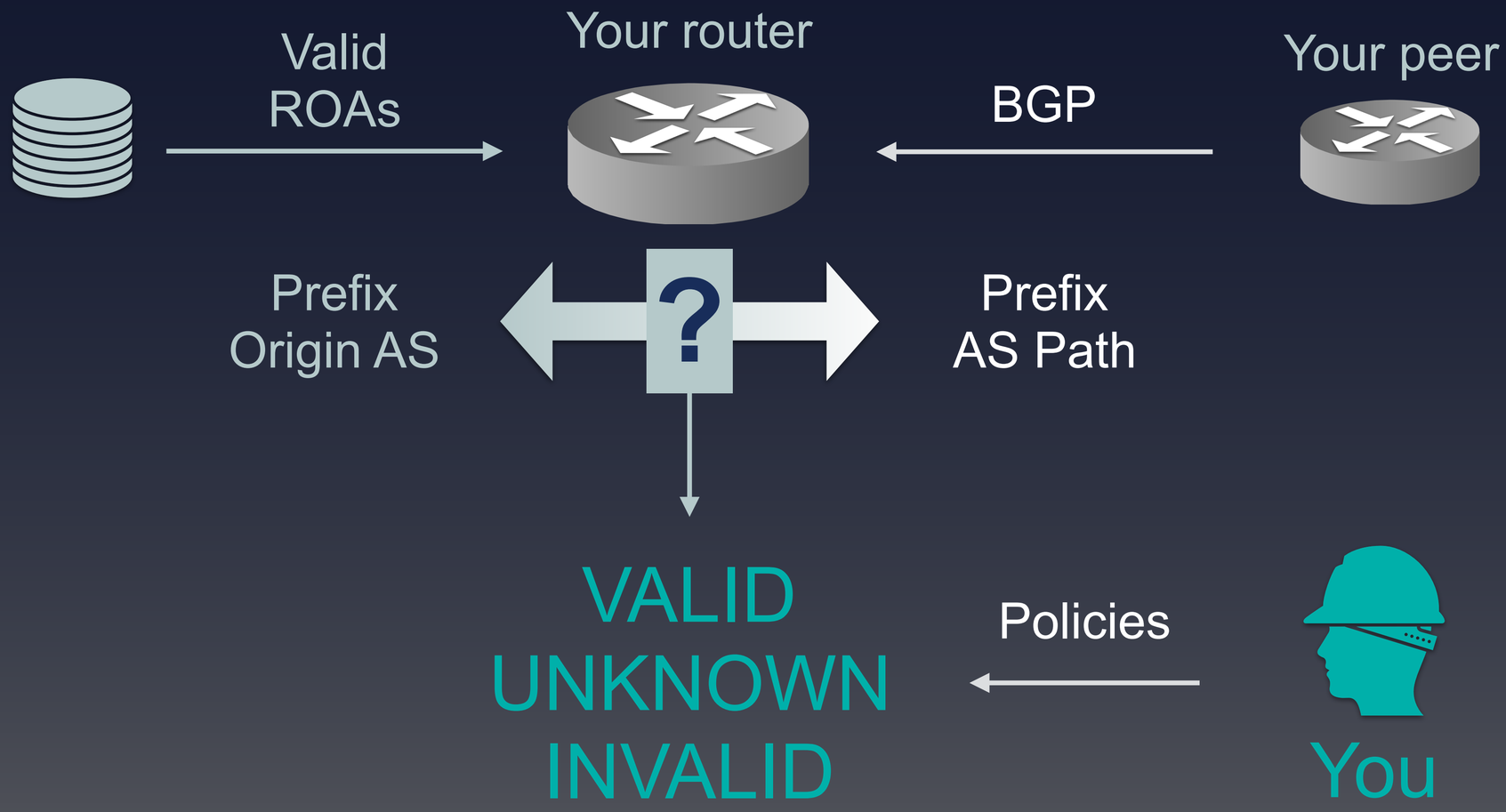
Validating Route Announcements



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?

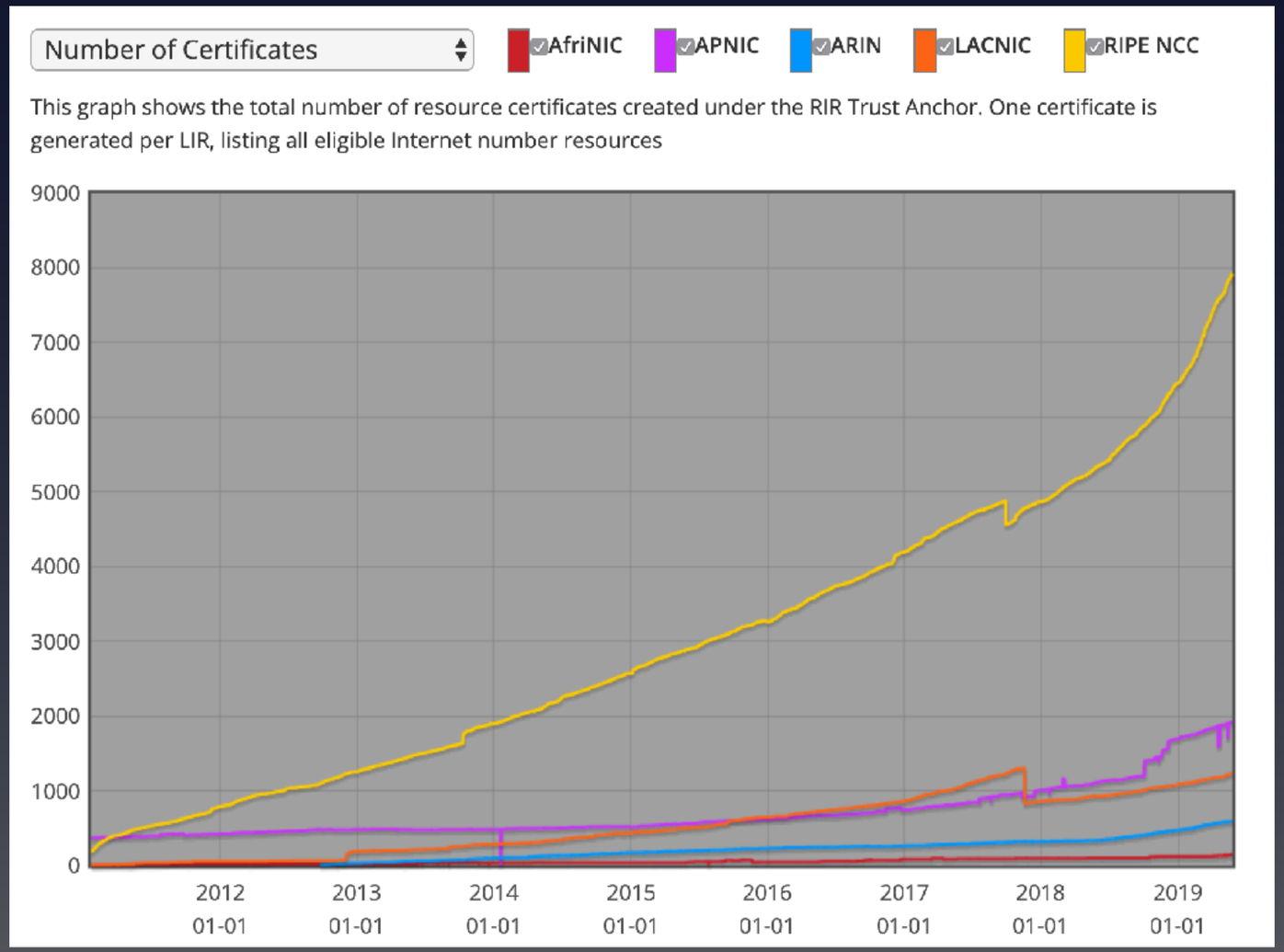
Invalid == reject ?

- 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

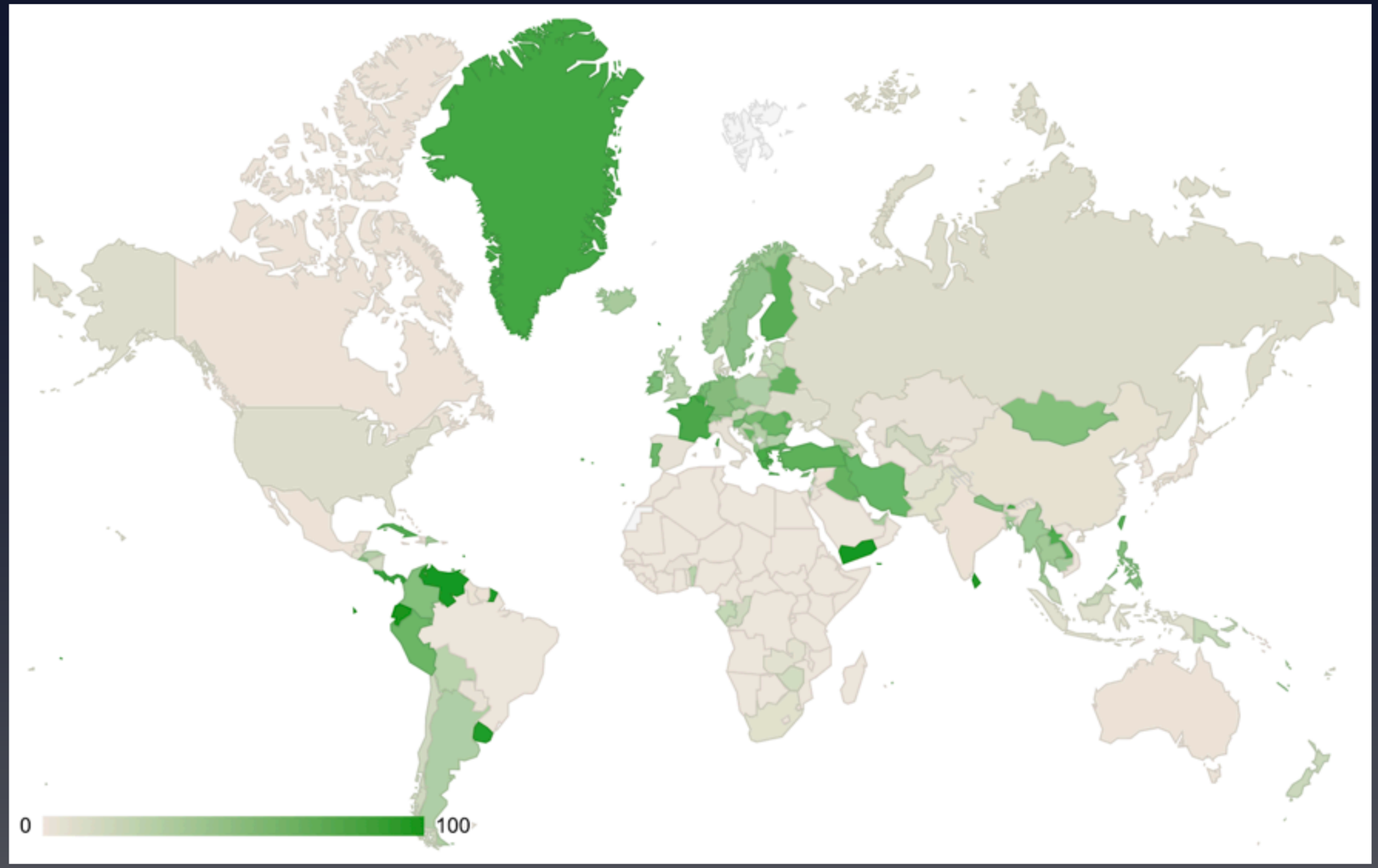
- ROA-based validation covers only part of the problem
- BGPsec could solve it, but can’t
- Autonomous System Provider Authorization (ASPA)
  - Work in progress
- Don’t wait, start now

Number of Certificates



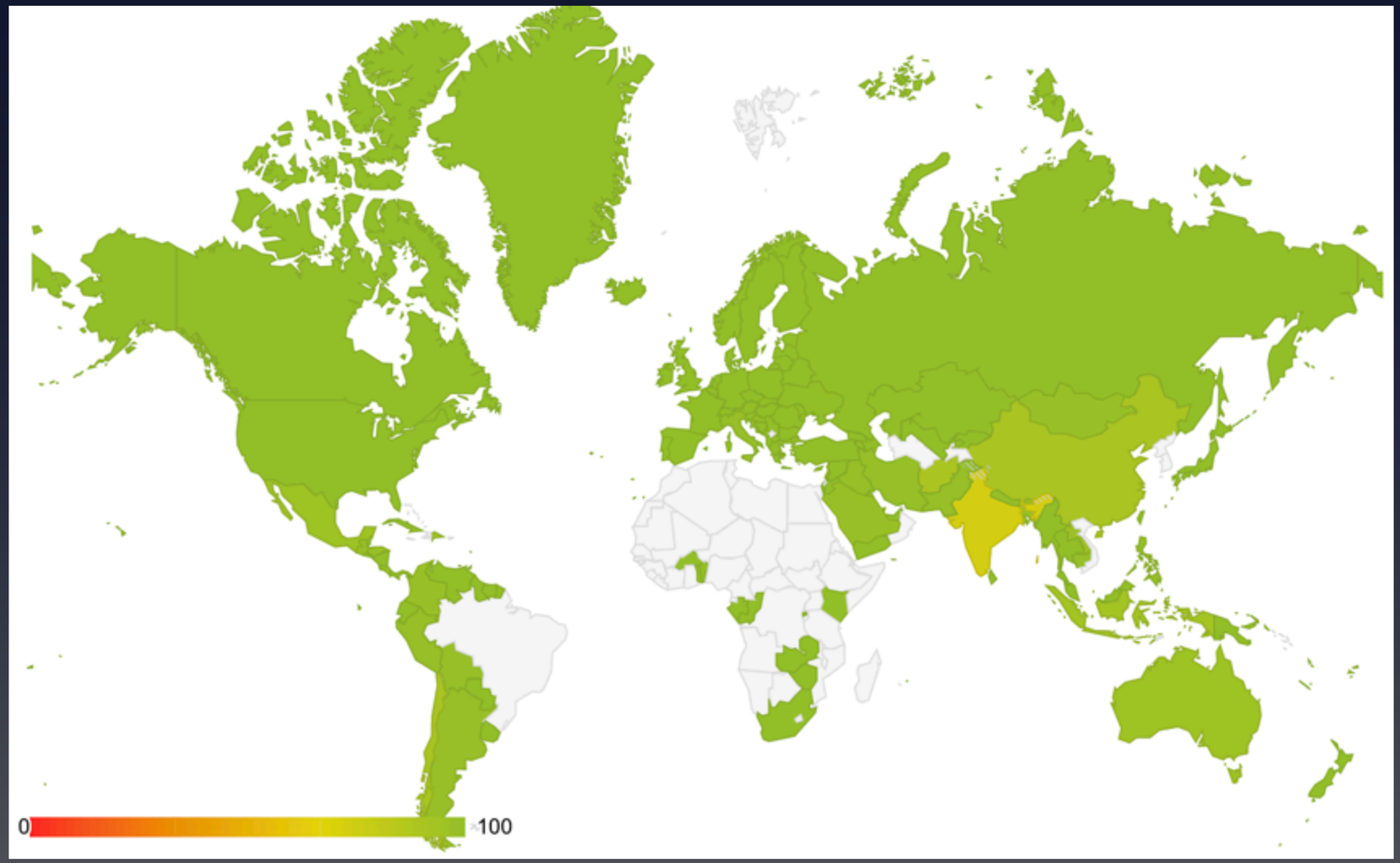
https://certification-stats.ripe.net/

Coverage – RPKI (all RIRs)



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

Accuracy – RPKI (all RIRs)



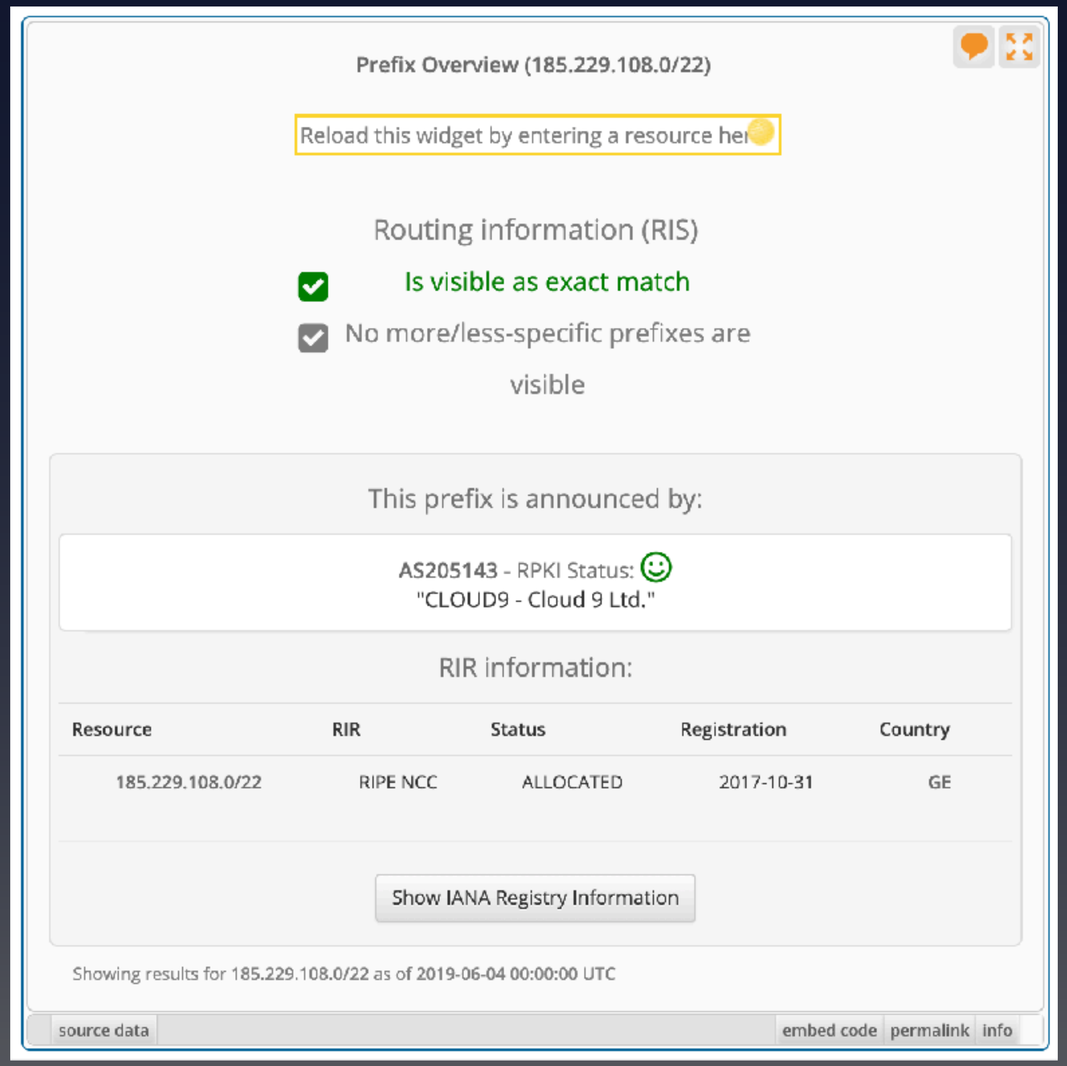
https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html

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



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