



**RIPE NCC**

RIPE NETWORK COORDINATION CENTRE

# BGP Routing Security: Update and Stats

Alvaro Vives  
RIPE NCC

ESNOG 29 | 19 May 2023

# What is the RIPE NCC?



Internet Assigned Numbers Authority



## RIR = Regional Internet Registry

- Not-for-profit organisation
- Funded by membership fees
- Policies developed by regional communities
- Neutral, impartial, open, and transparent

- 
- A magnifying glass is held over a blurred background, focusing on a list of items. The magnifying glass is positioned in the center of the frame, with its handle extending towards the bottom right. The background is a soft, out-of-focus gradient of blue and orange, suggesting a sunset or sunrise over water. The list of items is centered within the magnifying glass's lens.
- **Origin Hijack**
  - **RPKI**
  - **Stats for Spain**



**RIPE NCC**  
ACADEMY

# BGP Security E-learning Course

- ✓ Free online course
- ✓ Interactive, you can study at your own pace
- ✓ Practical lab environment and activities



[academy.ripe.net/bgp-security/](https://academy.ripe.net/bgp-security/)

My network - AS100

Router 1

[open logs](#) [reconnect](#) [pop out](#)

```
AS100 - R1 router  
R1#
```

"ubuntu-focal" 15:01 24-Aug-22

[open logs](#) [reconnect](#) [pop out](#)

```
100 - R3 router  
R3#
```

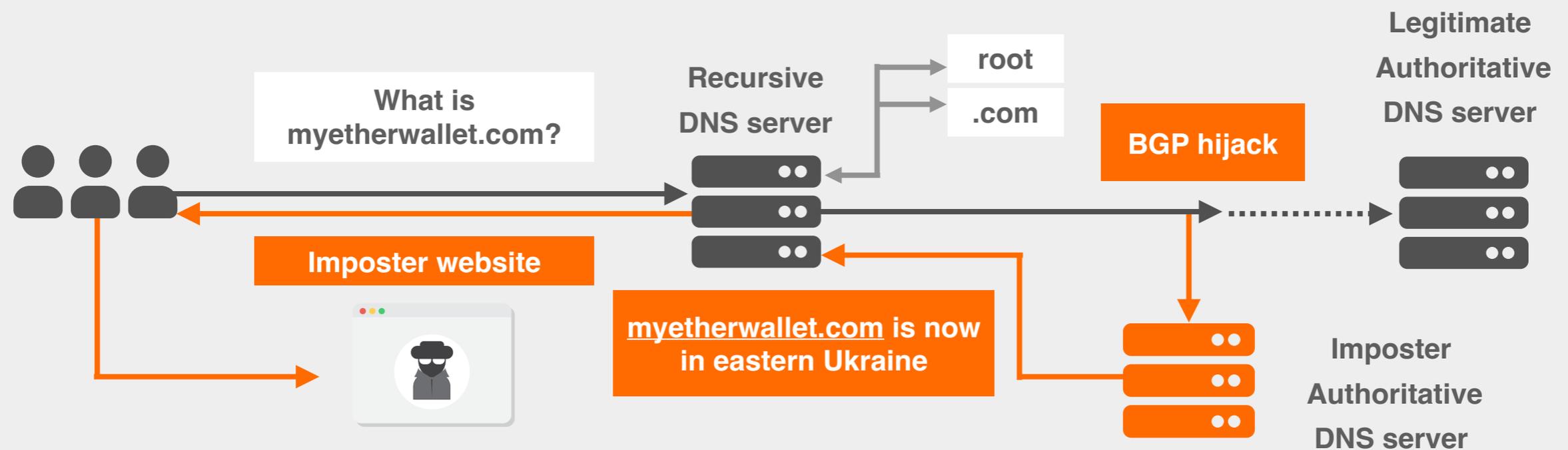
[R3-vtysh]0: lxc\*

"ubuntu-focal" 15:01 24-Aug-22

# April 2018: Amazon-MyEtherWallet



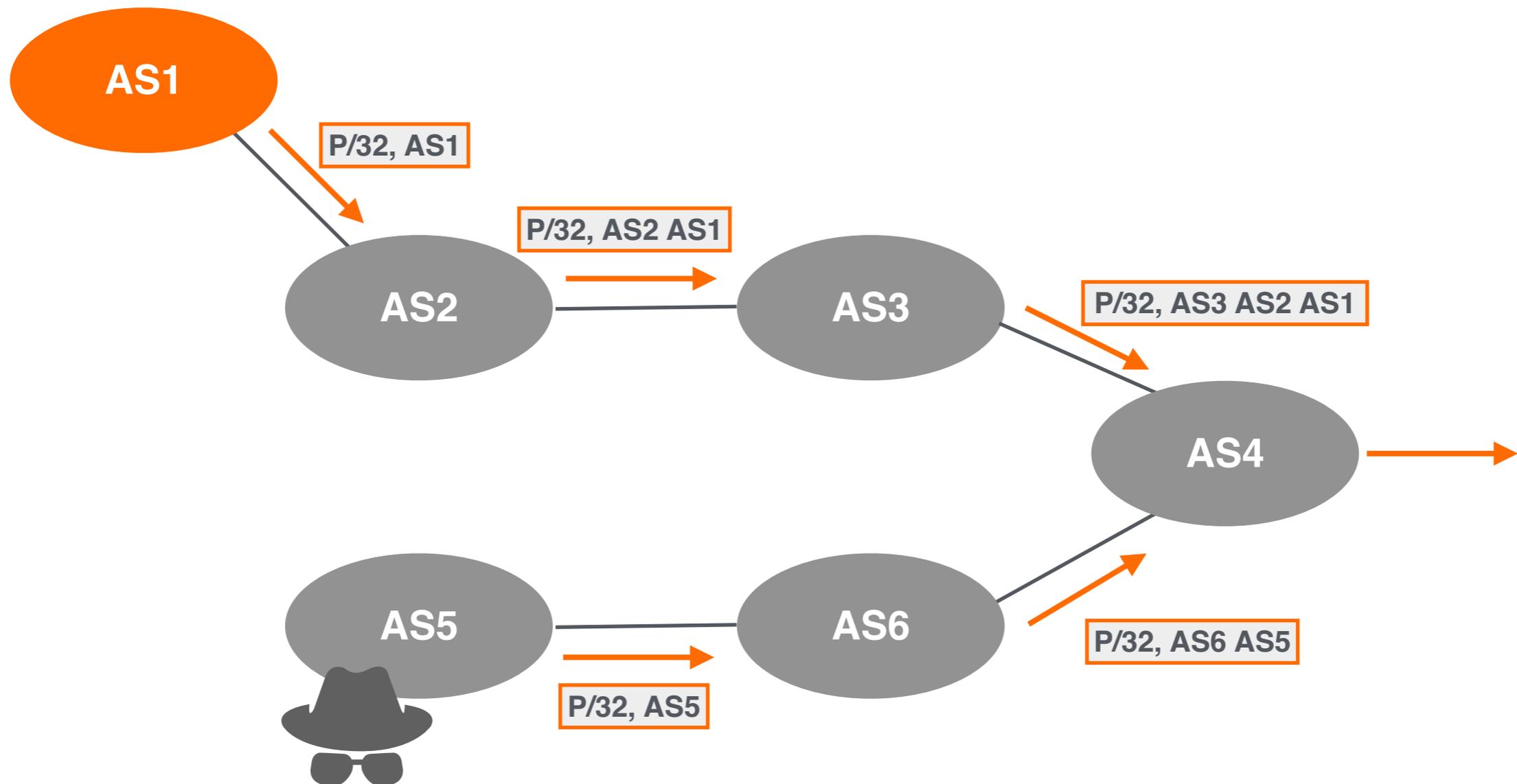
- BGP hijack of Amazon DNS
- How did it happen?
- Why? To steal cryptocurrency



# Origin Hijack: Same Prefix



Prefix-P, 2001:db8::/32



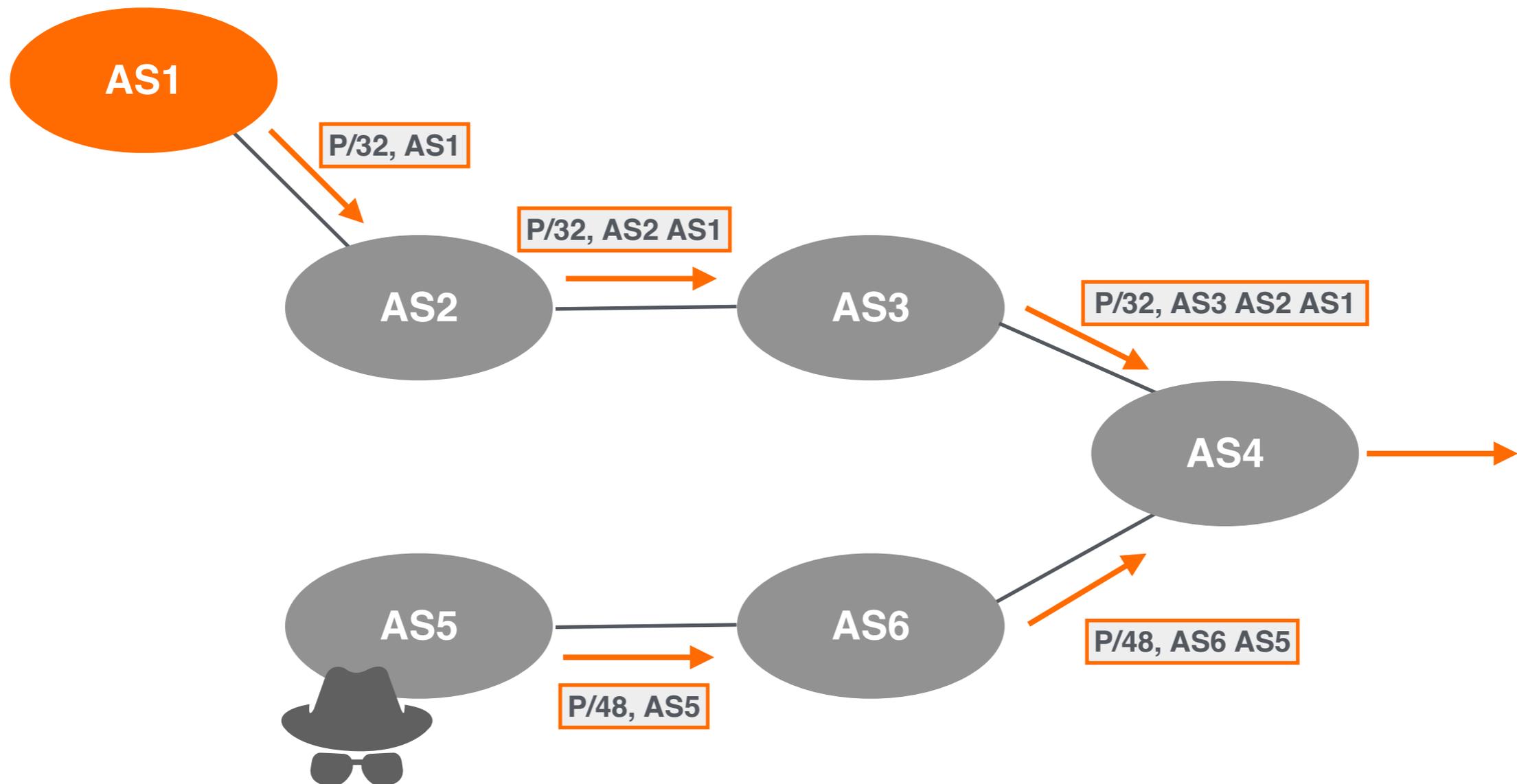
This is a **local hijack!**

Only some networks are affected based on BGP path selection process.

# Origin Hijack: More Specific Prefix



Prefix-P, 2001:db8::/32



This is a **global hijack!**

All traffic for more specific will be forwarded to the attacker's network network.



# What is RPKI?



- A security framework using Public Key Infrastructure and **Resource certification** (X.509 PKI certificates) for BGP route origin validation (ROV)
- Allows resource (IPs) holders to prove ownership, and create authorisations (ROAs)
- ASNs can use ROAs to validate the origin of BGP announcements
  - Is the originating ASN authorised to originate a particular prefix?



# How does it work?



# Elements of RPKI



- RPKI system consists of two parts...

## SIGNING

Create ROAs for your prefixes  
in the RPKI system



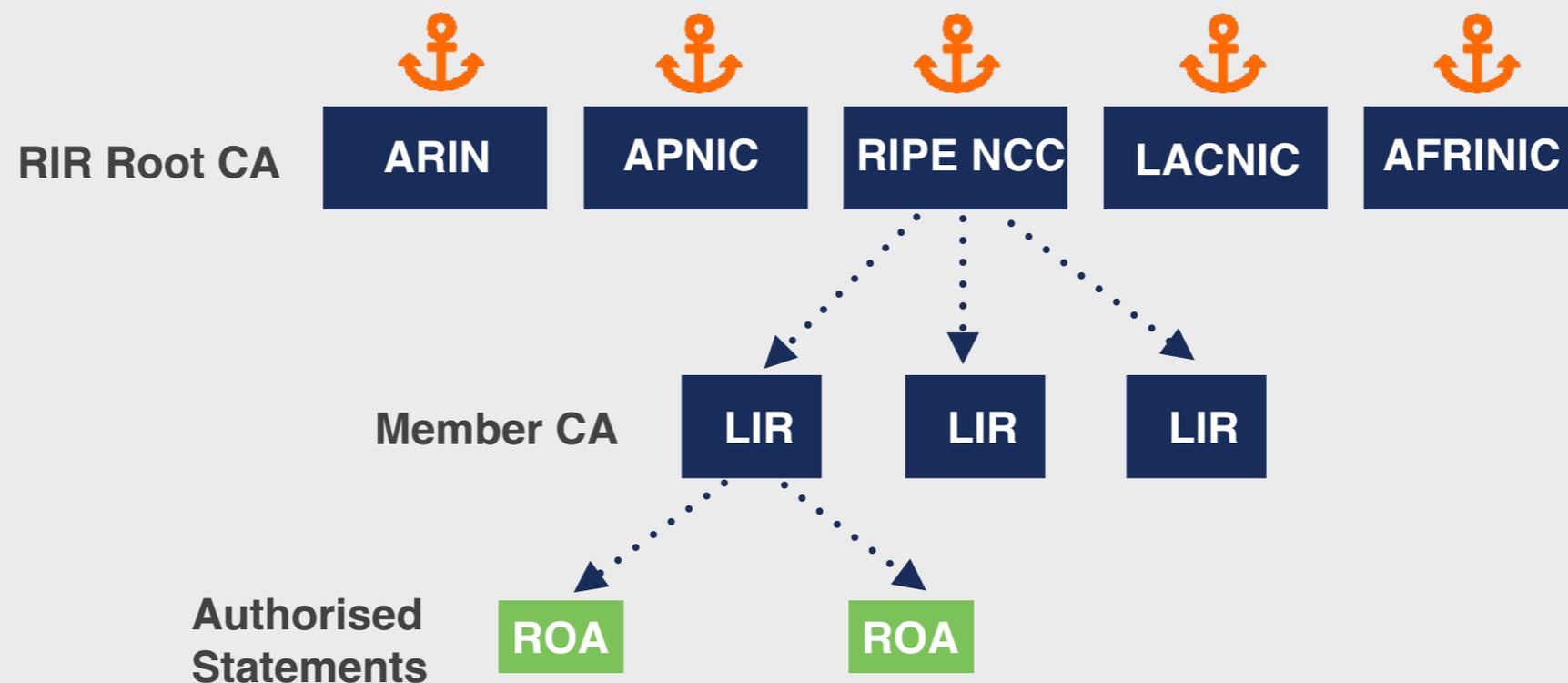
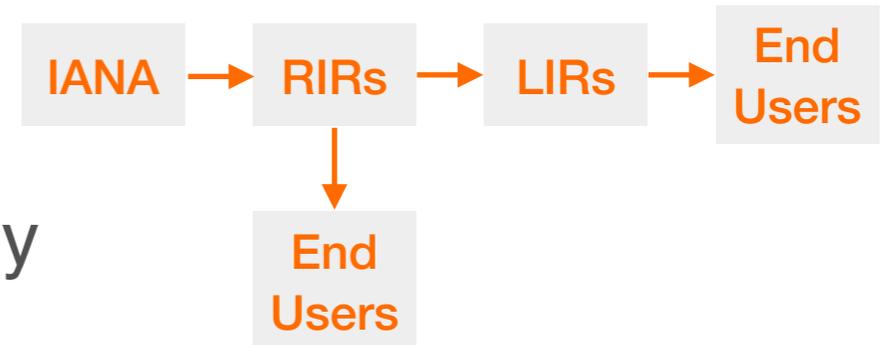
## VALIDATION

Verify the information  
provided by others

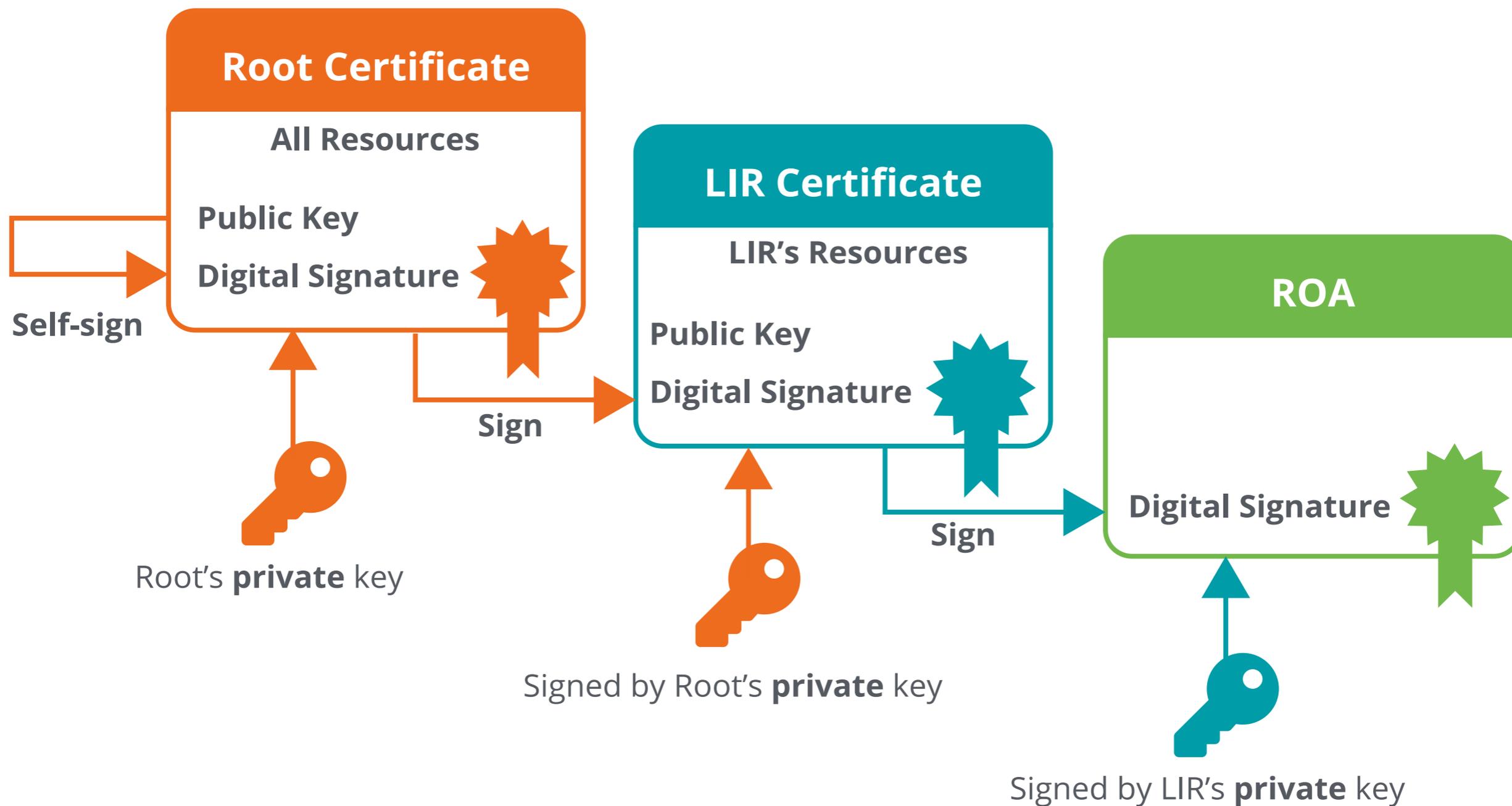
# Trust in RPKI



- RPKI relies on five RIRs as Trust Anchors
- Certificate structure follows the RIR hierarchy
- RIRs issue certificates to resource holders



# RPKI Chain of Trust





# What are ROAs?

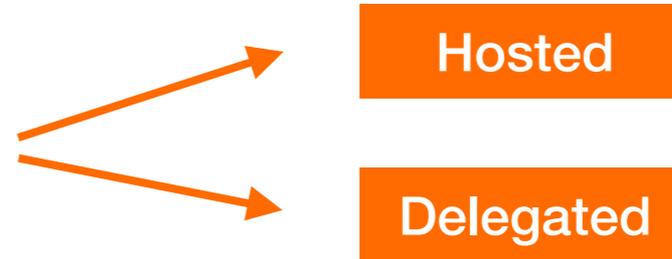
- An **authorised statement** created by the resource holder
- States that a certain prefix can be originated by a certain AS
- LIRs can create ROAs for their resources
- Multiple ROAs can exist for the same prefix
- ROAs can overlap

ROA	
Prefix	2001:db8::/48
Max Length	/48
Origin ASN	AS65536



# How to create a ROA?

- Login to LIR Portal ([my.ripe.net](https://my.ripe.net))
- Go to the RPKI Dashboard
- Choose which RPKI model to use



The screenshot shows the LIR Portal interface. On the left is a dark blue sidebar with a menu. The 'RPKI RPKI Dashboard' item is circled in orange. An orange arrow points from this menu item to a form titled 'Create a Certificate Authority for bh.viacloud'. The form contains the following text:

**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**

**Type of Certificate Authority**

You can choose between asking the RIPE NCC to host your RPKI Certificate Authority (Hosted RPKI) or running your own Certificate Authority (Delegated RPKI).

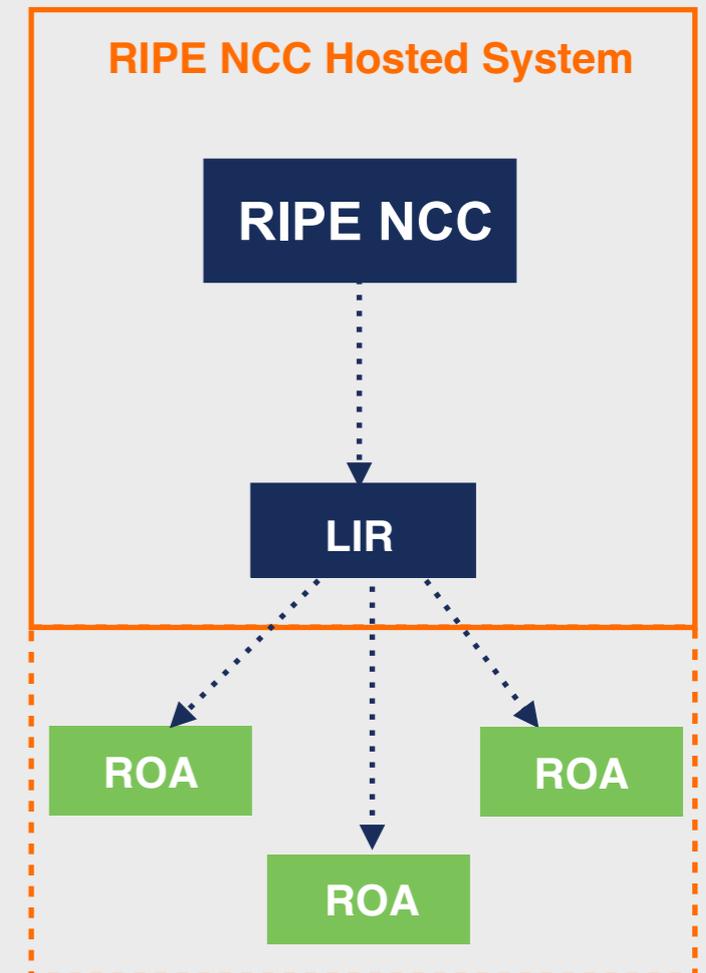
Select "Hosted" if you would like the RIPE NCC to host your Certificate Authority keys, ROAs ,manifests etc. and publish the information in our repository. You will only need to maintain your ROAs in our dashboard. This is the recommended option if you are not an RPKI expert.

Select "Delegated" to run your own Certificate Authority and to host your own keys, ROAs, manifests etc. you will need to run additional software to proceed.

At the bottom of the form, there are two radio button options:  Hosted and  Delegated. The 'Hosted' option is selected and is enclosed in an orange box. An orange arrow points from the 'RPKI RPKI Dashboard' menu item to this box.

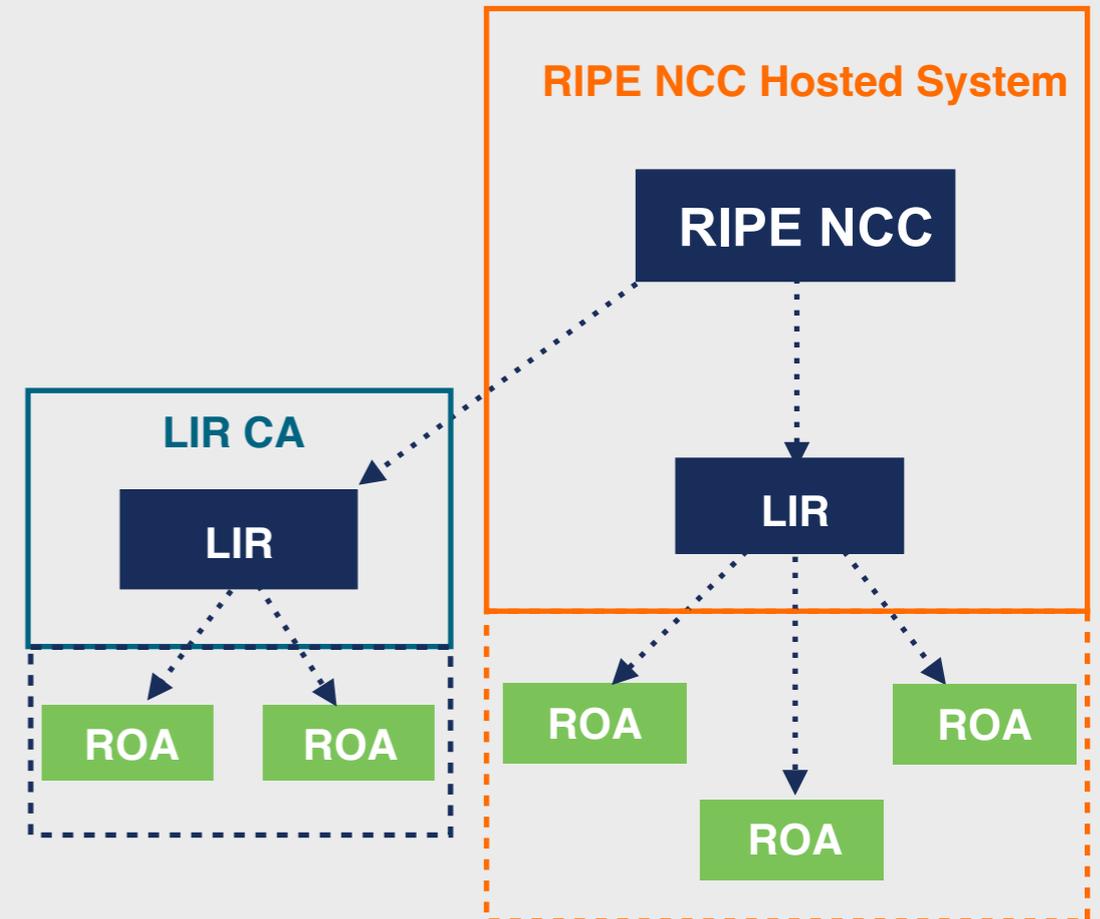
# Hosted RPKI

- ROAs are created and published using the **RIR's member portal**
- RIR hosts a CA (Certification Authority) for LIRs and signs all ROAs
- Automated signing and key rollovers



# Delegated RPKI

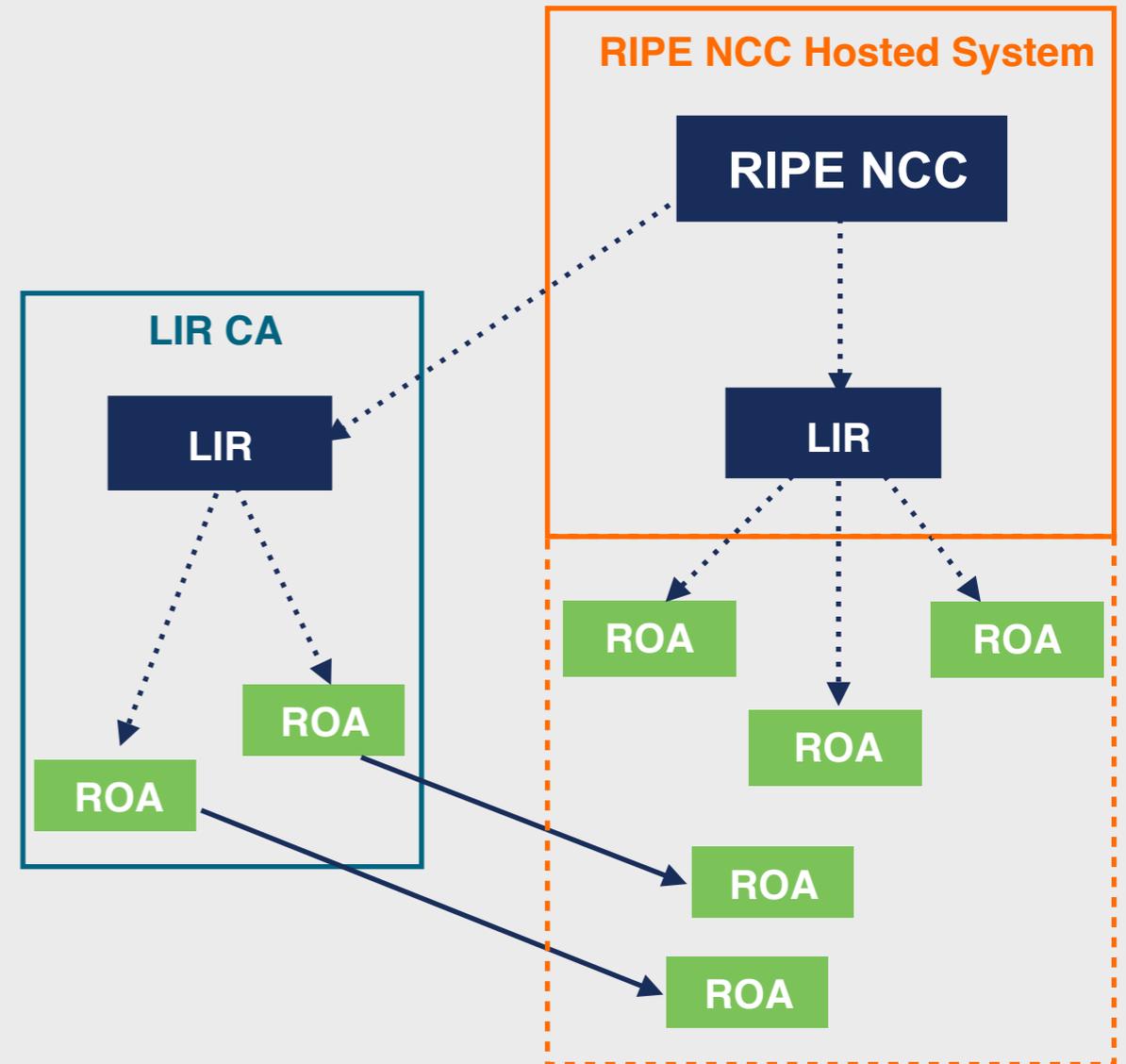
- Each LIR manages its part of the RPKI system
  - Runs its own CA as a child of the RIR
  - Manages keys/key rollovers
  - Creates, signs and publishes ROAs
- Certificate Authority (CA) Software
  - **Krill** (NLnet Labs)
  - **rpkid** (Dragon Research Labs)



# Publication as a Service

**NEW!**

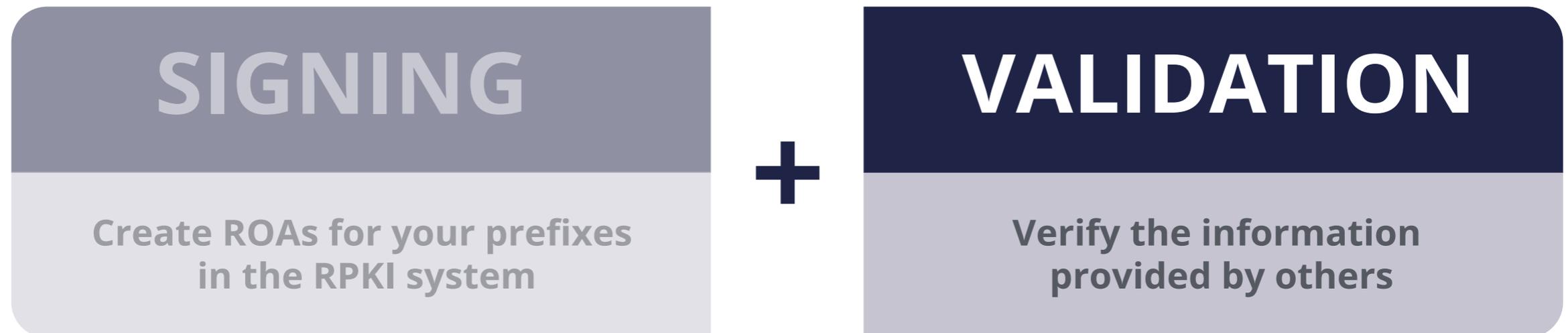
- In-between Hosted and Delegated
  - Runs its own CA as a child of the RIR
  - Manages keys/key rollovers and ROAs
  - Maintain key pairs and objects and send them to RIR
  - RIR publishes ROAs on behalf of LIR
- Also APNIC, ARIN, RIPE NCC, NIRs
- AKA “Publication in parent” or “Hybrid RPKI”



# Elements of RPKI



- RPKI system consists of two parts...



# RPKI Validation

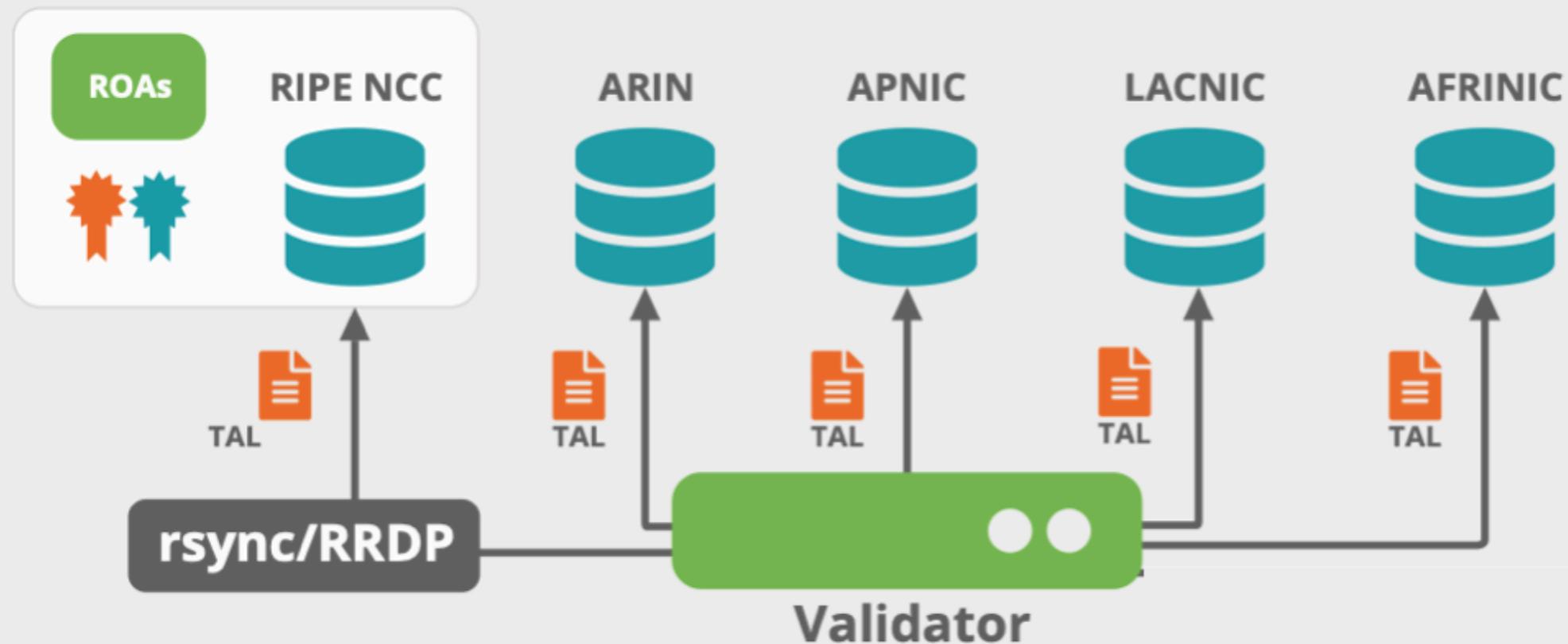


- Verifying the information provided by others
  - Proves holdership through a public key and certificate infrastructure
- In order to validate RPKI data, you need to ...
  - install a **validator software** locally in your network
- Goal is to validate the **“origin of BGP announcements”**
  - Known as BGP Origin Validation (BGP OV) or Route Origin Validation (ROV)

# RPKI Validator



- Connects to RPKI repositories via rsync or RRDP protocol
- Uses TALs to connect to the repositories and download ROAs
- Validates chain of trust for all ROAs and associated CAs
- Creates a local “**validated cache**” with all the **valid ROAs**



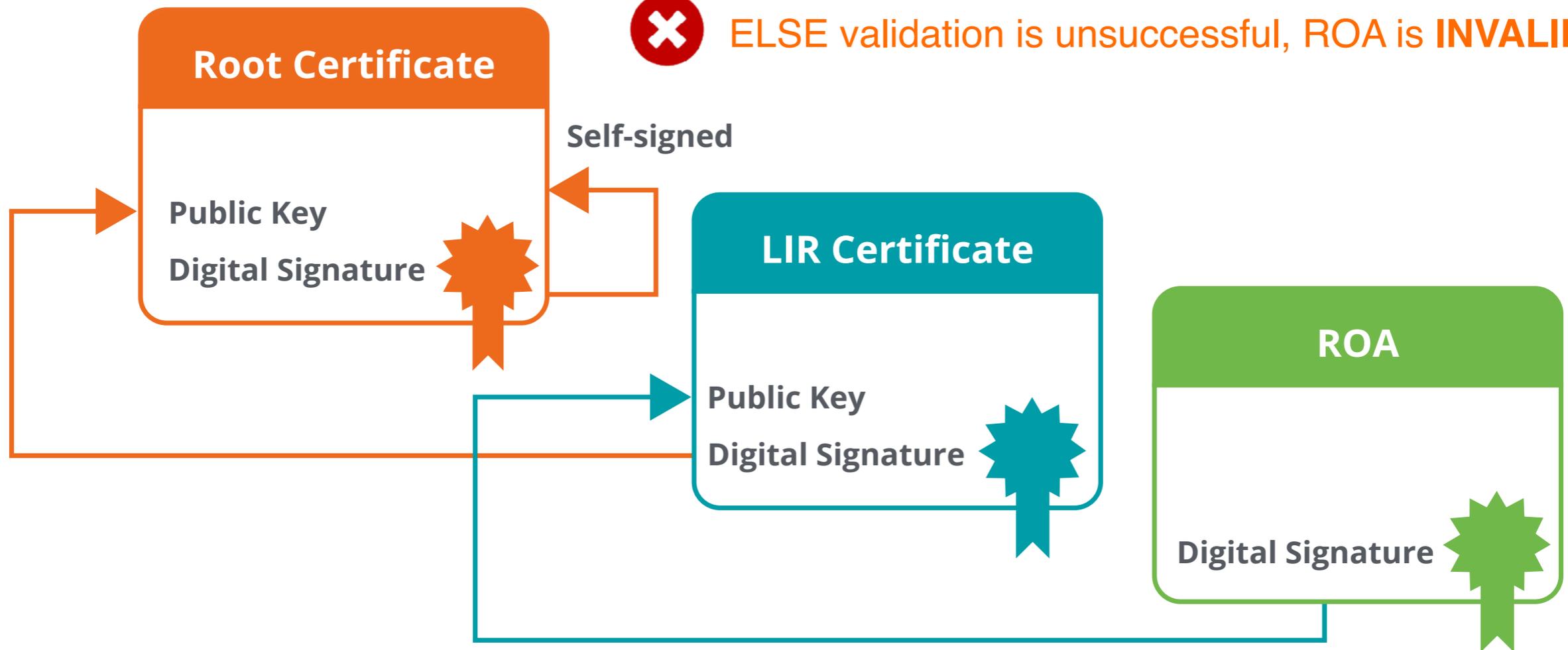
# ROA Validation Process



IF chain is complete, it means ROA is **VALID!**



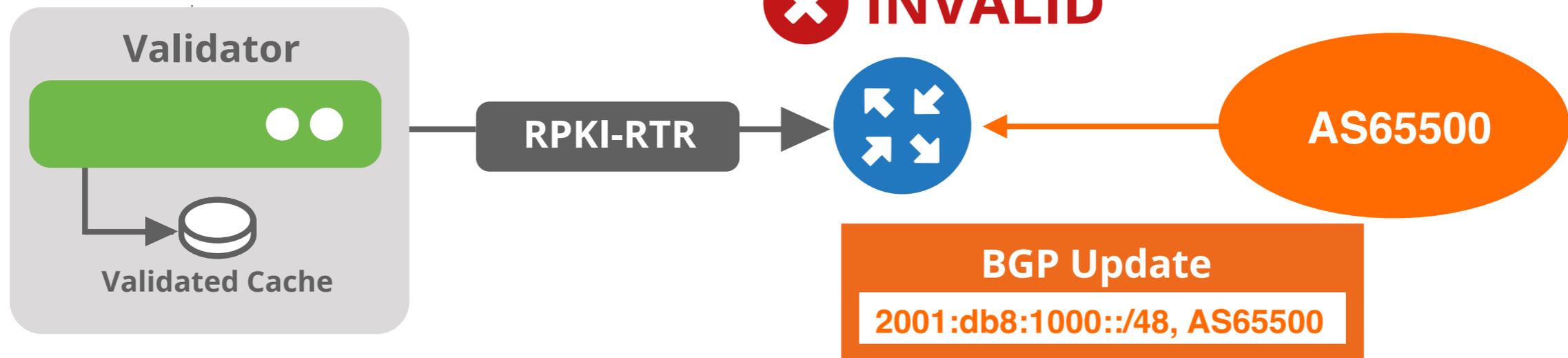
ELSE validation is unsuccessful, ROA is **INVALID!**



# Valid ROAs Are Sent to the Router!



✓ VALID  
OR  
✗ INVALID



Router uses this information to make better routing decisions!

What's New?



# RPKI Validators are Mature



- Much better than 5 years ago
- Installation, configuration, documentation is way better
- Big research work on vulnerabilities in 2021
  - Multiple fixes in all validators, mostly addressing potential DoS attacks
  - Source: <https://arxiv.org/pdf/2203.00993.pdf>

# Run Different Validators



Validator	Number (13/5/23)	%
Routinator	2297	79%
rpki-client	253	9%
OctoRPKI	181	6%
FORT	91	3%
<b>Validator</b>	<b>87</b>	<b>3%</b>
Other	6	0%

Source (13/5/23): <https://rov-measurements.nlnetlabs.net/stats/>

# RPKI Validator Options



- **Routinator**
  - Built by NLNetlabs
- **OctoRPKI**
  - Cloudflare's relying party software
- **FORT**
  - Open source RPKI validator
- **rpki-client**
  - Integrated in OpenBsd

## Links for RPKI Validators

<https://github.com/NLnetLabs/routinator.git>

<https://github.com/NICMx/FORT-validator/>

<https://github.com/cloudflare/cfrpki#octorpki>

<https://www.rpki-client.org/>

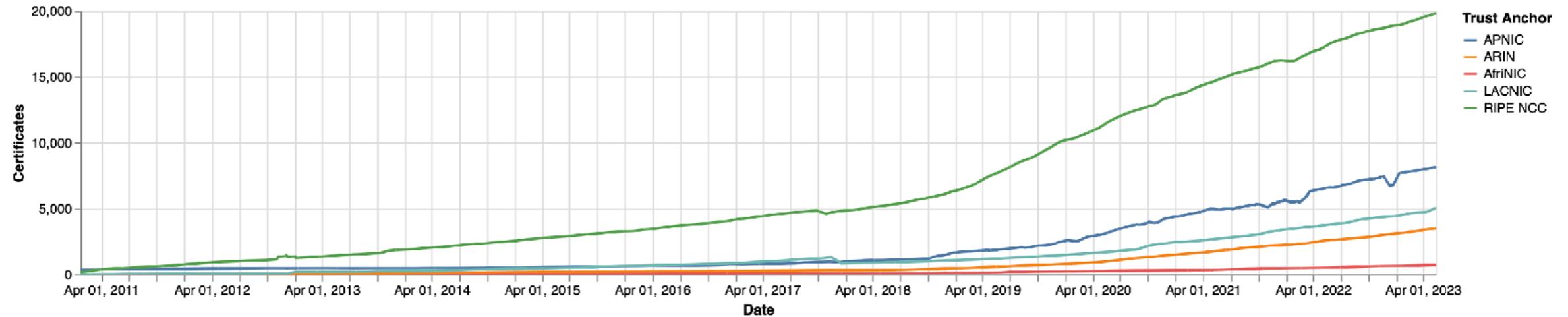
## For more info...

<https://rpki.readthedocs.io>

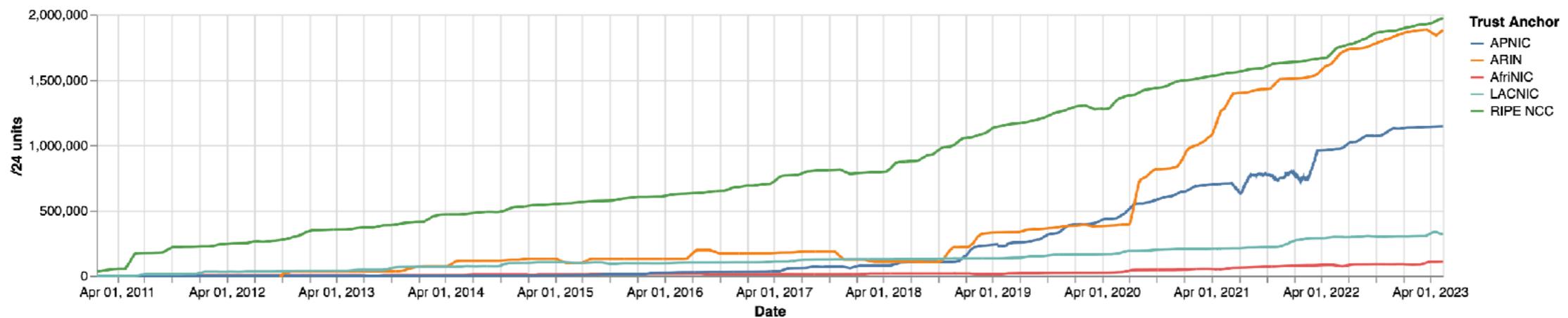
# Steady growth: Adoption and ROAs



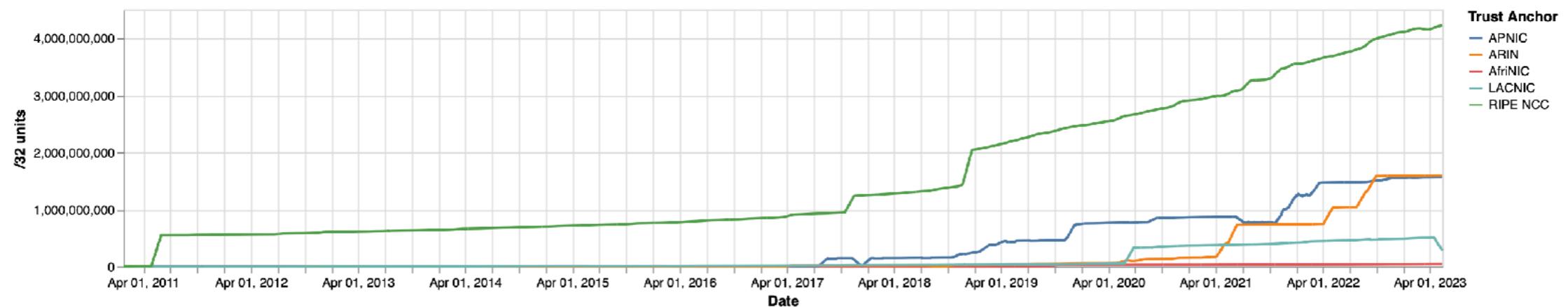
## Number of Certificates



## IPv4 address space in ROAs (/24s)



## IPv6 address space in ROAs (/32s)



Source (14/5/23): <https://certification-stats.ripe.net/>

# Adoption per RIR

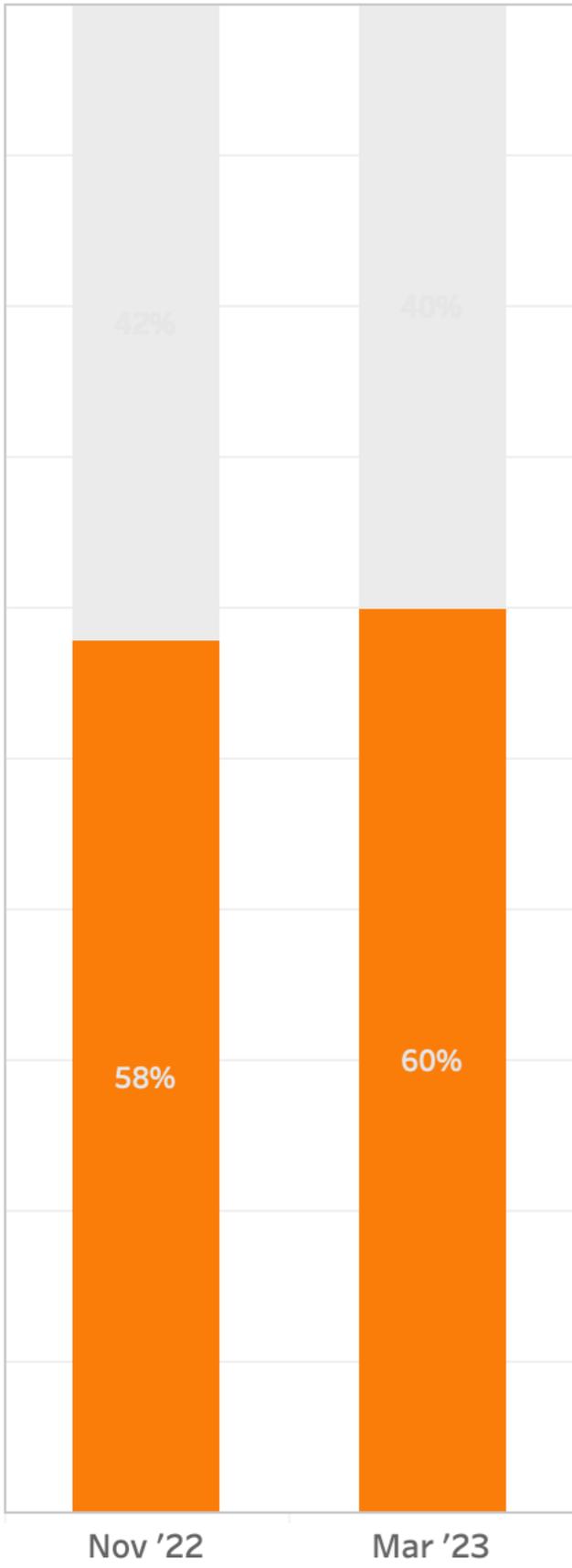


RIR	IPv4 Addr. Space	IPv6 Addr. Space
APNIC	33%	23%
RIPE NCC	61%	37%
LACNIC	42%	23%
ARIN	29%	35%
AFRINIC	25%	7%

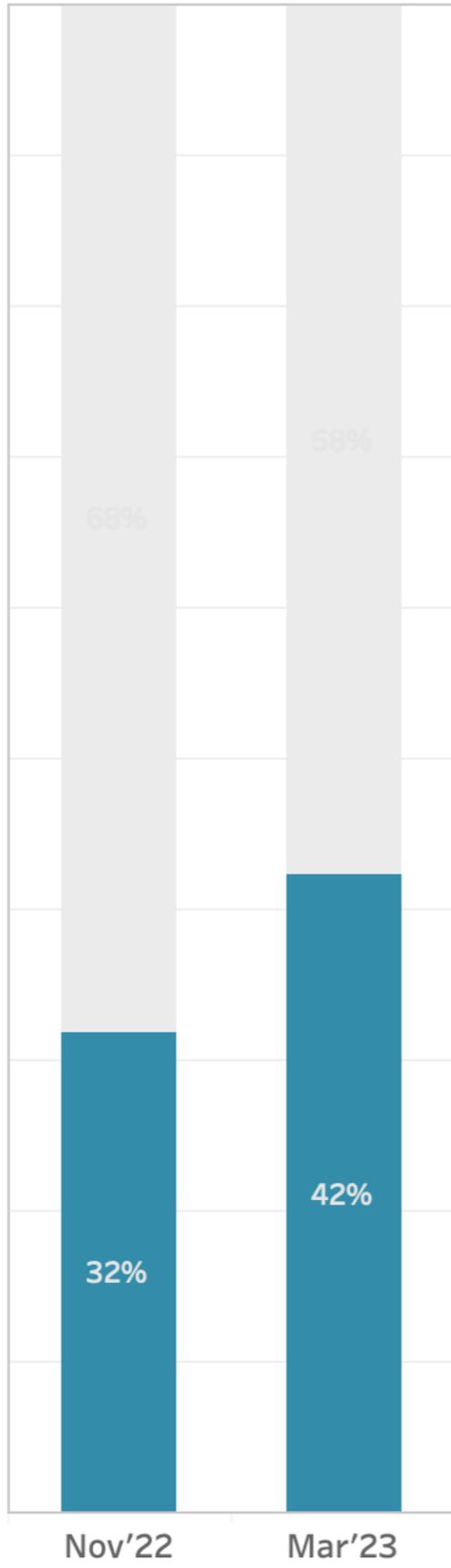
Source (14/5/23): <https://ftp.ripe.net/pub/stats/ripencc/nro-adoption/latest/>



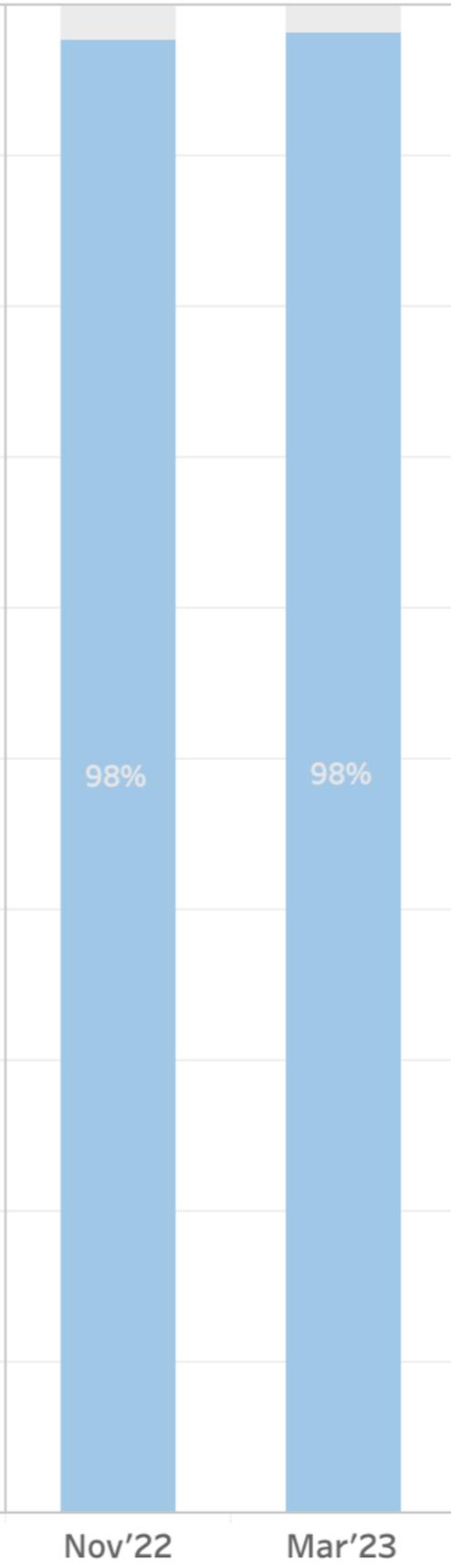
### RIPE NCC



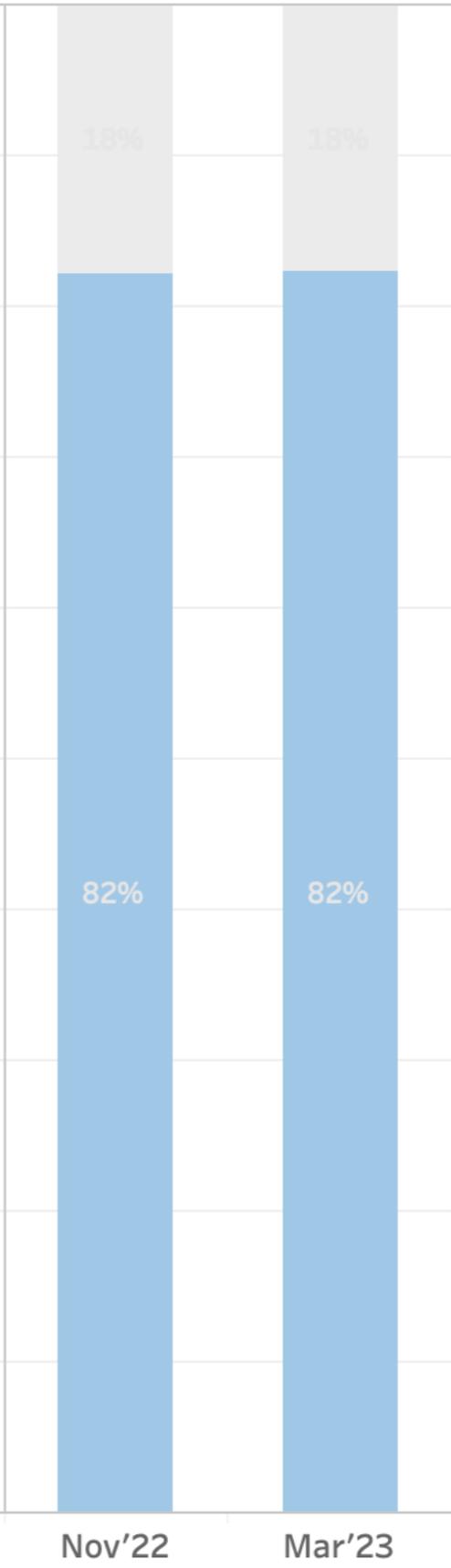
### SPAIN



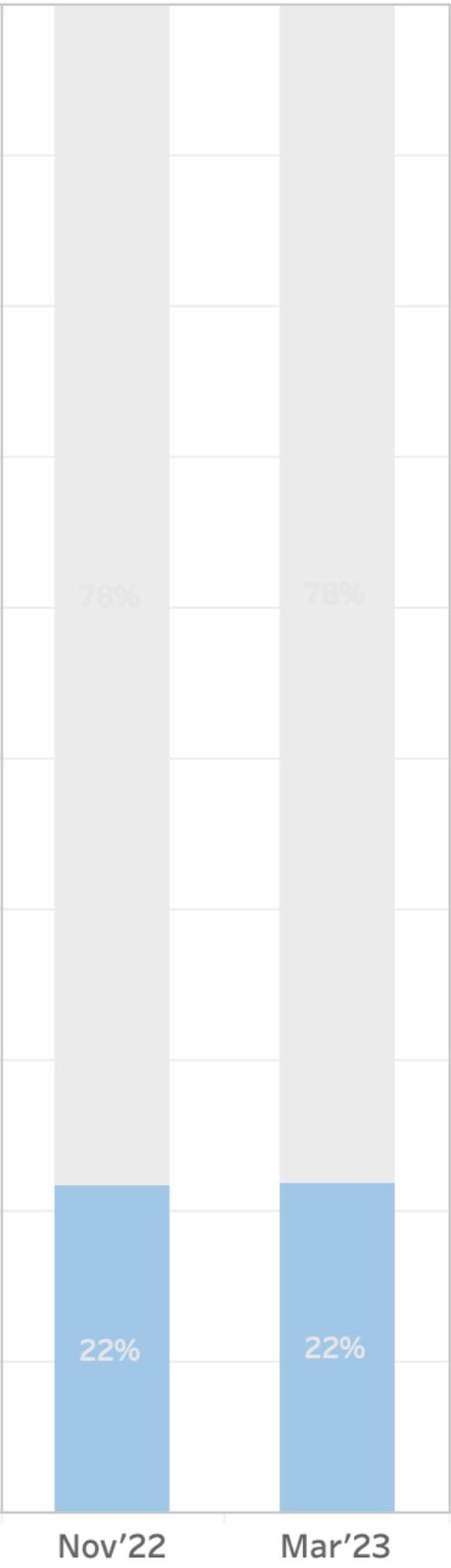
### PORTUGAL



### FRANCE



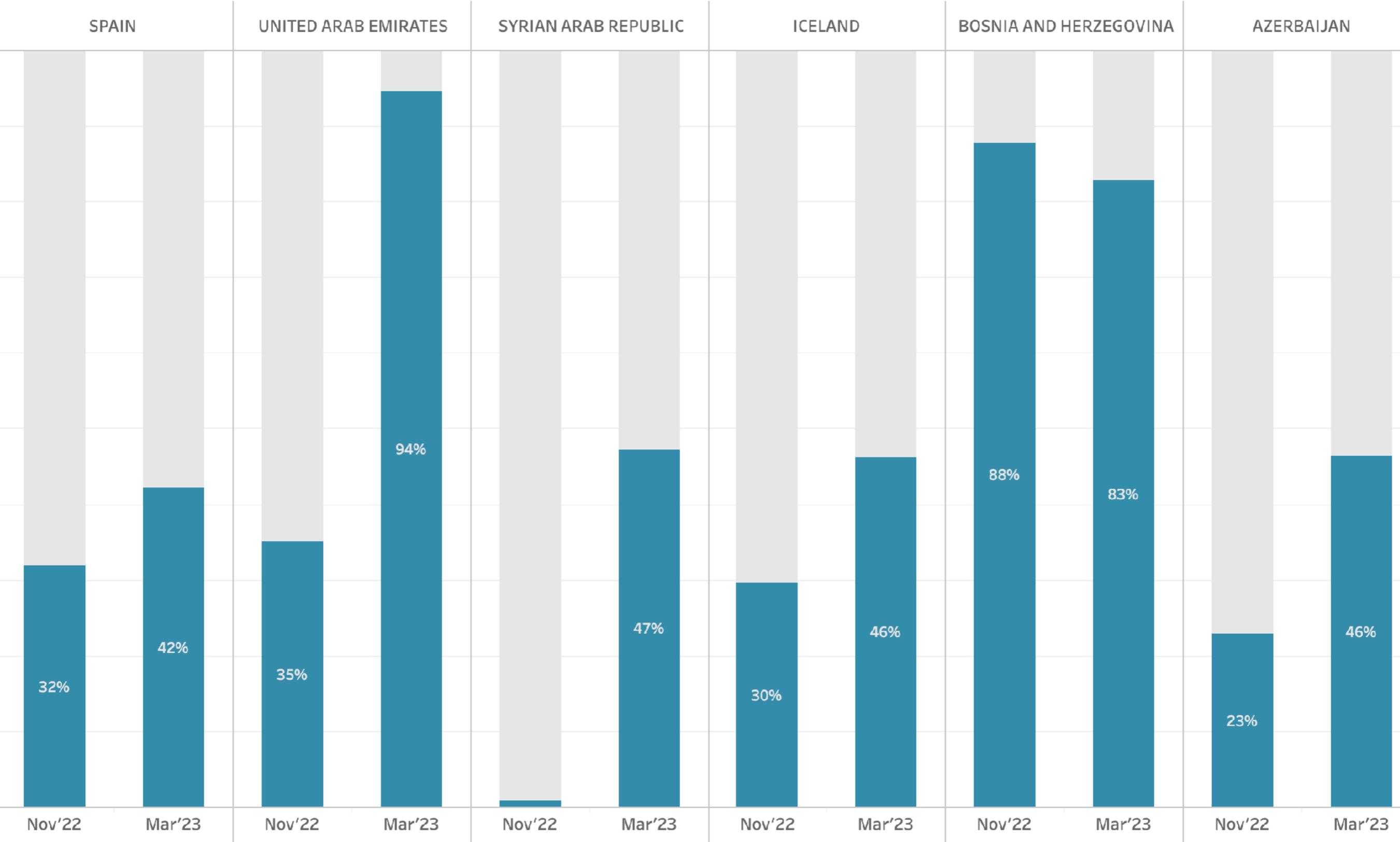
### ITALY



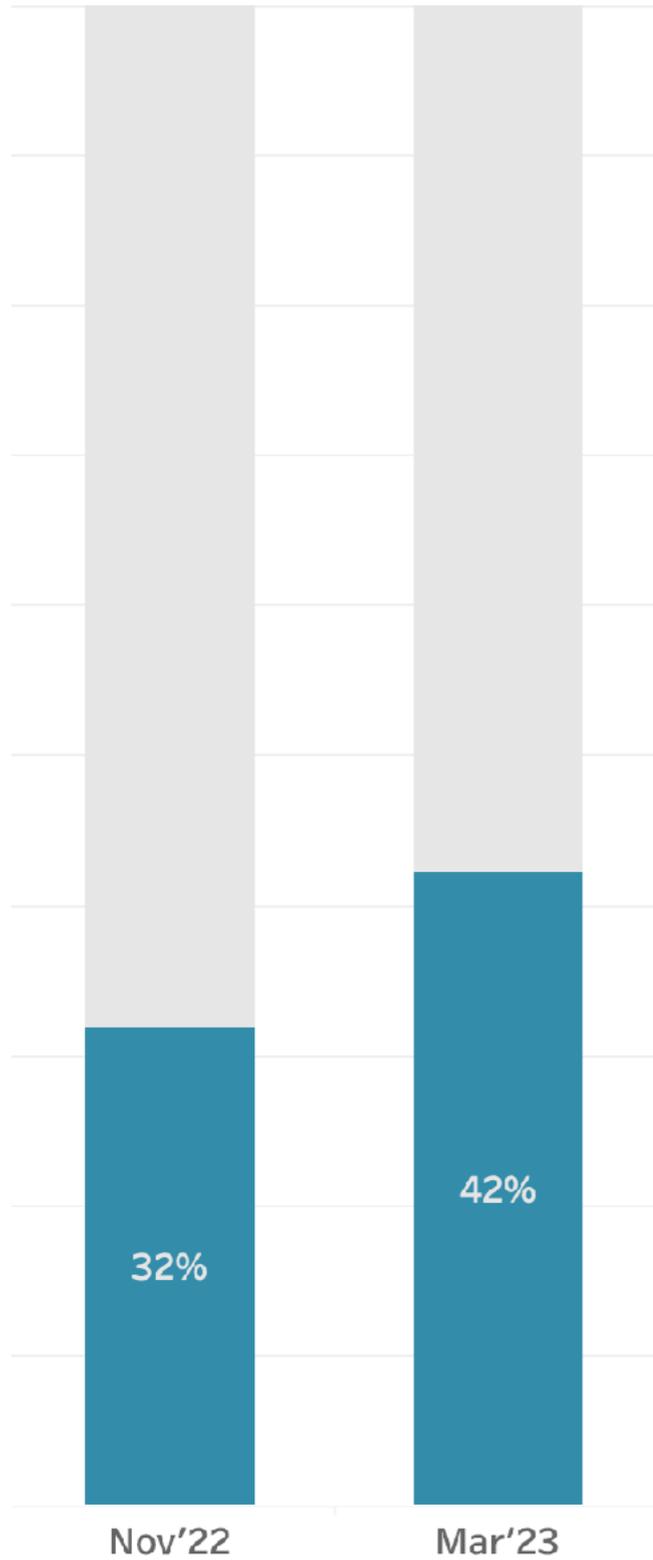


# Countries with the most change in IPv4 ROA Coverage

November 2022 vs March 2023

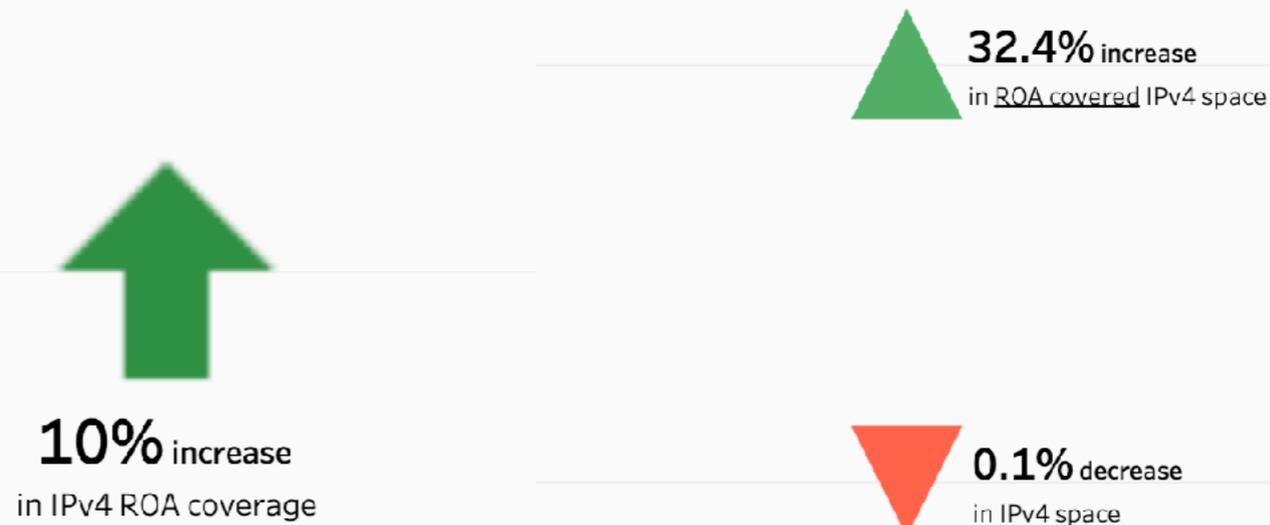


## IPv4 ROA Coverage in SPAIN November 2022 vs March 2023



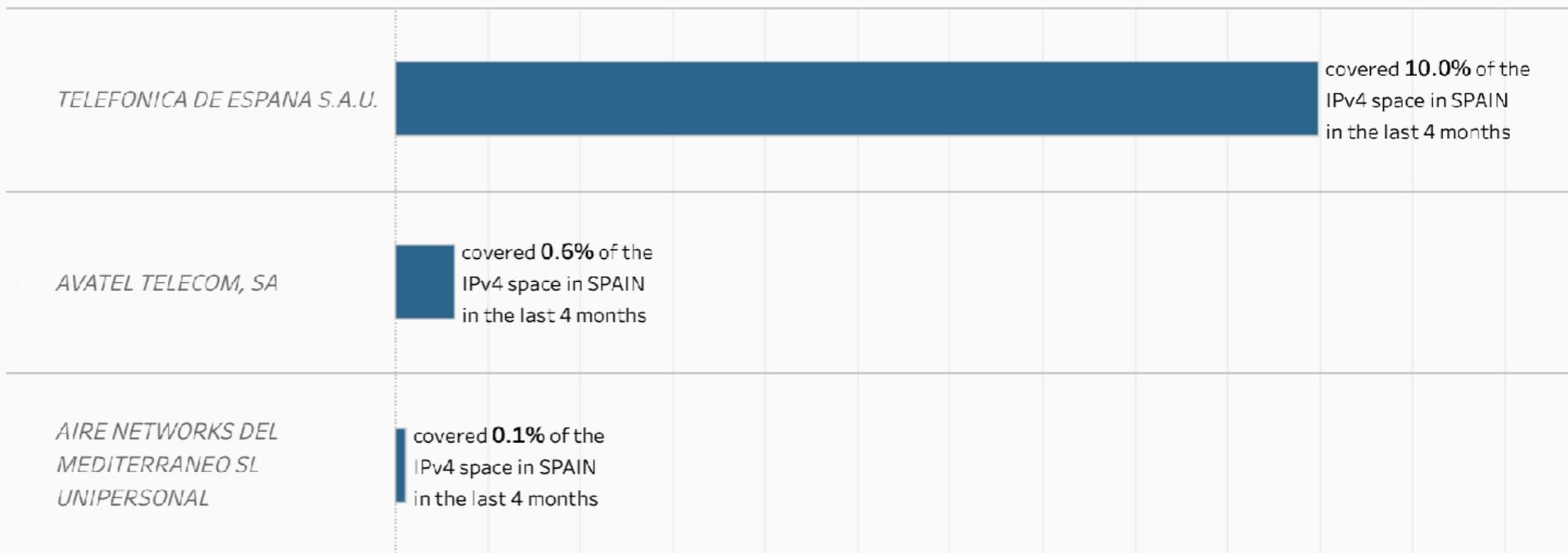
### Change

Select Country SPAIN



### Who to thank??

#### Top 3 contributors to the increase in IPv4 ROA coverage in SPAIN





■ covered  
■ uncovered

Änn Соңы An Críoch Y Diwedd  
Vége Endir ڤايان  
Son Ժասահրուտի ڤتړږ  
Lõpp Amaia תסוה Tmíem  
Sfârşit Loppu Slutt Liðugt Kraja  
Kraj Конец Fund  
Fin النهاية Konec Τέλος  
Fine Fí Край  
Einde Fim Pabaiga  
Slut Beigas





# Questions

