RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Developments in Routing Security and RPKI

Oleg Muravskiy

23 September 2022 | RIPE NCC Days Tashkent

RIPE NCC – Who We Are

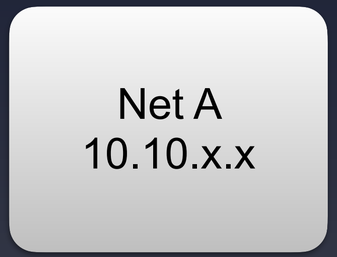
- **We manage ASN and IP address allocations in Europe, the Middle East and parts of Central Asia**
  - Ensure unique holdership
  - Document holdership in the RIPE Database (whois)
  - Issue digital certificates for allocated IP resources
  - Enable operators to document use of their address space

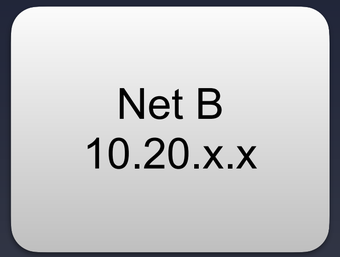
Routing Security Is in Our DNA

- In 1993, RIPE-81 was the first document published that used a common language to describe routing policies
- We co-developed standards for the Internet Routing Registry (IRR) and Resource Public Key Infrastructure (RPKI)
- We are one of the five RPKI Trust Anchors

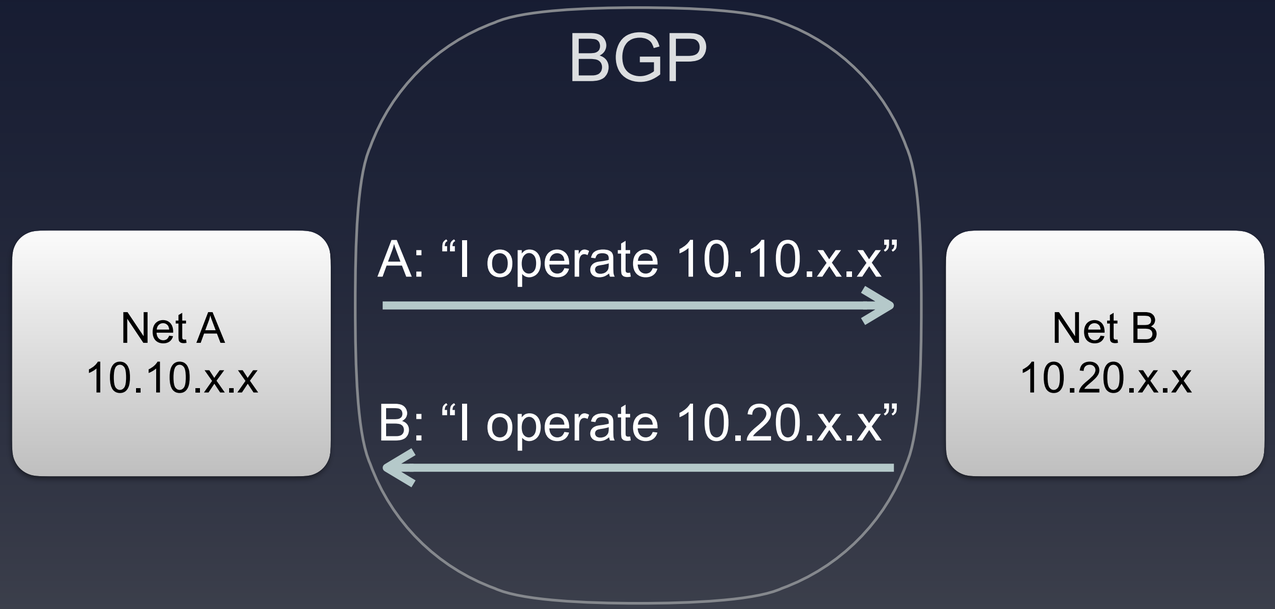
Internet Routing (In)Security

Routing on the Internet (BGP)

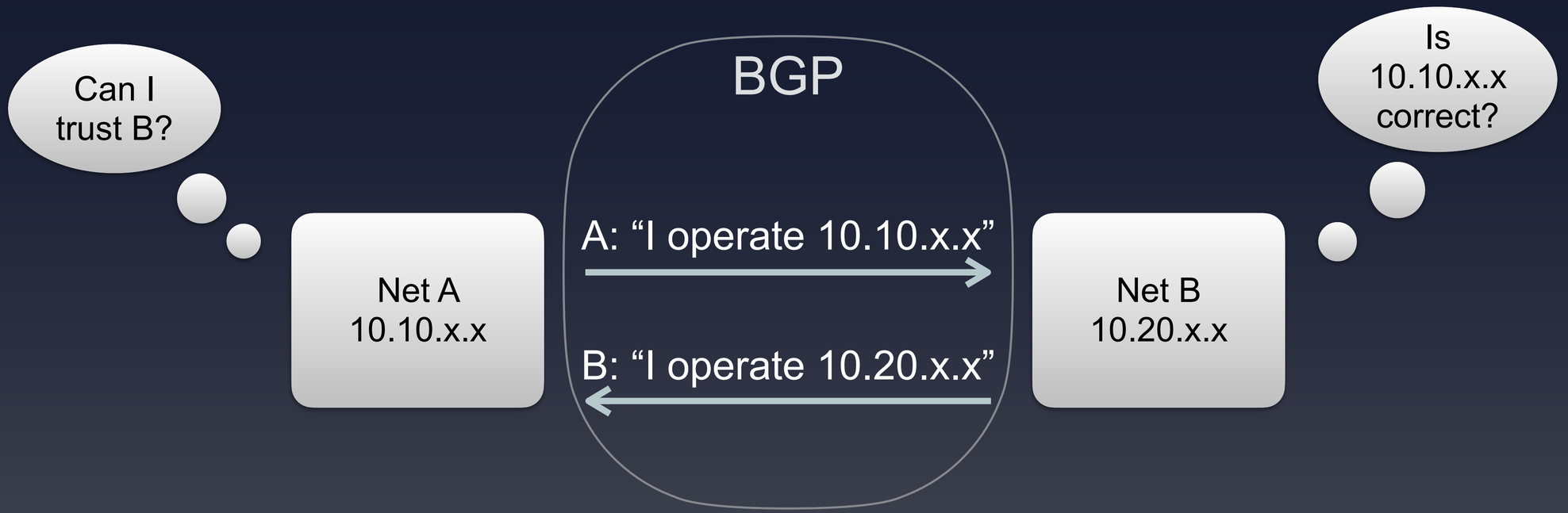




Routing on the Internet (BGP)



Routing on the Internet (BGP)



Incidents Are Common

- 2017 Routing Security Review by the Internet Society
  - 14k incidents
  - 10% of all ASes affected
    - 3k ASNs were victims of at least one incident
    - 1.5k ASNs caused at least one incident
- BGP Security in 2021 by the Internet Society
  - 775 possible hijacks + 830 BGP leaks

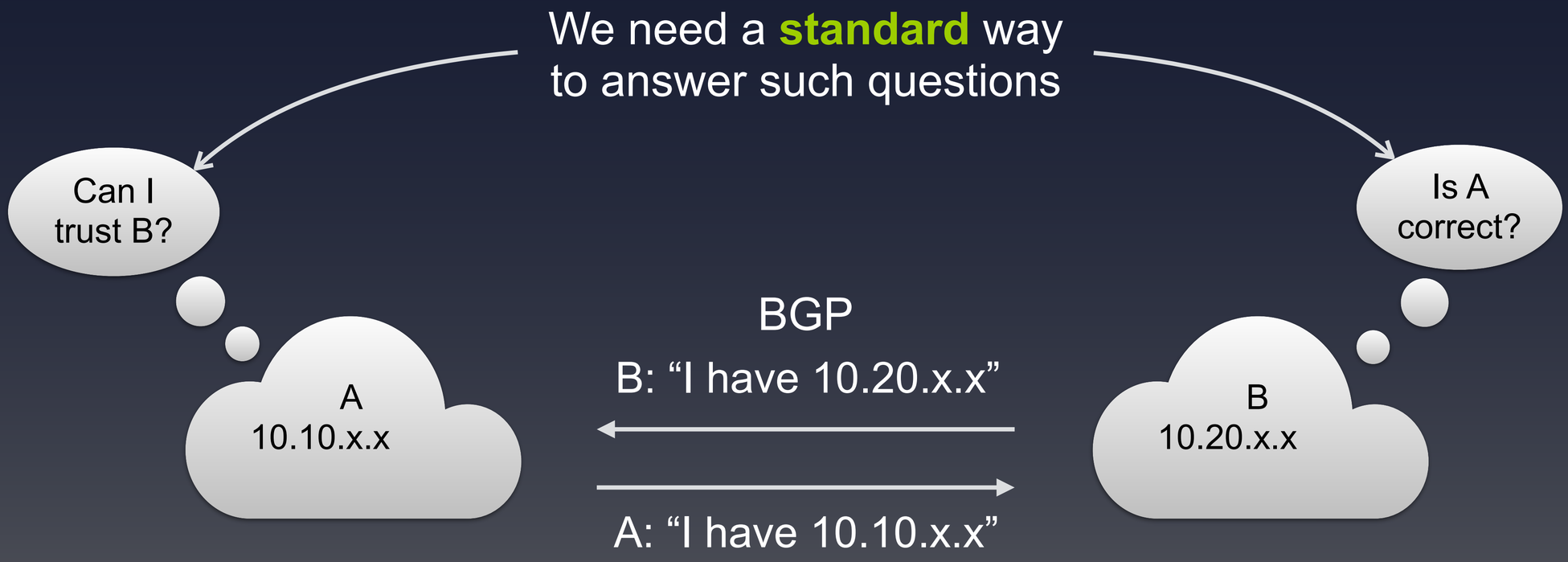
Incidents in 2022

- A misconfiguration on Mikrotik routers looked like a hijack from single-digit ASNs
- 26 July – Rostelecom hijacked Apple for 12 hours
- 28 March – RTComm hijacked Twitter

Non-Incidents Also Became Common

- BGP and DNS hijack targeting Amazon and MyEtherWallet.com (April 2018)
- BGP hijack of Amazon space attacking users of Celer Network (August 2022)

How to Secure Routing?



Resource Public Key Infrastructure (RPKI)

- RIRs issue digital certificates (X.509) to IP and ASN holders
- Certificate holders can cryptographically sign (routing-related) statements, for example:
  - AS X is authorised to announce my IP prefix Y
  - Signed by the holder of Y
- RPKI repositories operated by all RIRs since 2011
- IETF works on standards

RPKI Route Origin Validation (ROV)

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 validation records

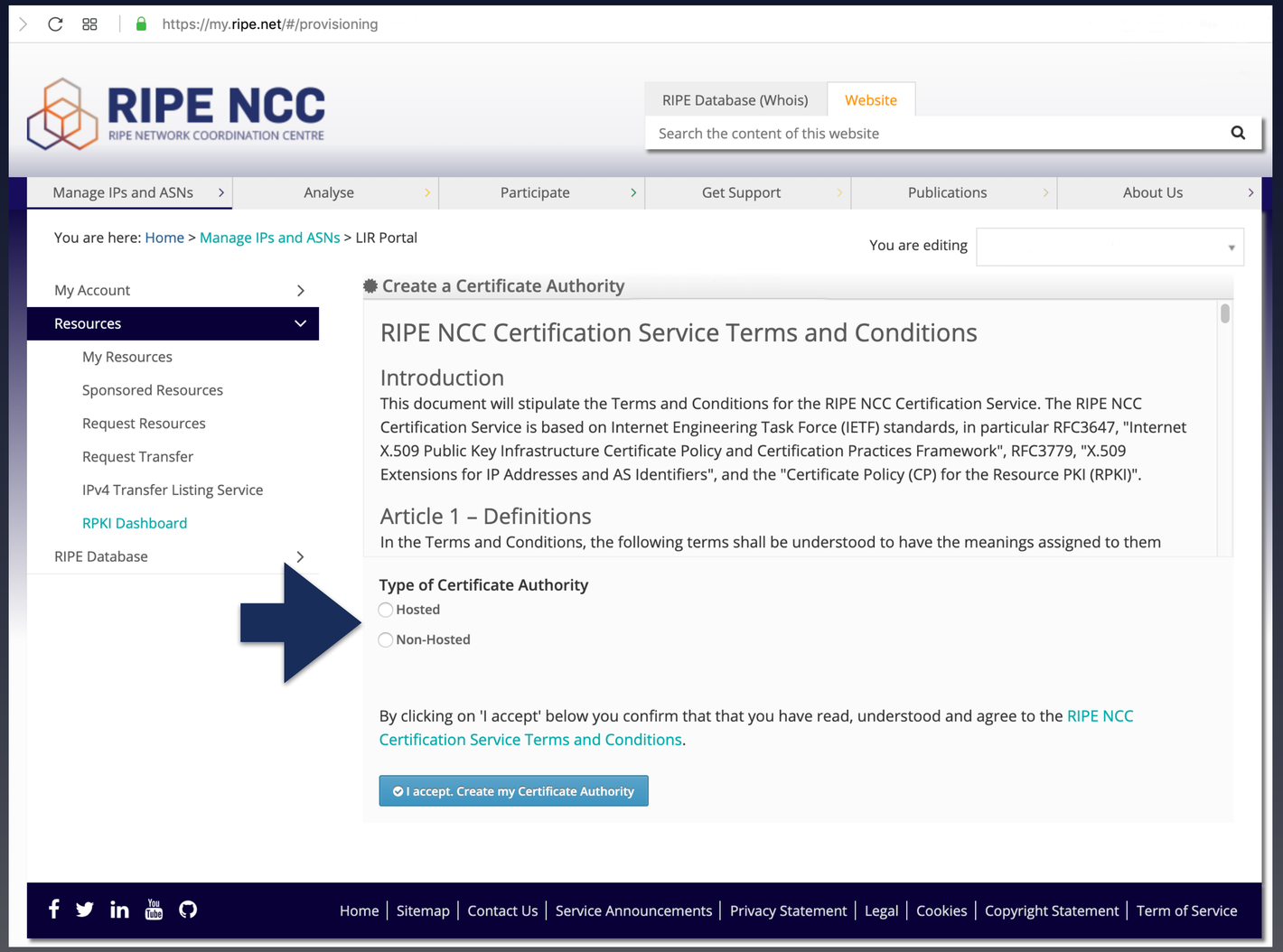
Creating RPKI Objects: Running Your Own CA

- **Install RPKI CA software**
  - Dragon Research Labs rpki.net RPKI toolkit
  - NLnet Labs Krill
- **Enable non-hosted CA on LIR Portal**
- **Set up 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)**

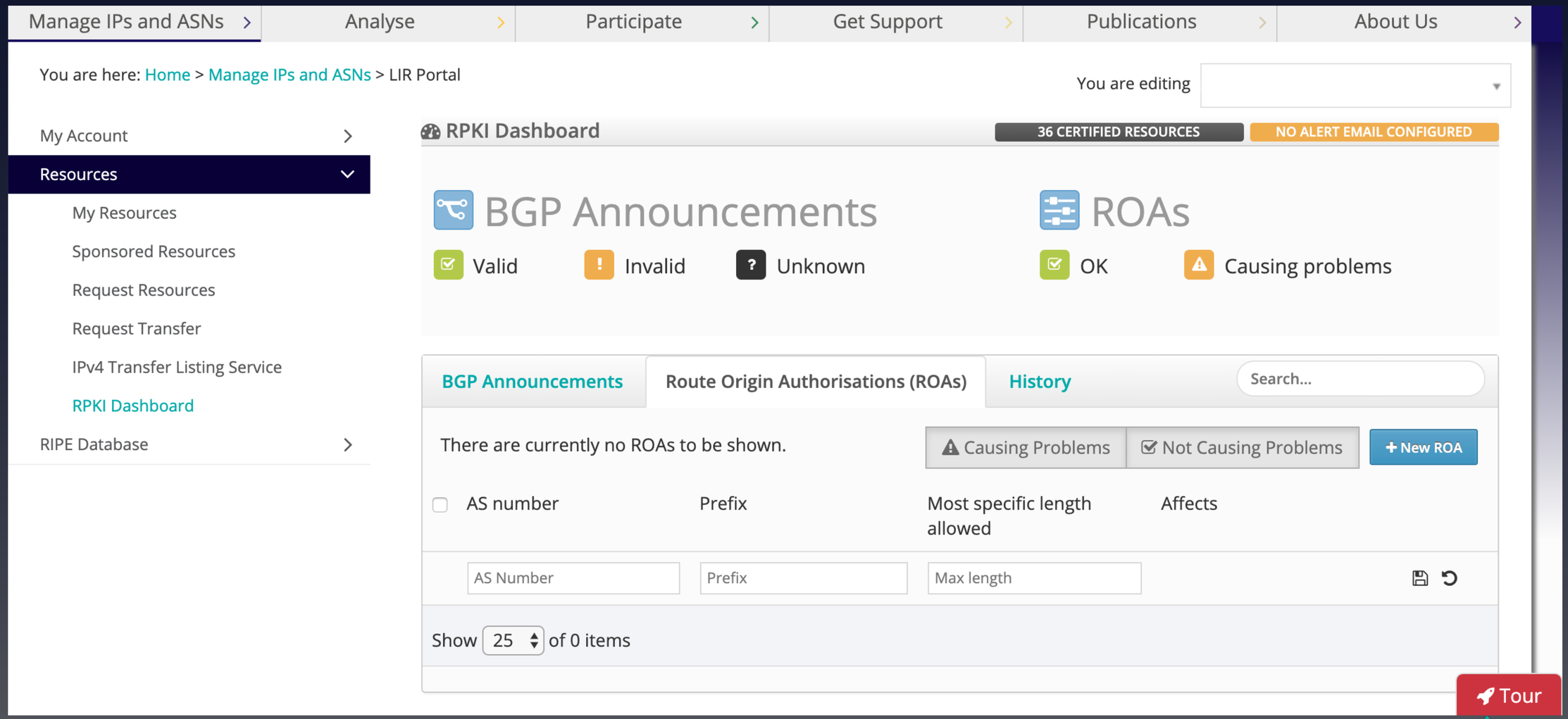
Creating RPKI Objects: Using Hosted CA

- Install RPKI CA software
  - Dragon Research Labs rpki.net RPKI toolkit
  - NLnet Labs Krill
- Enable non-hosted CA on LIR Portal
- Set up 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)

Enable Hosted CA on the LIR Portal

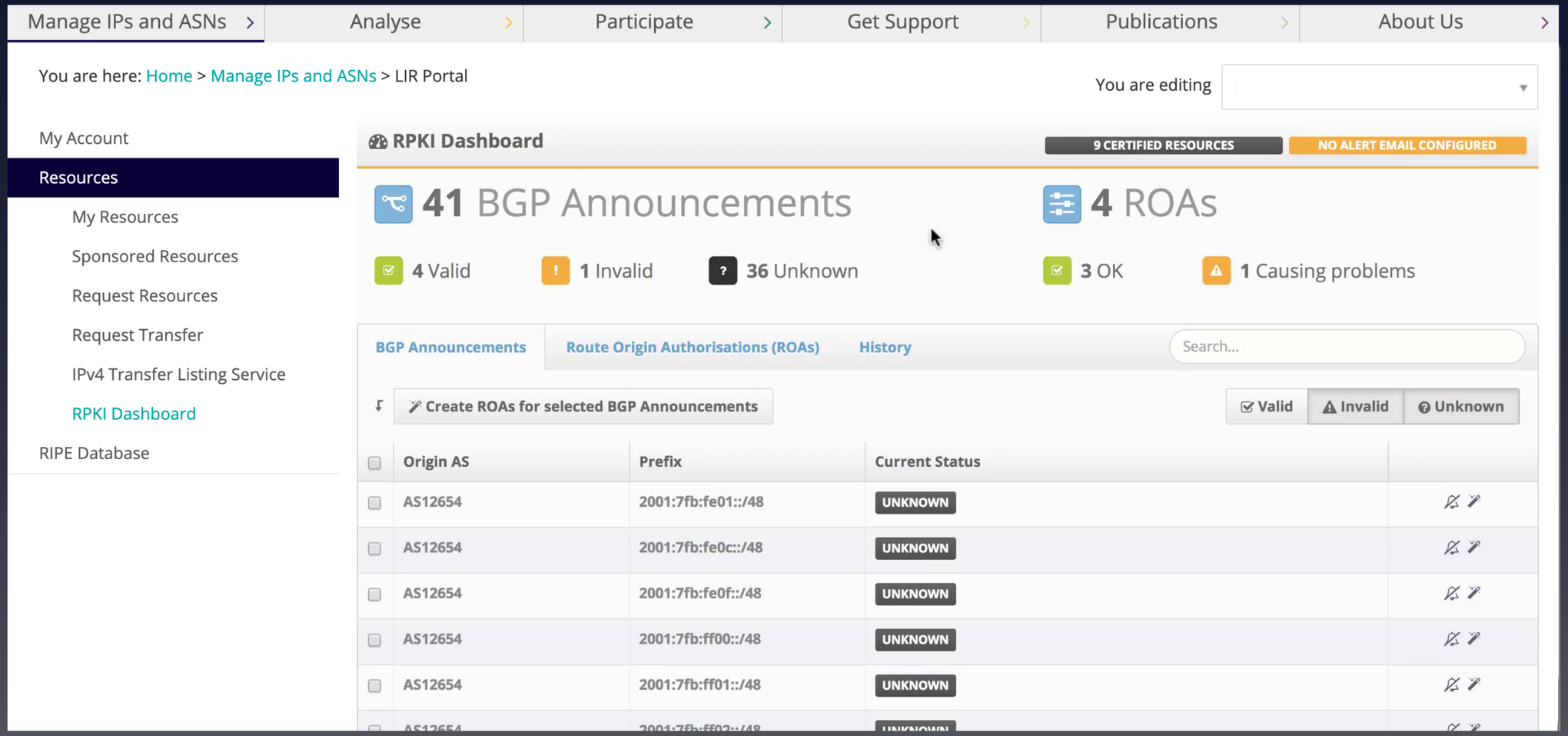


Create Your ROA Objects in a Hosted CA



https://youtu.be/gLwHp12wOGw

Create Your ROA Objects in a Hosted CA



Creating RPKI Objects: Using Hosted CA

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

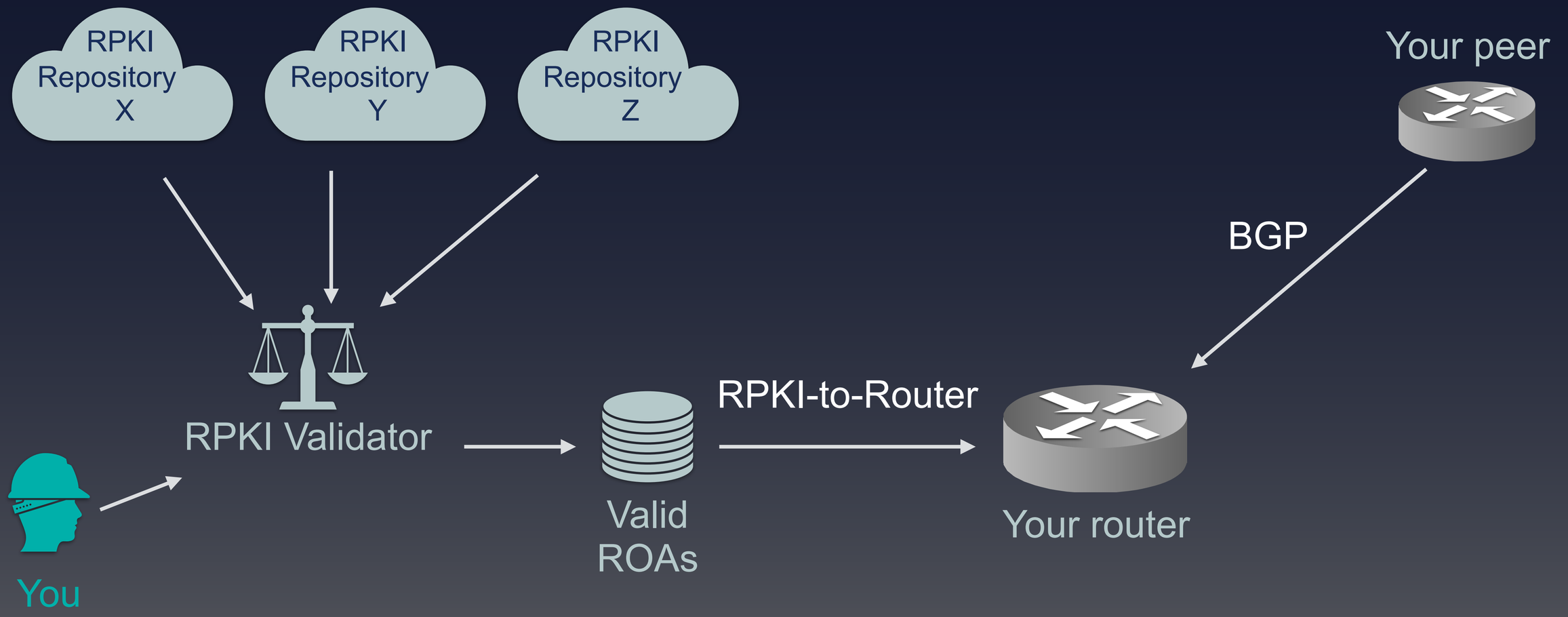
45 seconds
(if you know your RIPE NCC Access password)

Hosted CA for PI End Users

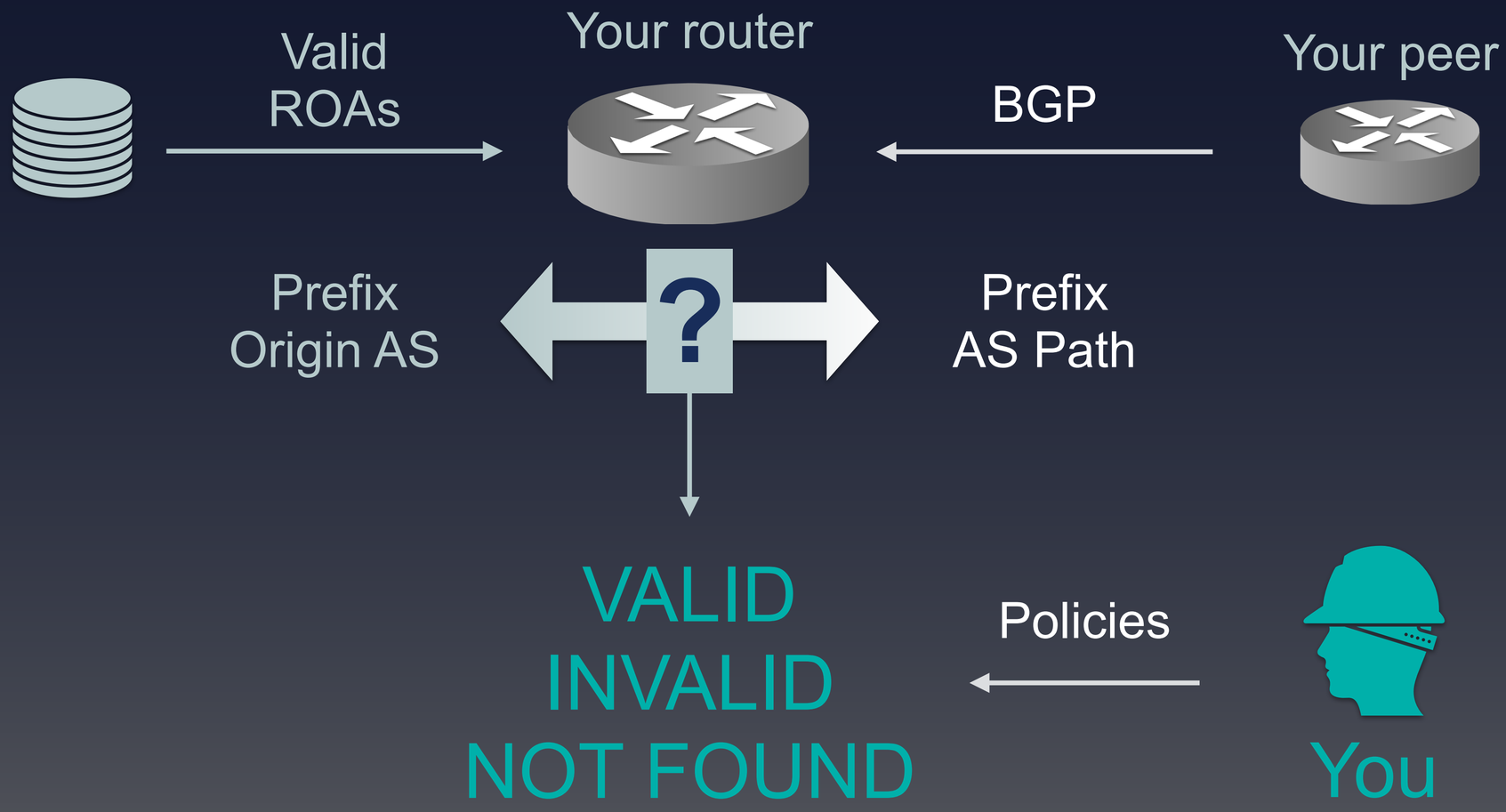
- By default, RPKI for PI resources is managed by the sponsoring LIR
- Your sponsoring LIR could make you the maintainer of an inetnum object for your resources in the RIPE DB
- Then you could link your RIPE NCC Access account to that maintainer
- …and enable your own RPKI CA
- Documentation

Validating received routes

Validating Route Announcements



Validating Route Announcements



Validating Route Announcements: Policies

- Prefer VALID over others
- Prefer NOT FOUND over INVALID
- Reject INVALID?
  - "There are too many of them!"

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 implements Path Validation, but too difficult for current hardware**
- **Work in progress:**
  - Autonomous System Provider Authorization (ASPA)
- **Don’t wait, start now**

Recommendations

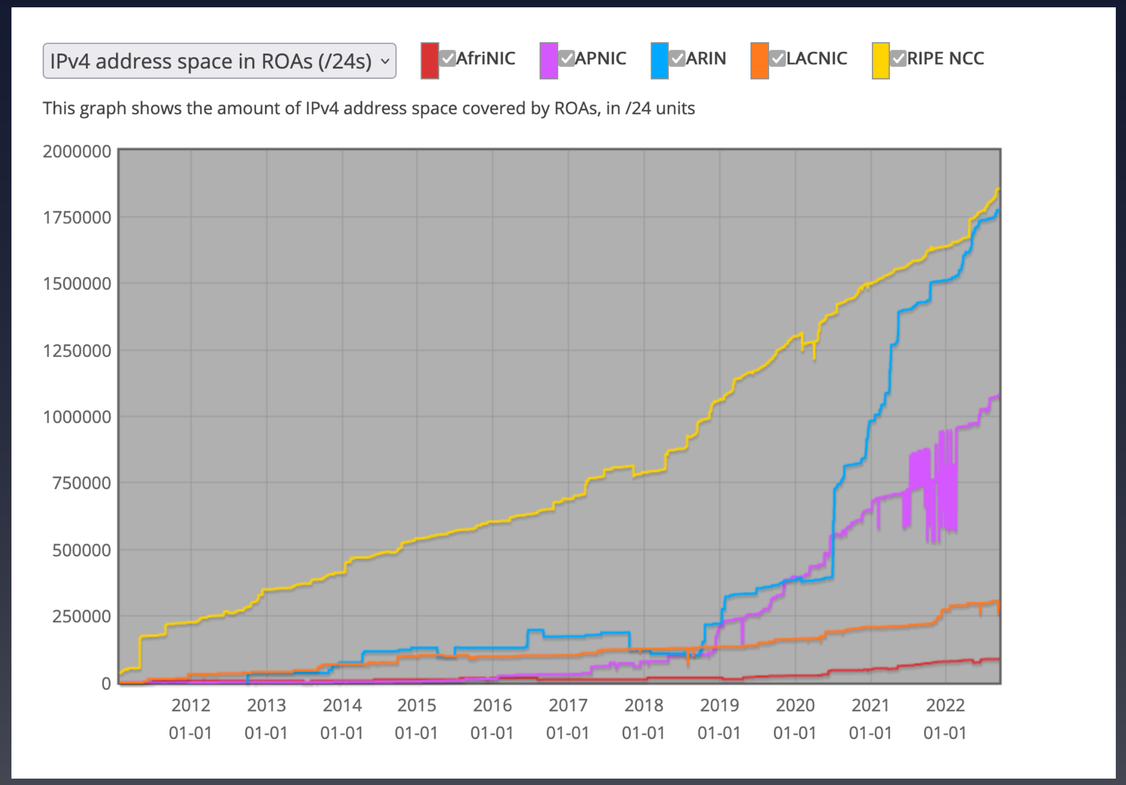
- Create Your ROAs
  - “My network becomes safer if you implement both signing and validation”
  - Pay attention to the maxLength
- Download a Validator, or two
- Check validation status manually: which routes are invalid?
- Set up monitoring, for example BGPalerter or pmacct

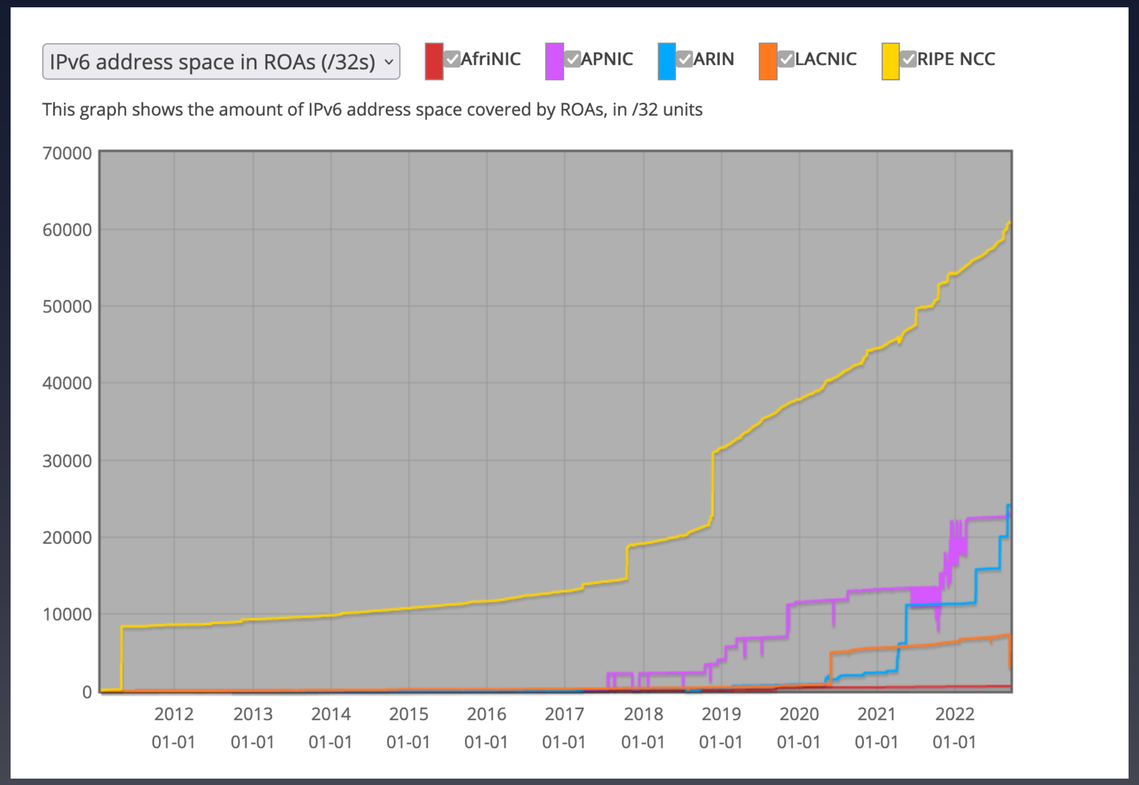
Making the Difference

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

Recent developments

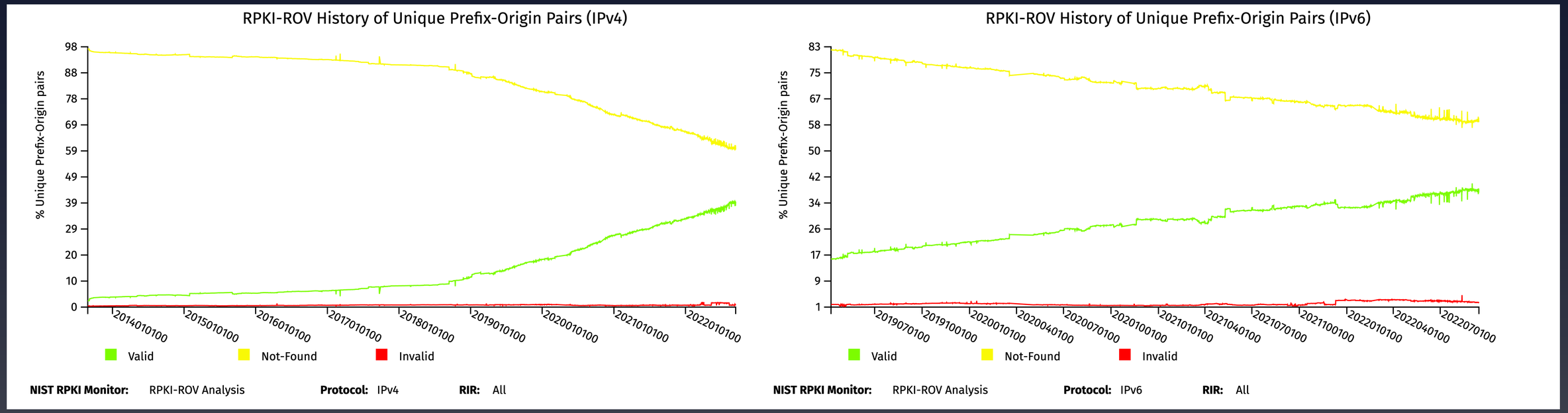
Address Space Covered by ROAs





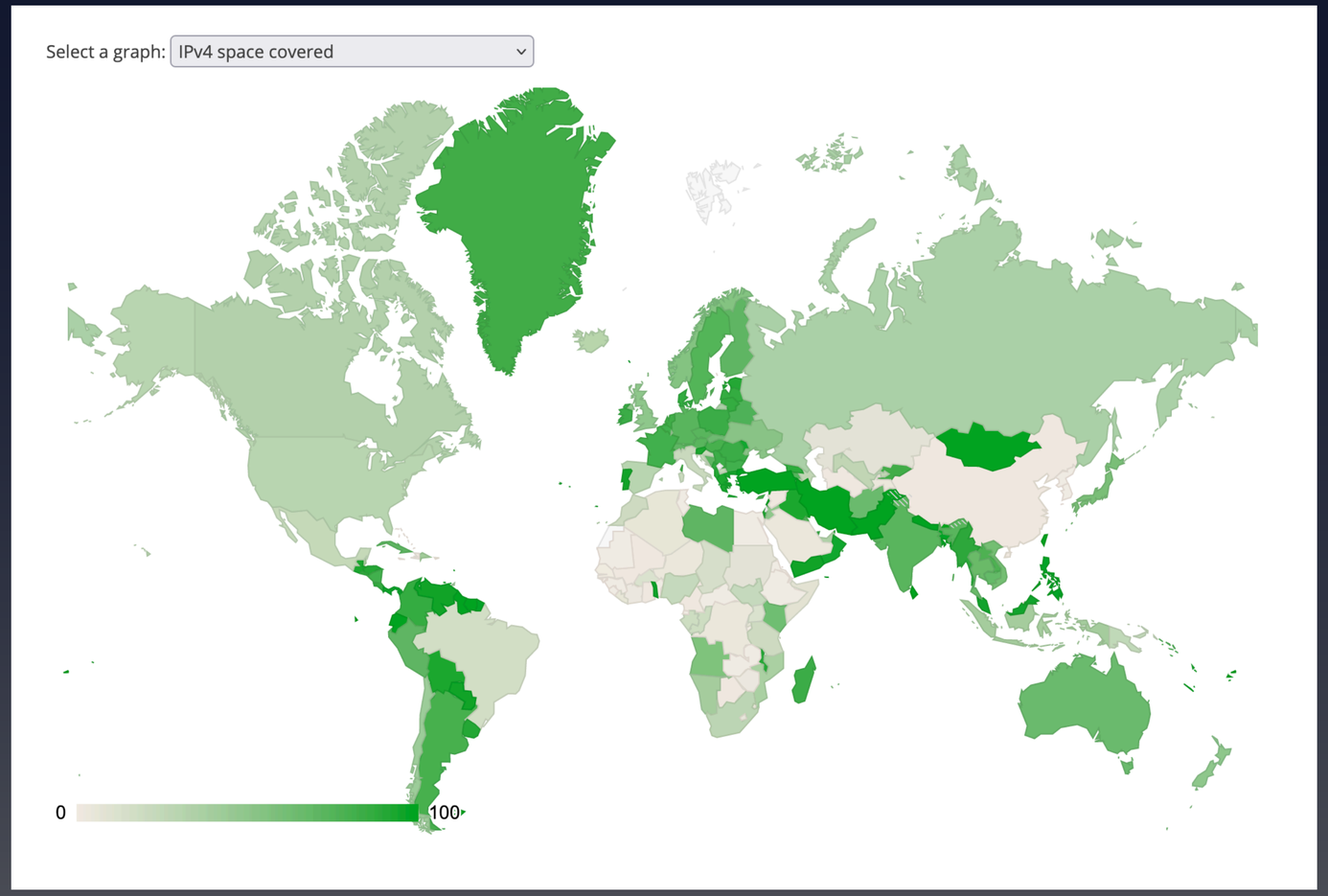
source: https://certification-stats.ripe.net/

Status of Routing Announcements



source: https://rpki-monitor.antd.nist.gov

IPv4 ROA Coverage (all RIRs)



AF	66%
IR	98%
KG	82%
KZ	8%
PK	98%
TJ	4%
TM	1%
UZ	26%

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

Recent developments

at the RIPE NCC

RIPE NCC RPKI Numbers

- 18,414 RPKI certificates
  - More than 75% of members
- 32,839 ROAs
  - More than 50% of the RIPE NCC's address space
  - 17% of members with certificates do not have ROAs

RIPE NCC RPKI Trust Anchor and Certification Authority

- **Improving security**
  - Finished migration to a new offline Hardware Security Module (HSM)
  - Planning migration to a new online HSM later this year
  - Regular penetration tests for our software
  - Red-team test (overall security exercise) this year

RIPE NCC RPKI Trust Anchor and Certification Authority

- **Improving transparency**
  - Updated RIPE NCC Certification Practice Statement
    - Next version will be reviewed by the community
  - All security test reports from external parties available online
  - We are transparent about our priorities and publish our quarterly plans
  - We open-sourced our RPKI CA code this year
    - Other parts are already open source

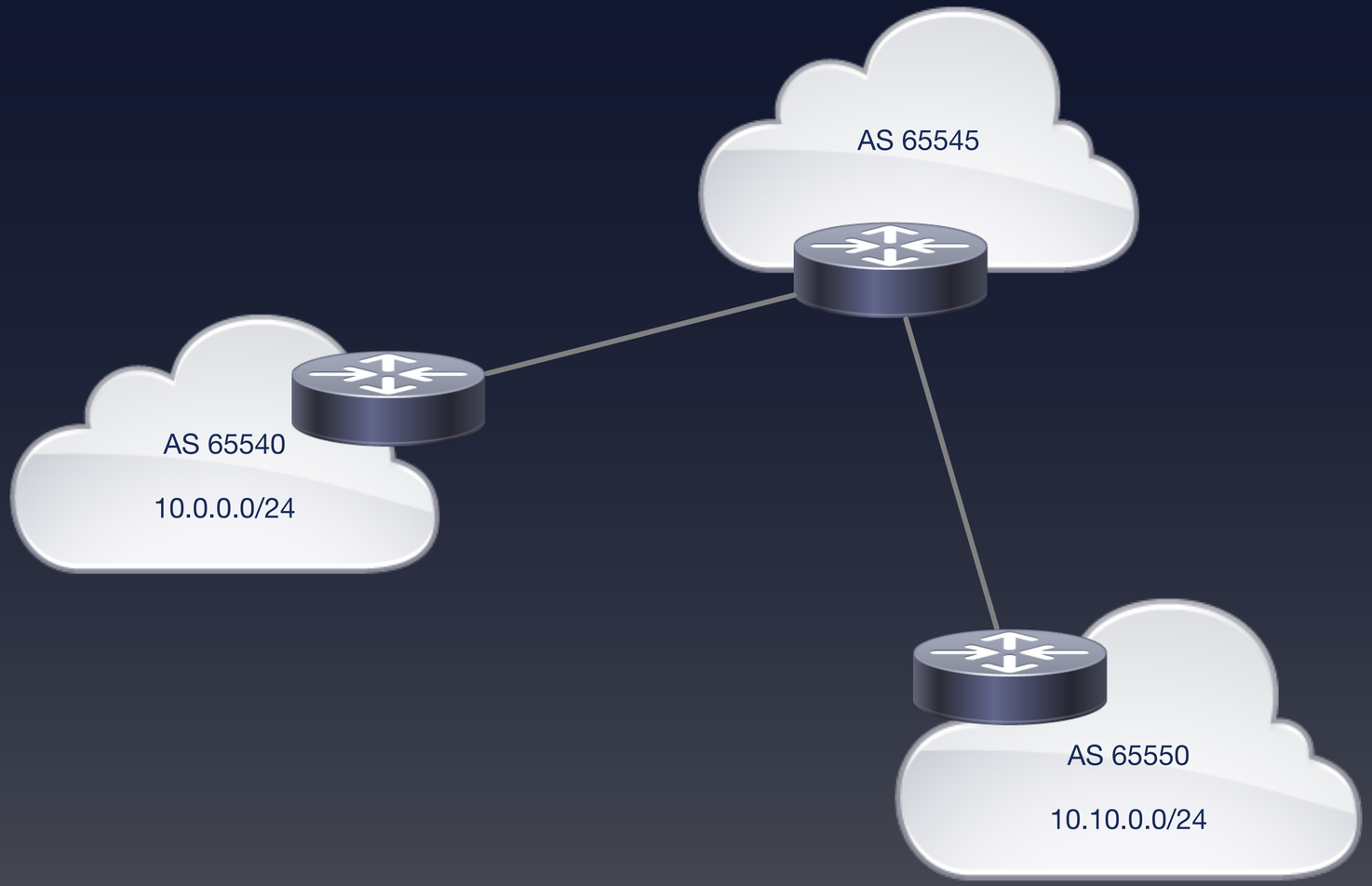
RIPE NCC RPKI Trust Anchor and Certification Authority

- **Improving auditability**
  - The RIPE NCC established an RPKI audit framework
  - ISAE 3000 Type 1 & 2
    - Type 1: Audit the framework
    - Type 2: Audit RPKI
  - We expect to have Type 1 done this year

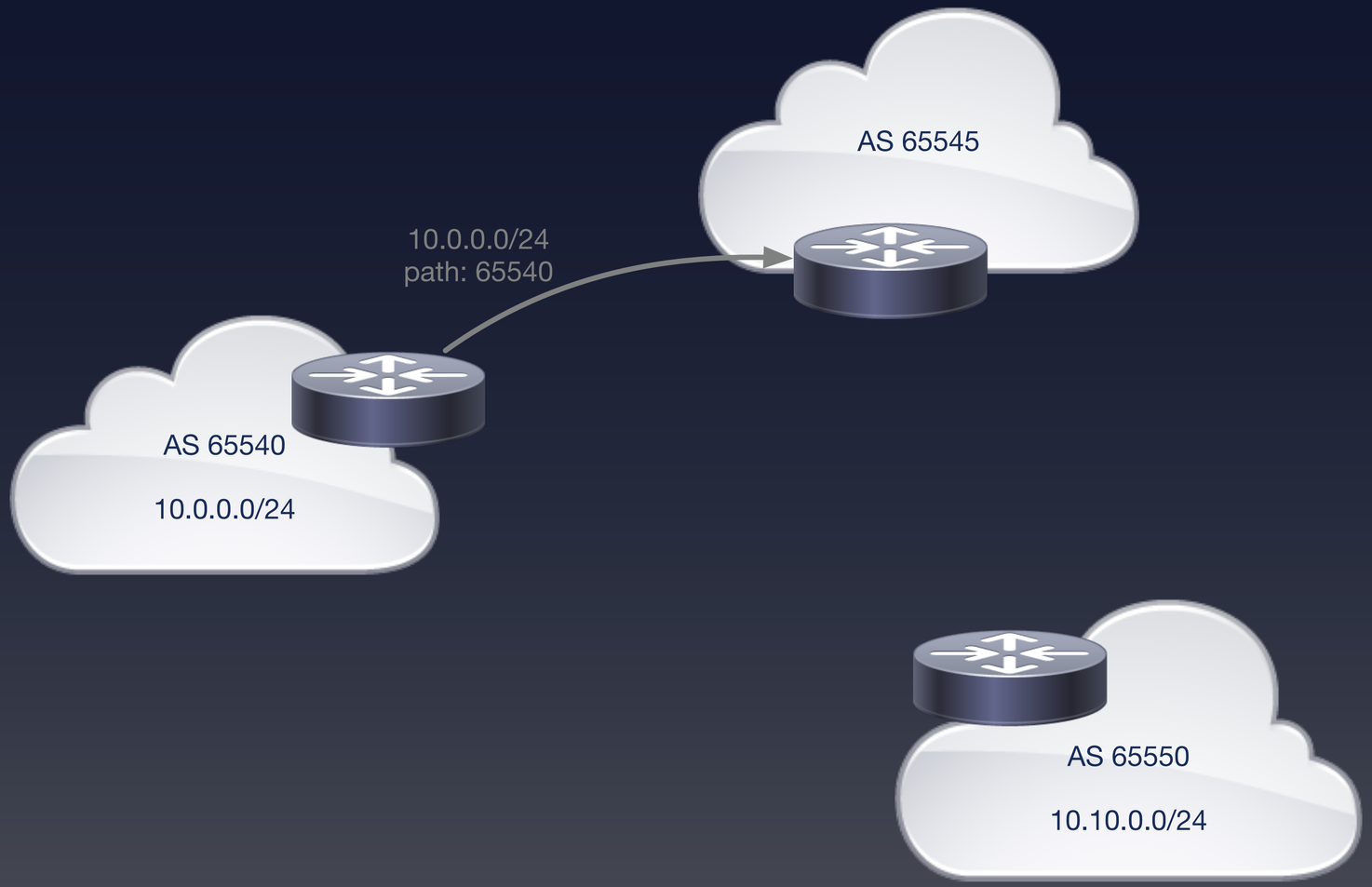
Questions

ncc@ripe.net

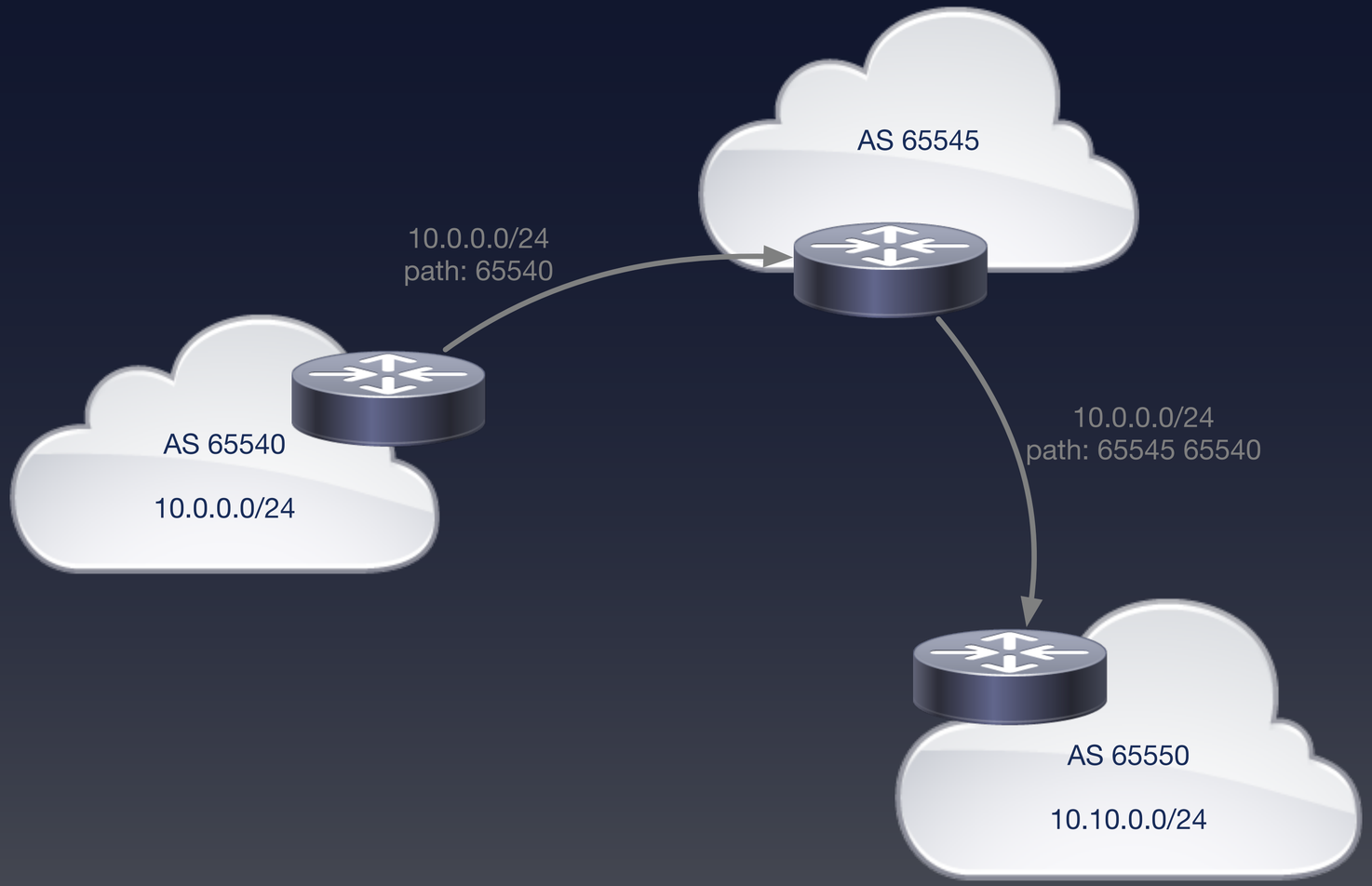
Autonomous Systems



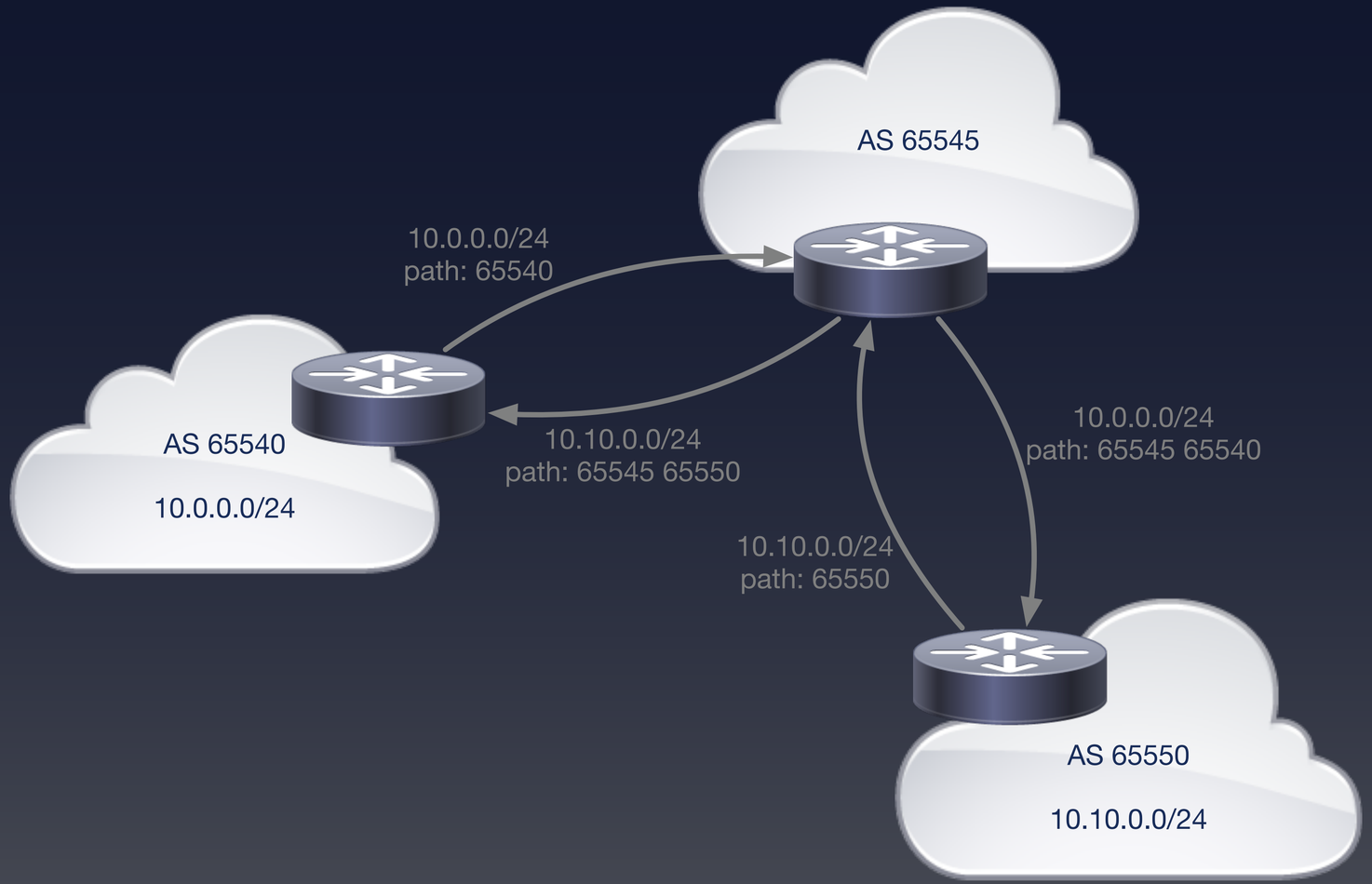
Origin AS


AS 65545
10.0.0.0/24
path: 65540
AS 65540
10.0.0.0/24
AS 65550
10.10.0.0/24

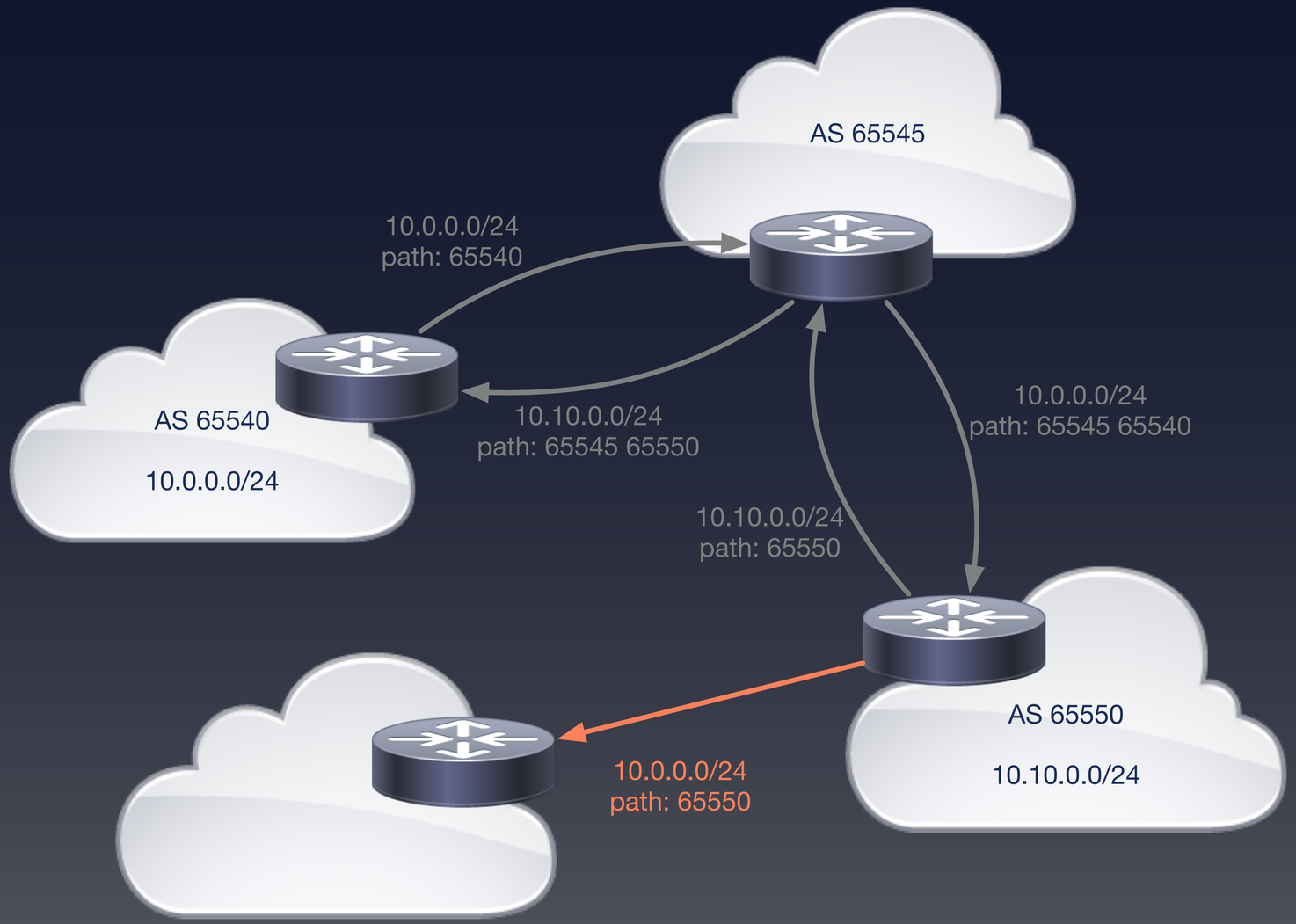
Origin AS and AS_PATH



Origin AS and AS_PATH



Origin hijack



AS_PATH hijack