



**RIPE NCC**

RIPE NETWORK COORDINATION CENTRE

# **BGP Routing Security: Hijacks vs RPKI**

**Alastair Strachan  
RIPE NCC**

# 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

# What is RPKI?



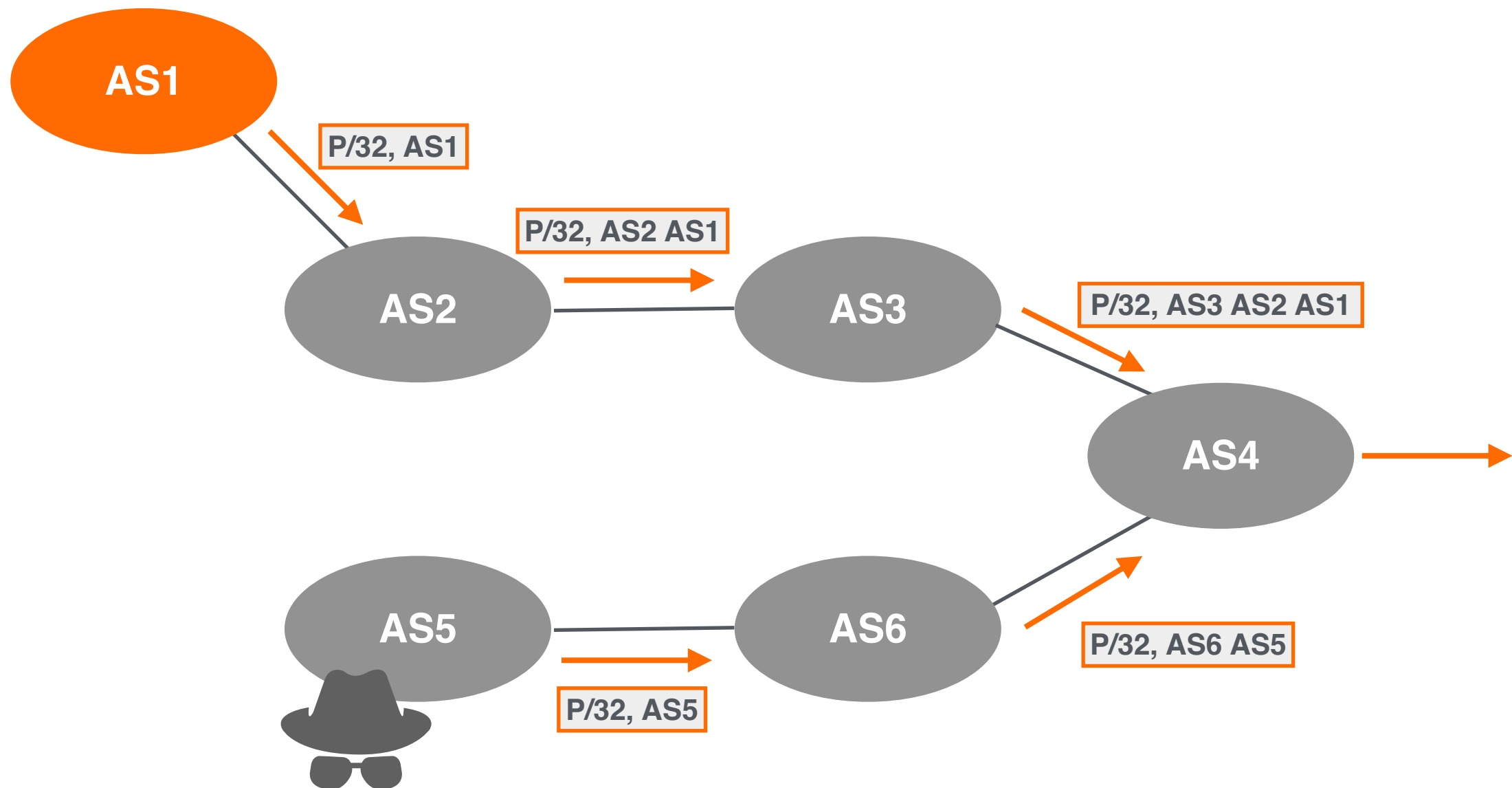
- A security framework using Public Key Infrastructure and **Resource certification** (X.509 PKI certificates) for BGP route origin validation (ROV)
- Allows resource (IPs) holders to prove ownership, and create authorisations (ROAs)
- ASNs can use ROAs to validate the origin of BGP announcements
  -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



# Origin Hijack: Same Prefix



Prefix-P, 2001:db8::/32



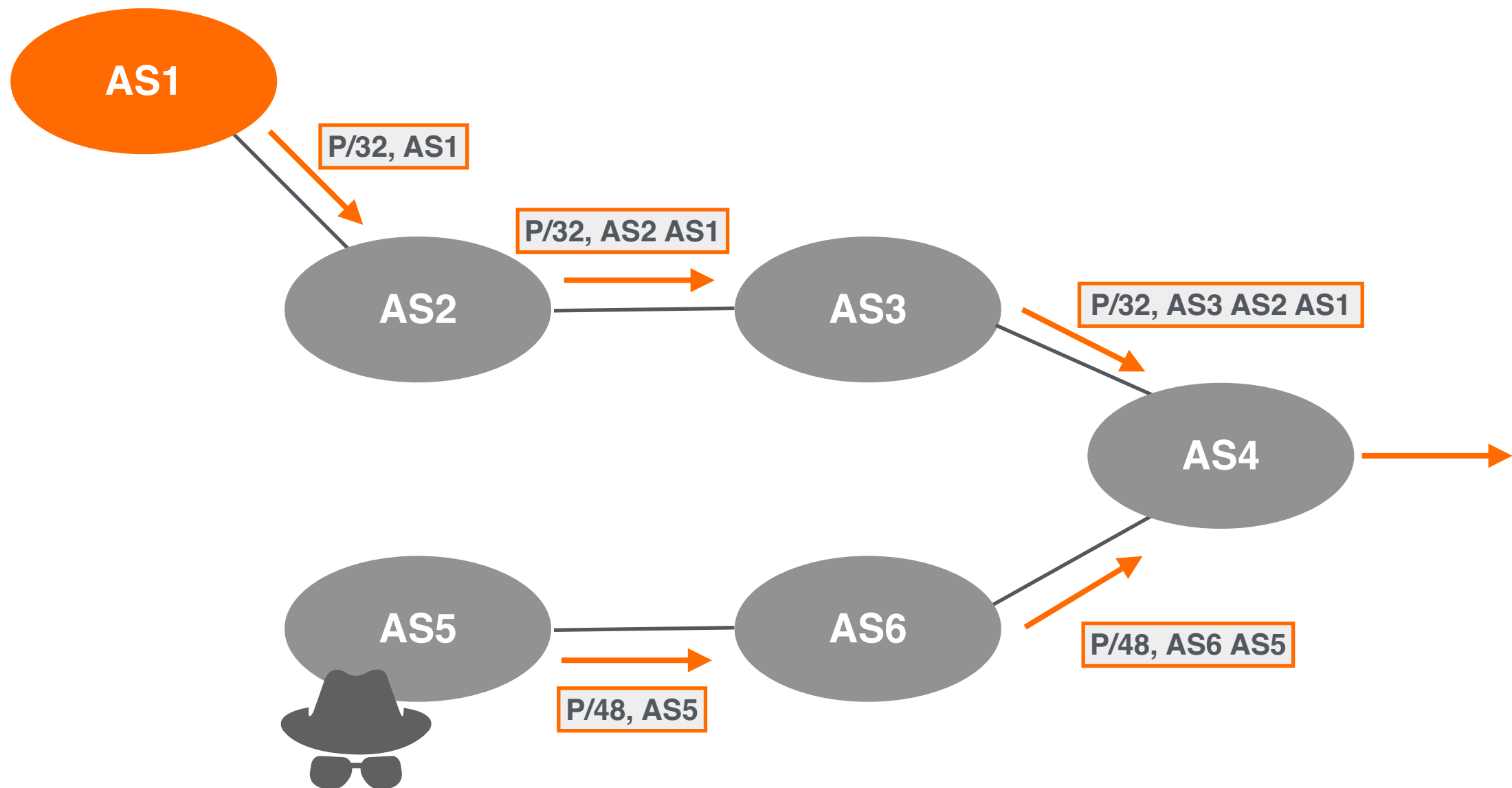
This is a **local hijack!**

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.

# How does it work?



# Elements of RPKI



- RPKI system consists of two parts...

## SIGNING

Create ROAs for your prefixes  
in the RPKI system



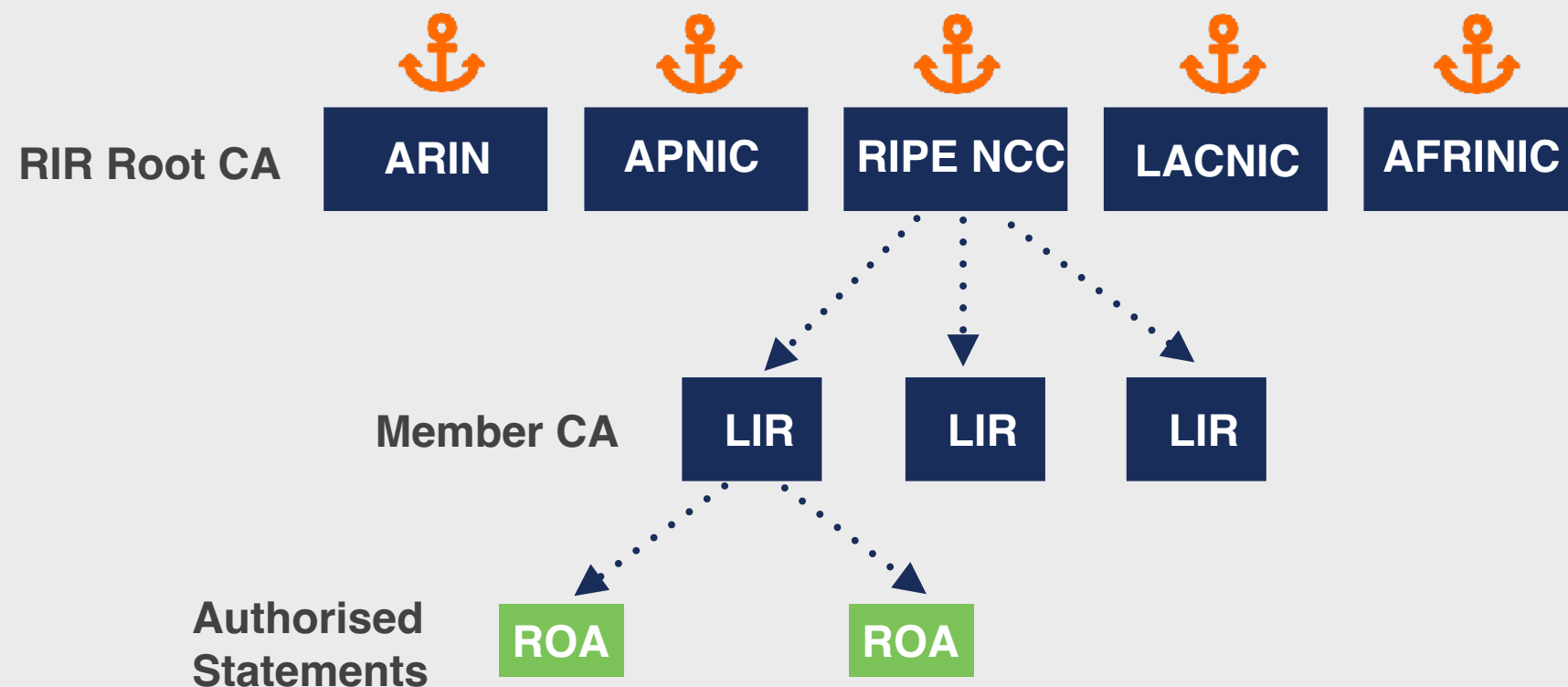
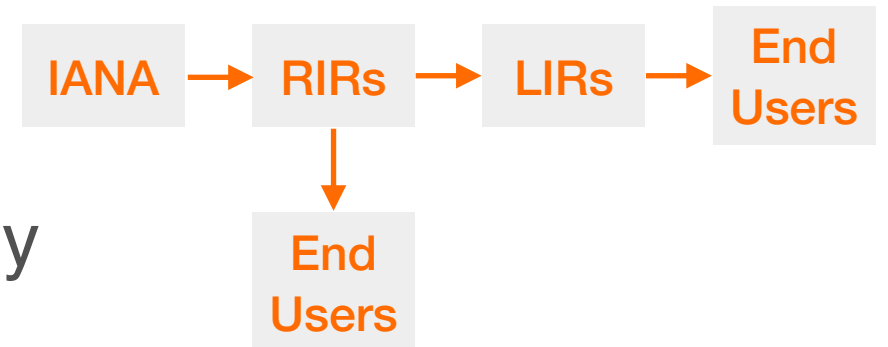
## VALIDATION

Verify the information  
provided by others

# Trust in RPKI

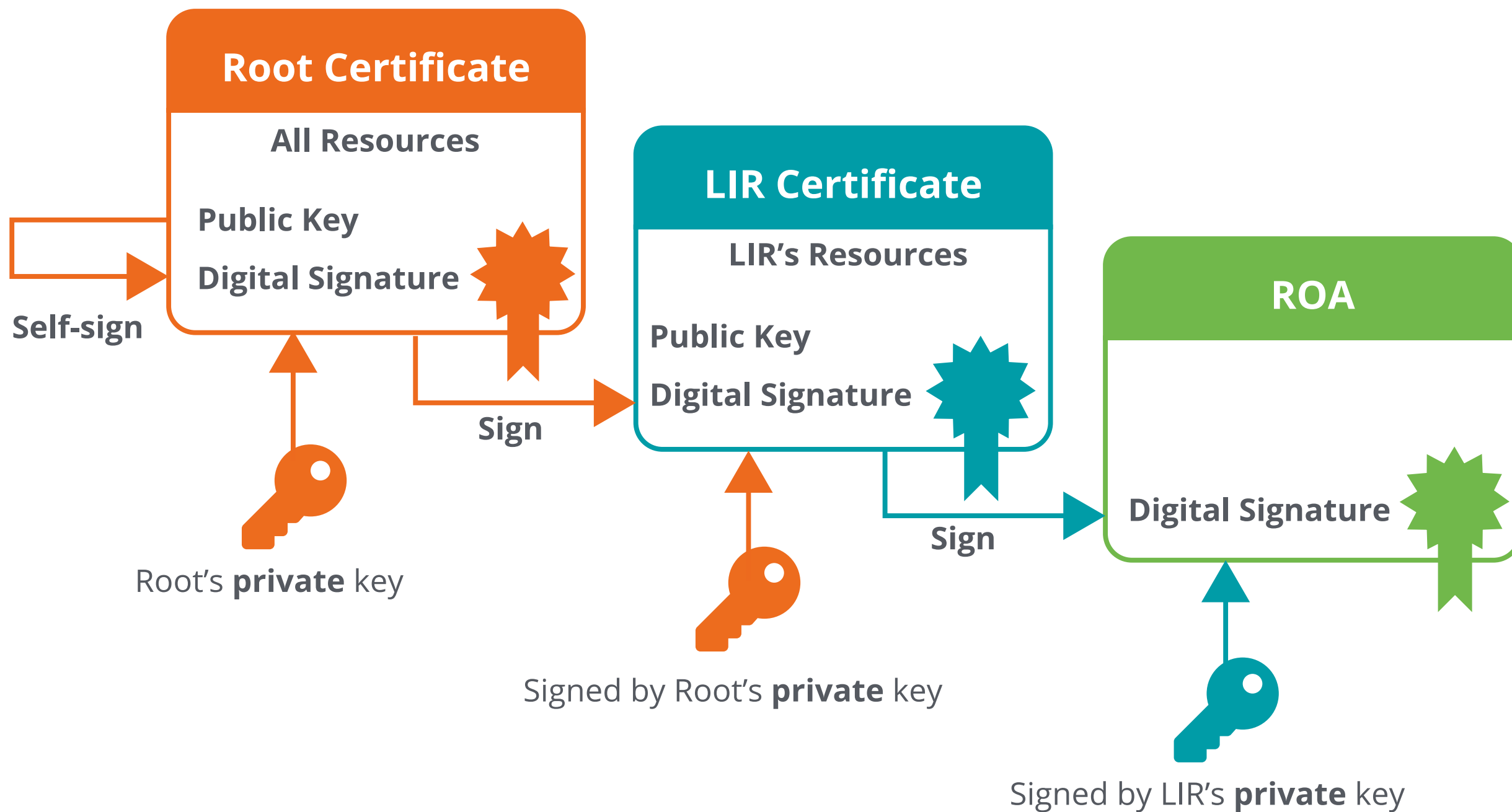


- RPKI relies on five RIRs as Trust Anchors
- Certificate structure follows the RIR hierarchy
- RIRs issue certificates to resource holders





# RPKI Chain of Trust





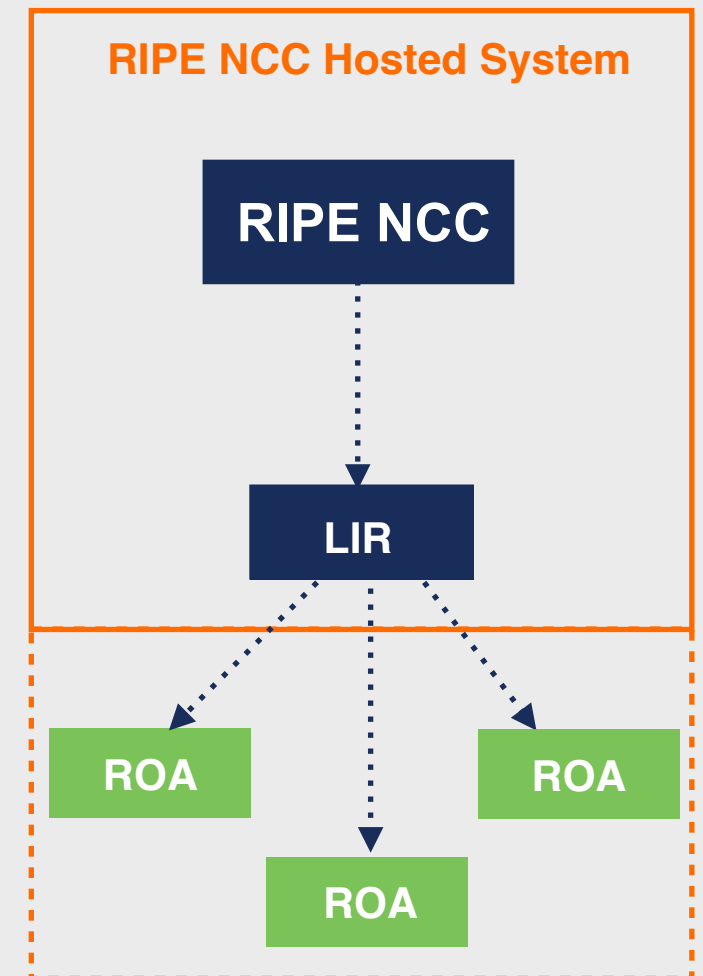
# What are ROAs?

- 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

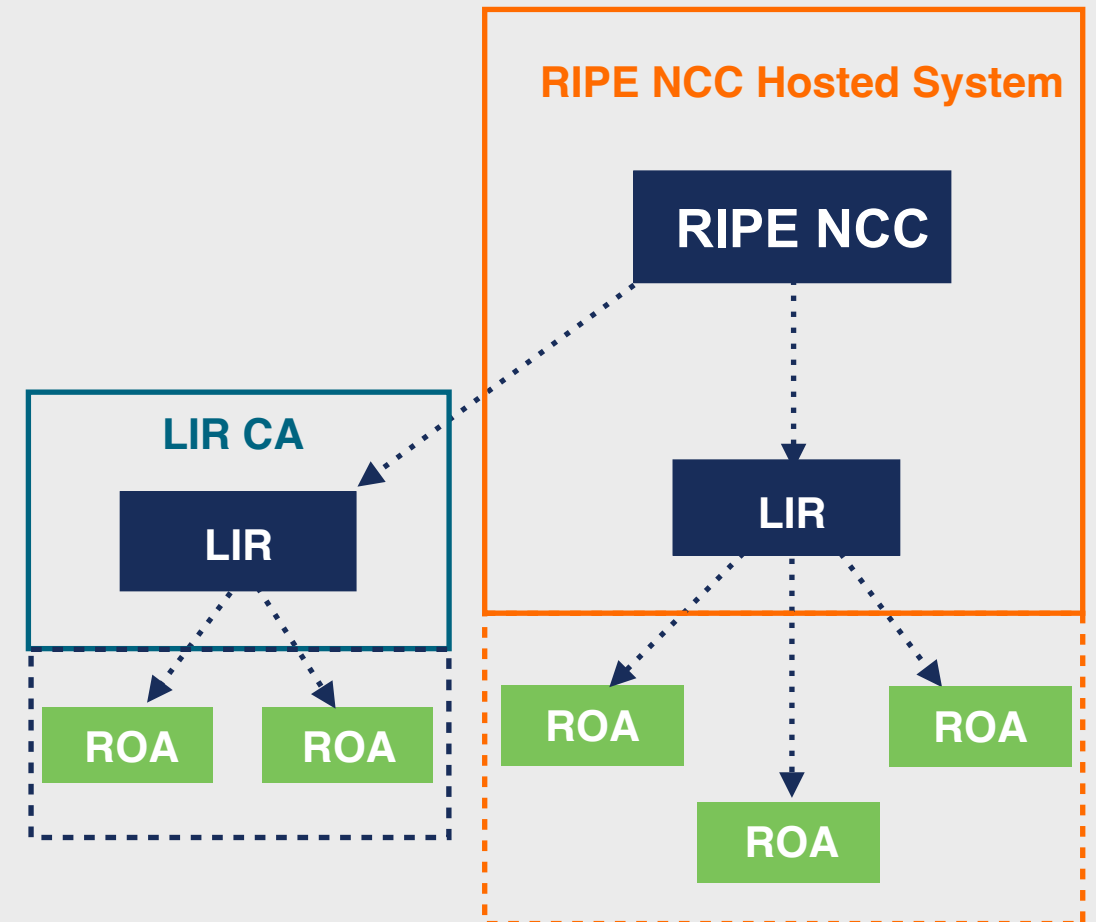
# Hosted RPKI

- 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

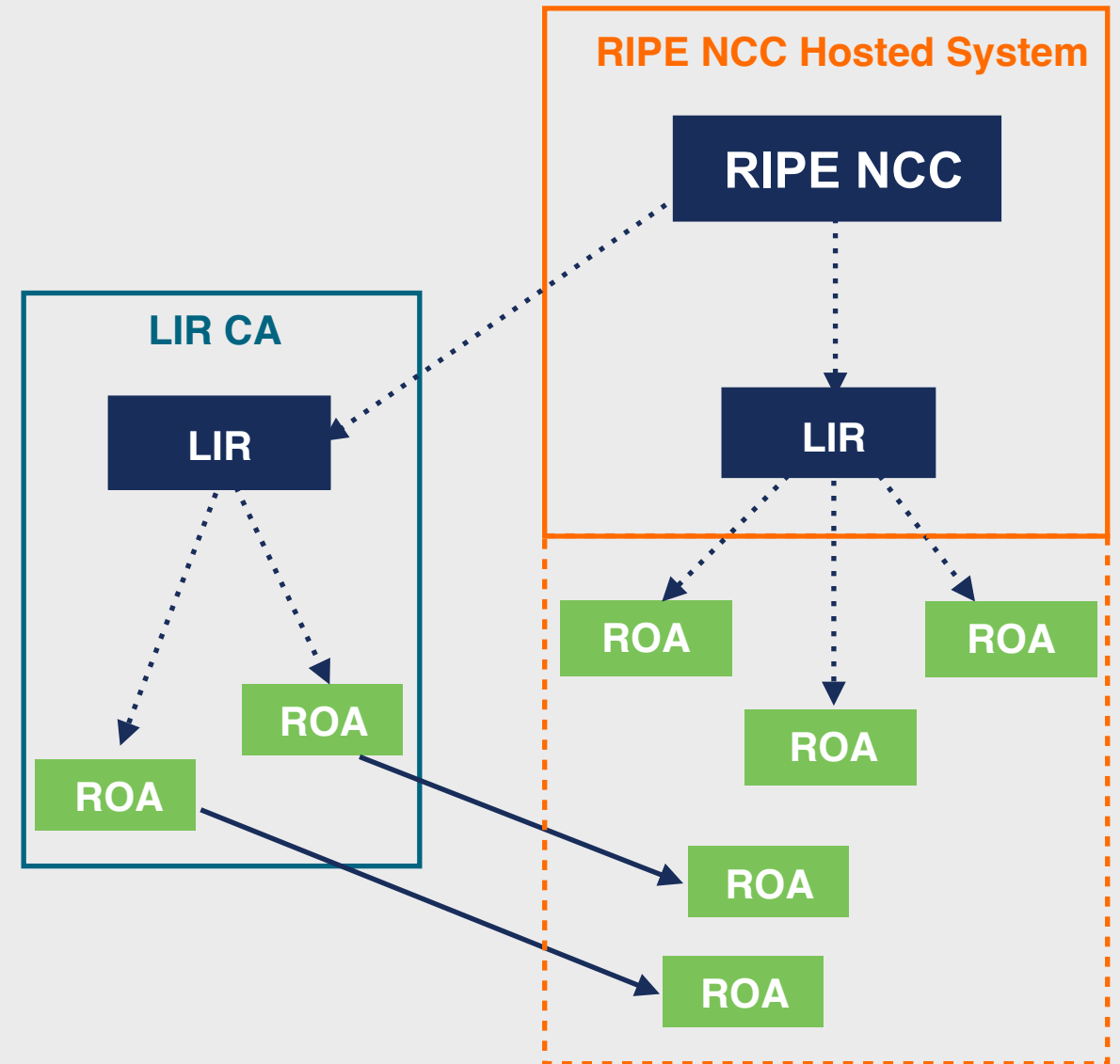
- Each LIR manages its part of the RPKI system
  - Runs its own CA as a child of the RIR
  - Manages keys/key rollovers
  - Creates, signs and publishes ROAs
- Certificate Authority (CA) Software
  - **Krill** (NLnet Labs)
  - **rpkid** (Dragon Research Labs)



# 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

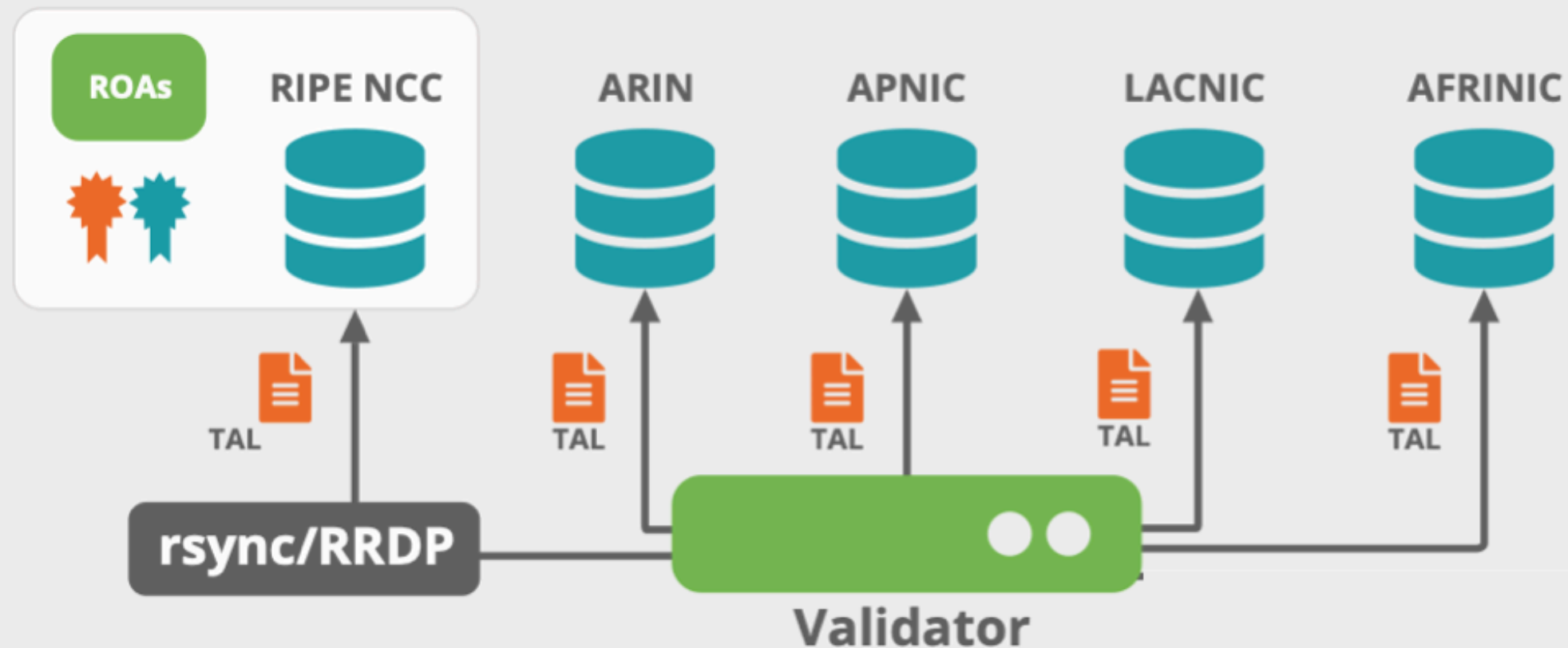


- Verifying the information provided by others
  - Proves holdership through a public key and certificate infrastructure
- In order to validate RPKI data, you need to ...
  - install a **validator software** locally in your network
- Goal is to validate the **“origin of BGP announcements”**
  - Known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





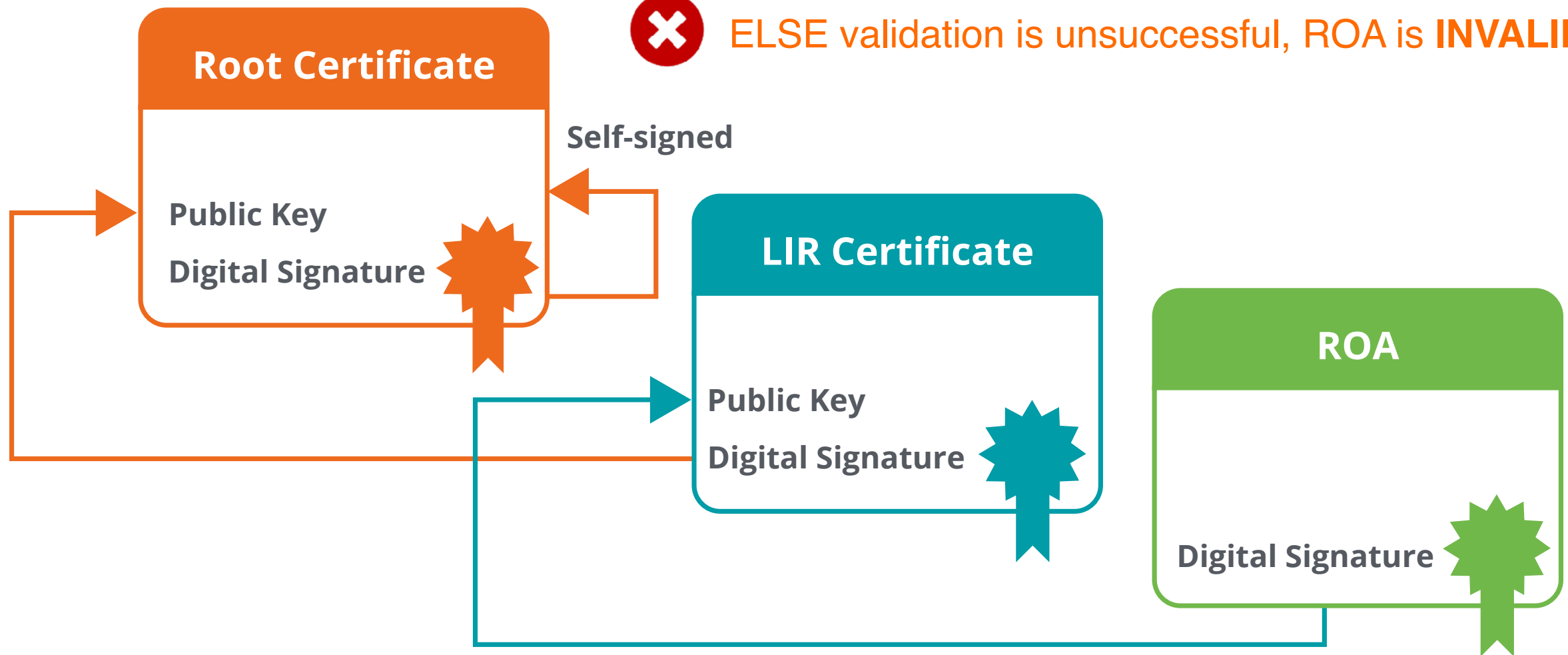
# ROA Validation Process



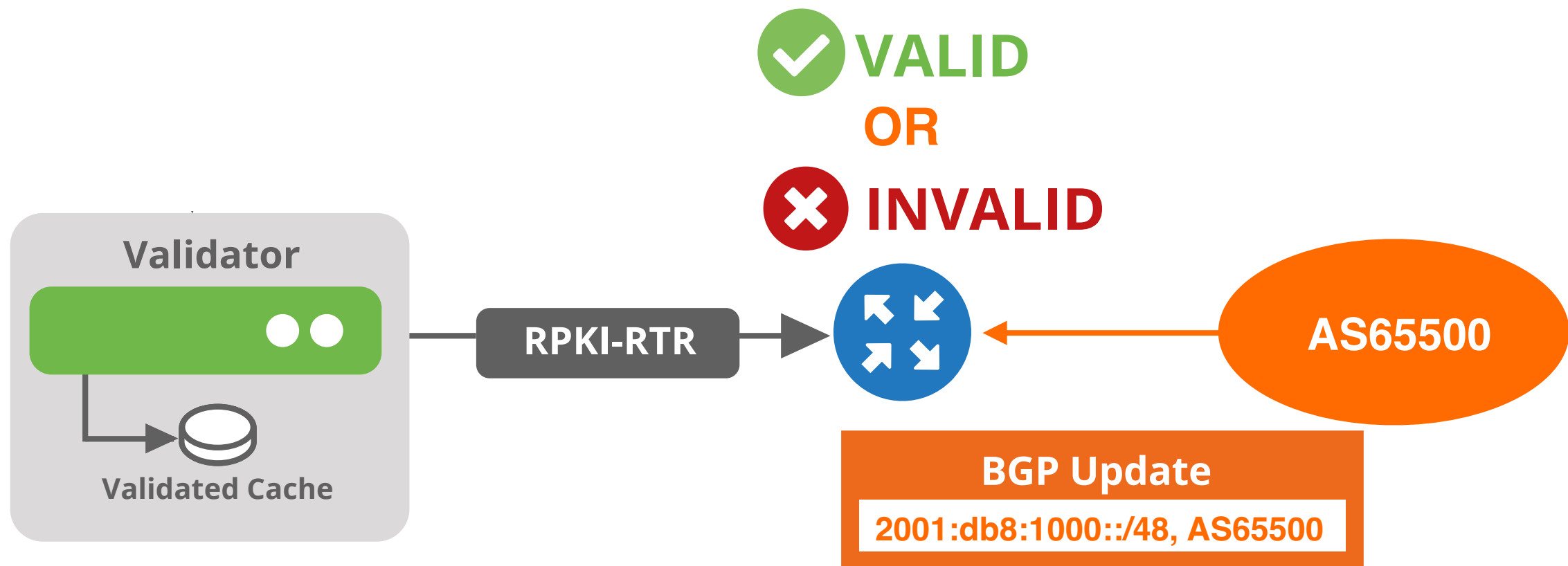
IF chain is complete, it means ROA is **VALID!**



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



# Valid ROAs Are Sent to the Router!



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>

# 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>

# 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%

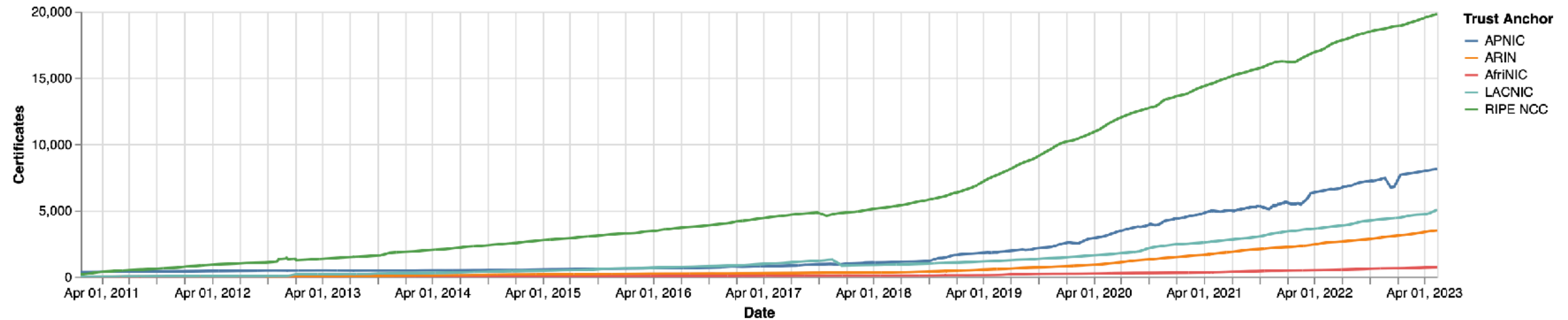
Source (13/5/23): <https://rov-measurements.nlnetlabs.net/stats/>



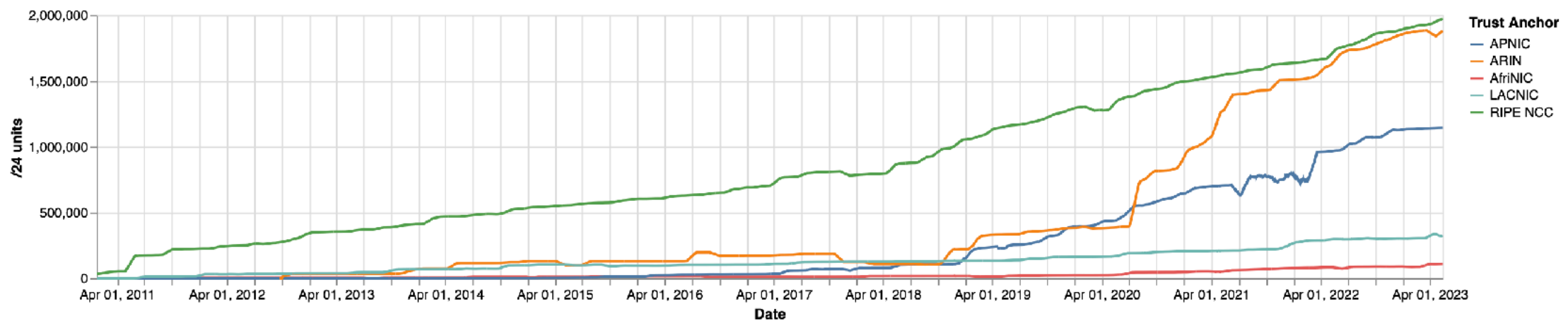
# Steady growth: Adoption and ROAs



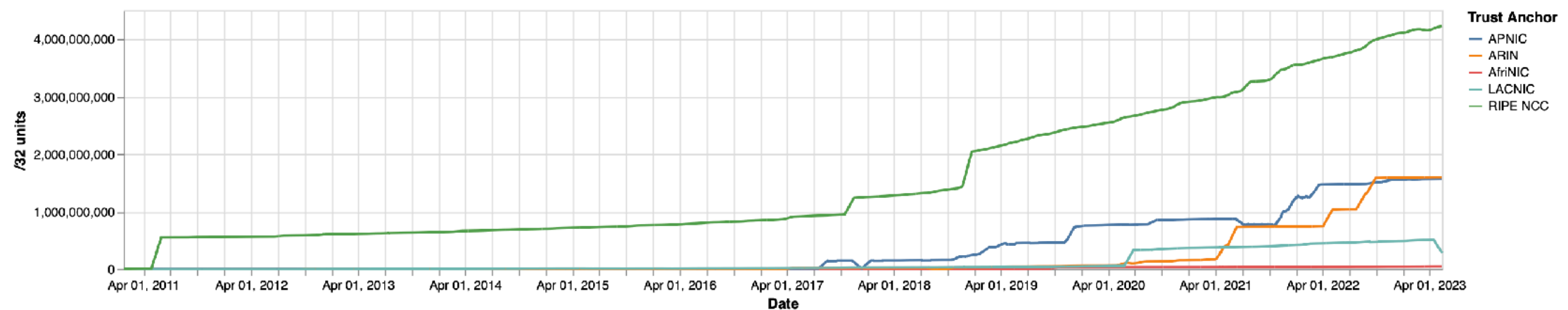
## Number of Certificates



## 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%

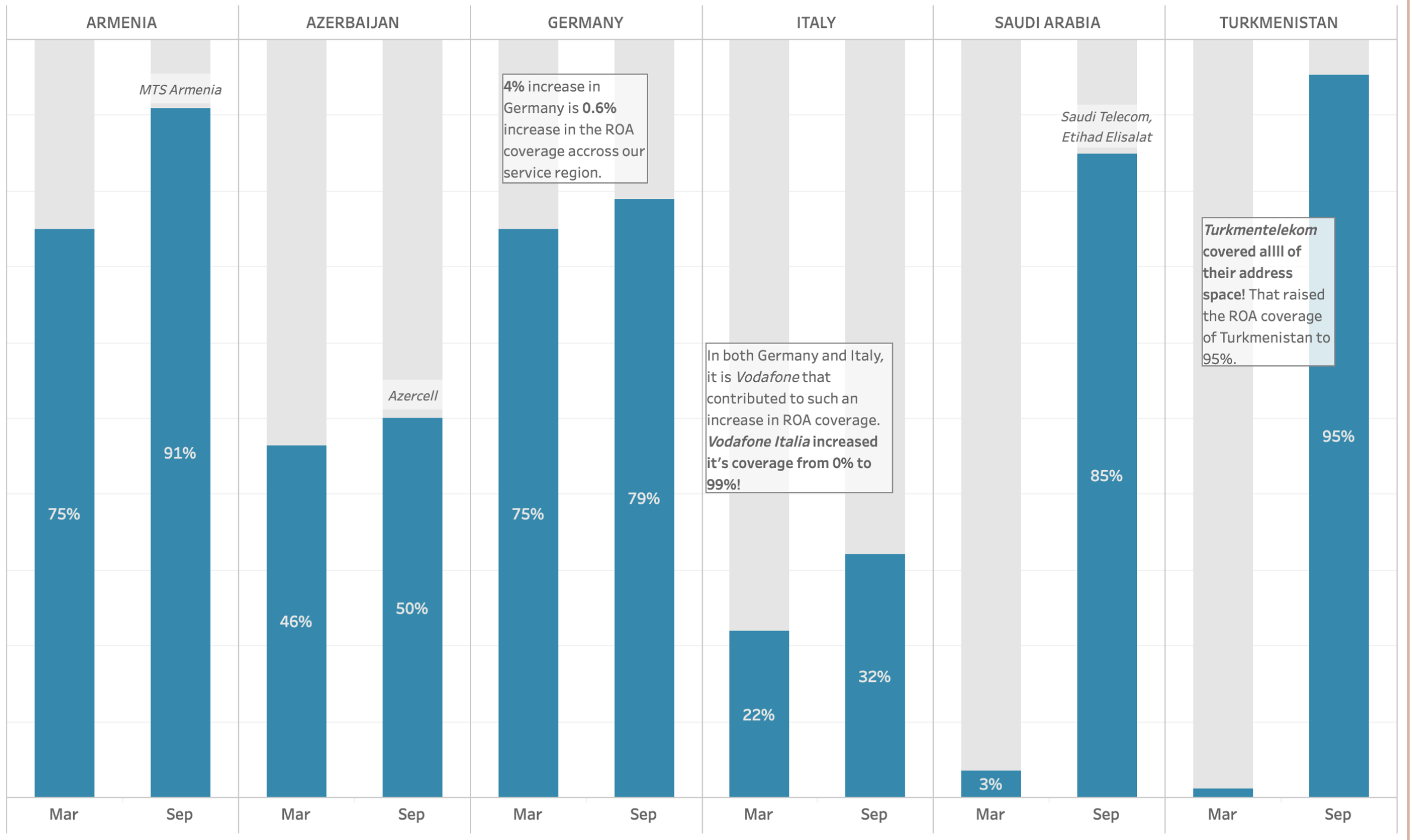
Source (14/5/23): <https://ftp.ripe.net/pub/stats/ripencc/nro-adoption/latest/>



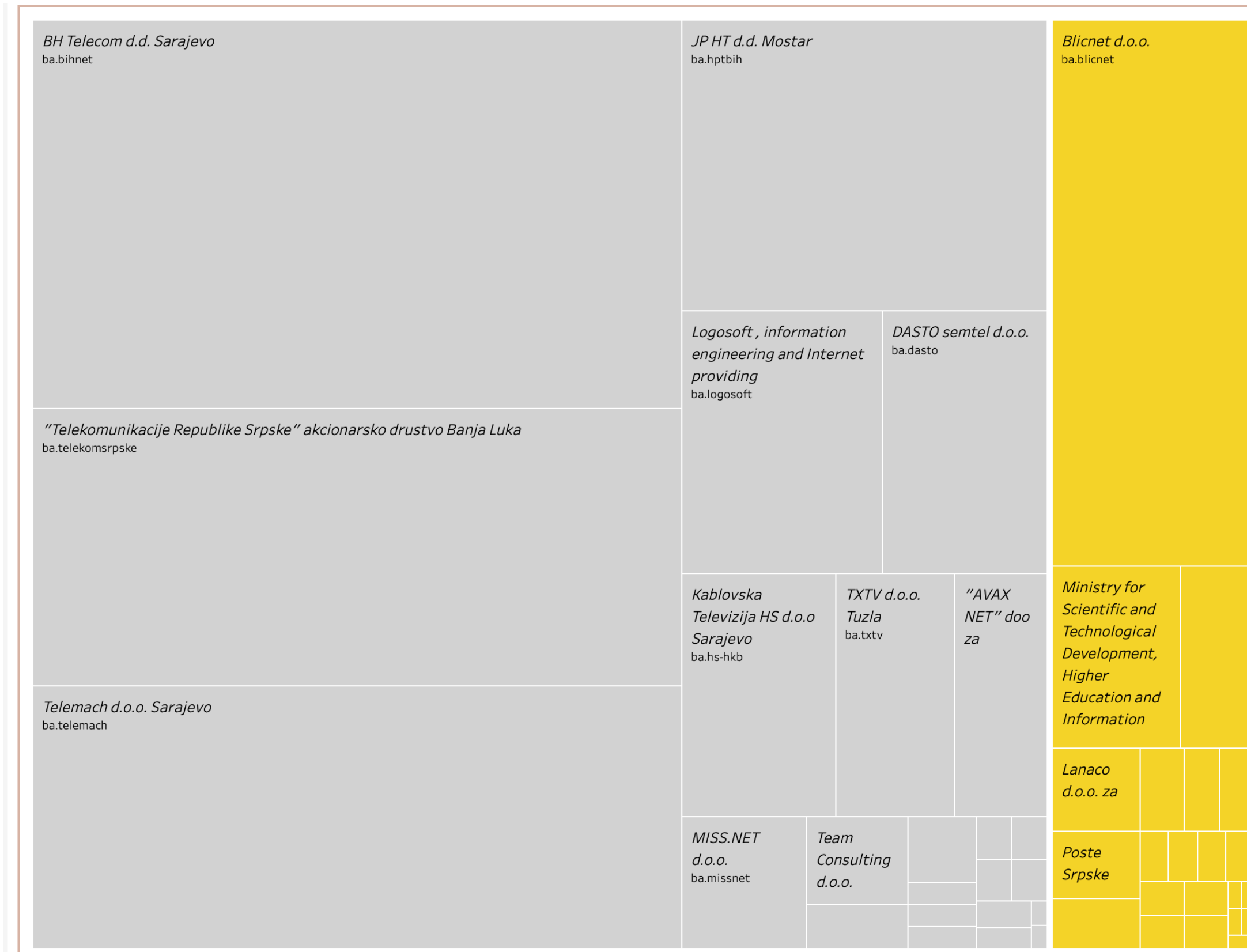


## Countries with significant change in IPv4 ROA Coverage

March 2023 vs September 2023



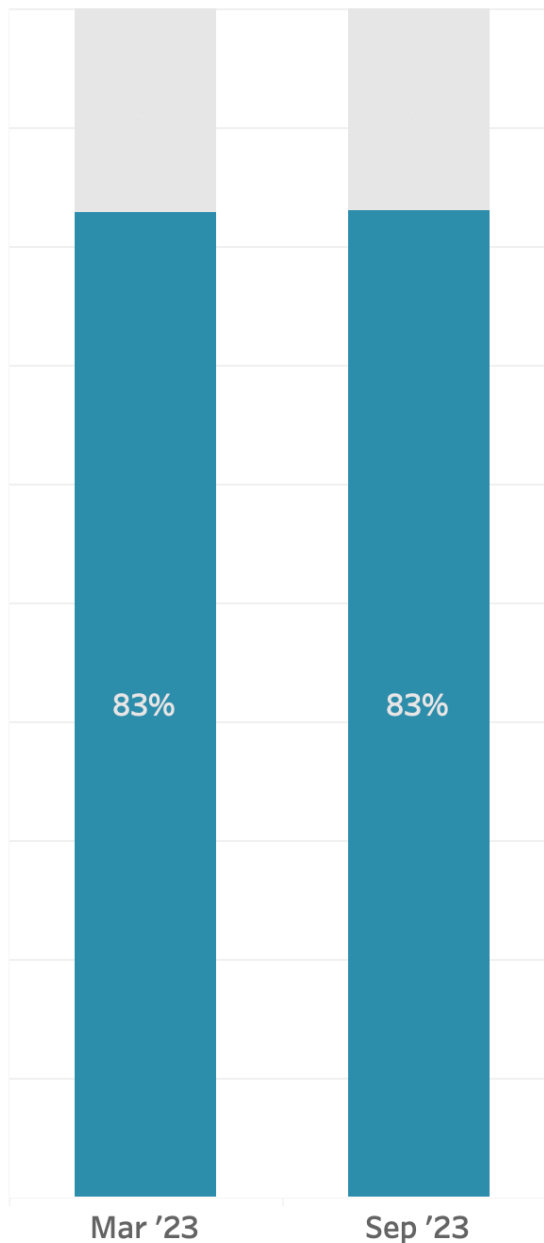
# IPv4 Covered vs Uncovered: Bosnia and Herzegovina



# Changes in IPv4 ROA Coverage



## IPv4 ROA Coverage in BOSNIA AND HERZEGOVINA March vs September 2023



### Change

Country Name  
BOSNIA AND HERZEG...

**0% increase**  
in IPv4 ROA coverage

**0.8% increase**  
in ROA covered IPv4 space

**0.5% increase**  
in IPv4 space

### Who to thank??

#### Top 3 contributors to the increase in IPv4 ROA coverage in BOSNIA AND HERZEGOVINA

<i>"AVAX NET" doo za telekomunikacije, racunarski inzenjering, konsalting i promet Lukavac</i>	covered <b>0.5%</b> of the IPv4 space in BOSNIA AND HERZEGOVINA in the last 6 months
<i>Terc Trade Company d.o.o.</i>	covered <b>0.1%</b> of the IPv4 space in BOSNIA AND HERZEGOVINA in the last 6 months
<i>Net-Flet d.o.o.</i>	covered <b>0.0%</b> of the IPv4 space in BOSNIA AND HERZEGOVINA in the last 6 months



# Questions

