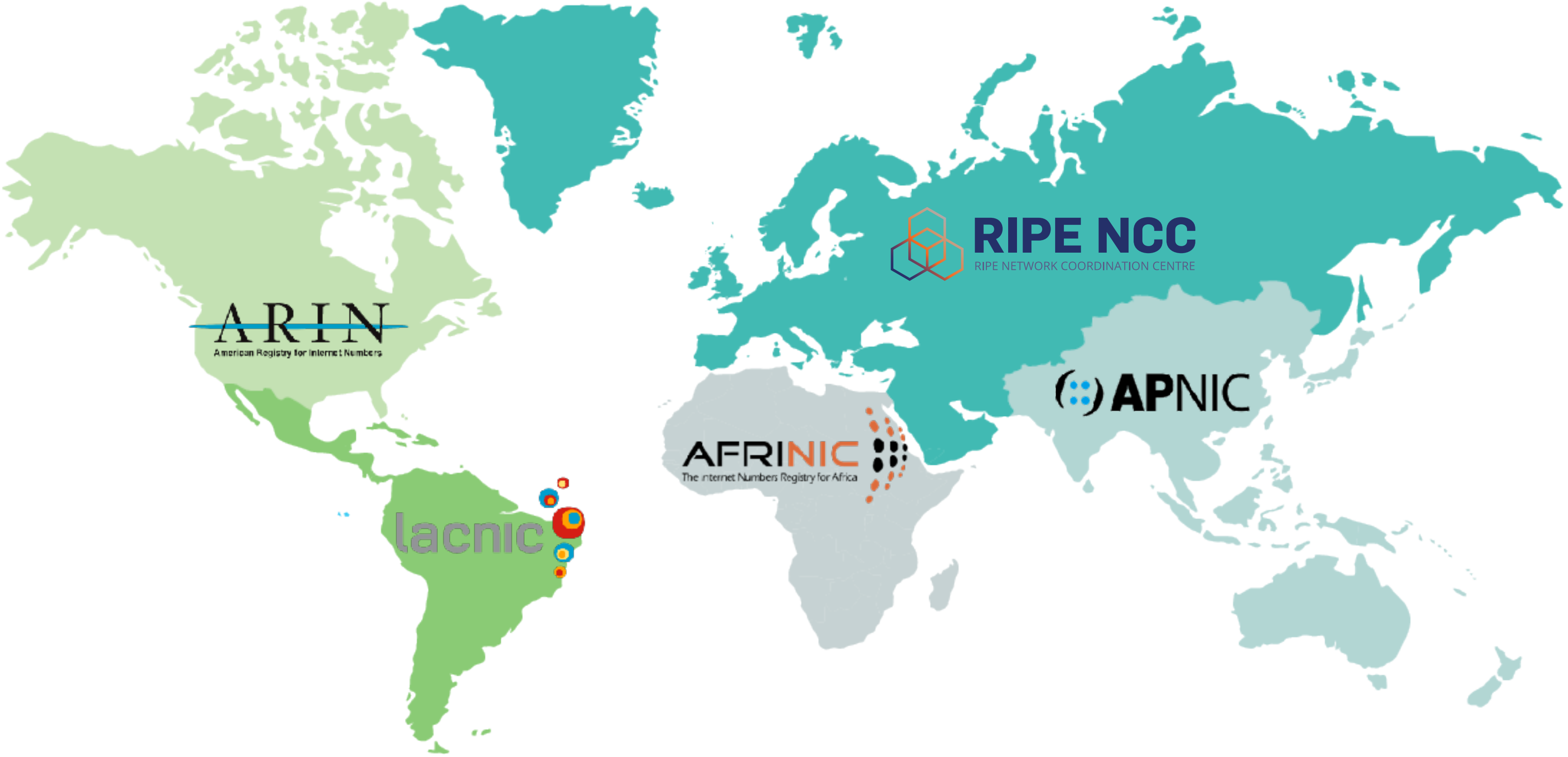
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

BGP Routing Security: Hijacks vs RPKI

Alastair Strachan
RIPE NCC

What is the RIPE NCC?

iana
Internet Assigned Numbers Authority



RIPE NCC
RIPE NETWORK COORDINATION CENTRE
ARIN
American Registry for Internet Numbers
APNIC
AFRINIC
The Internet Numbers Registry for Africa
lacnic

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?

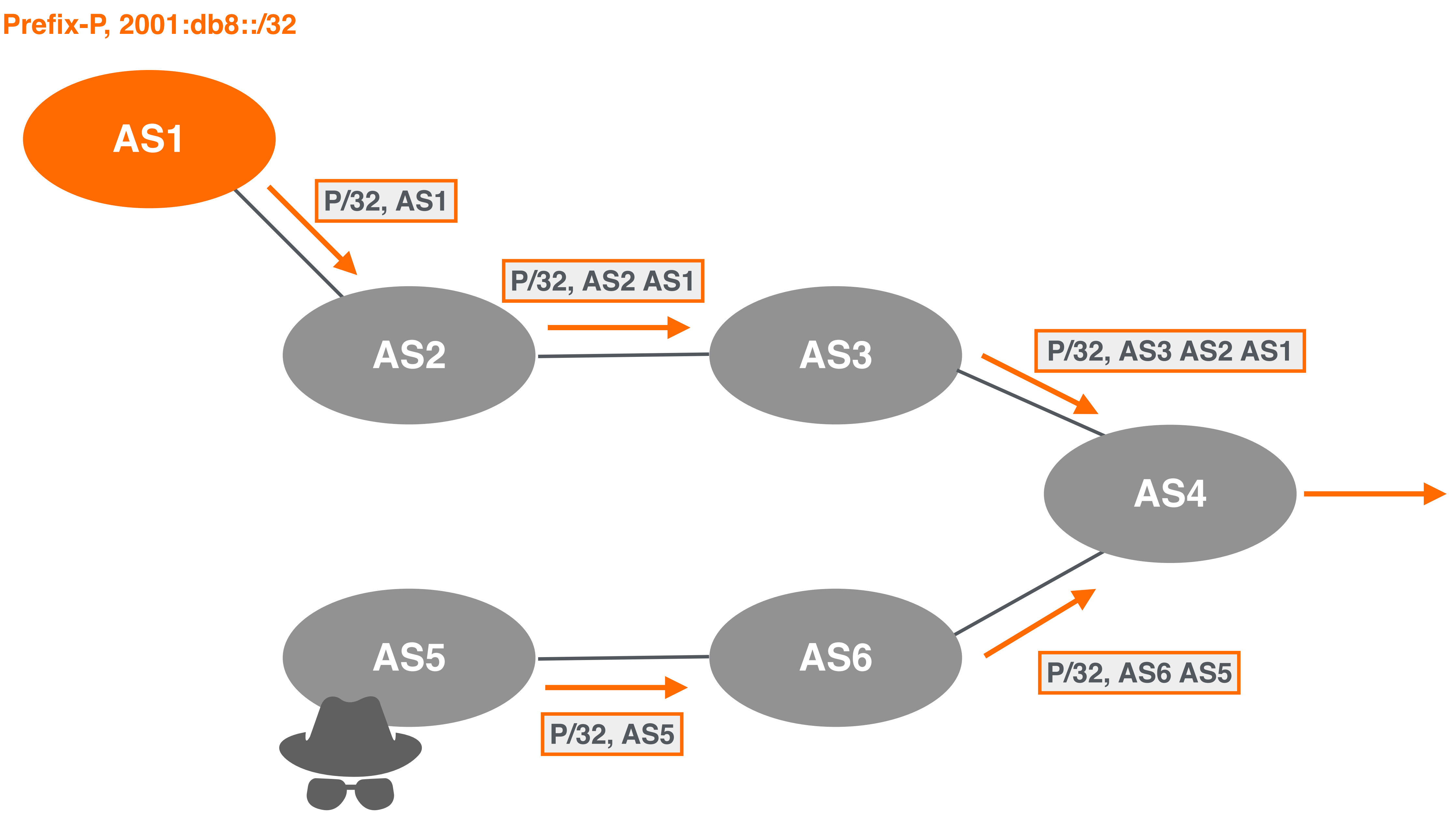
- A security framework using Public Key Infrastructure and **Resource certification** (X.509 PKI certificates) for BGP route origin validation (ROV)

- 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?

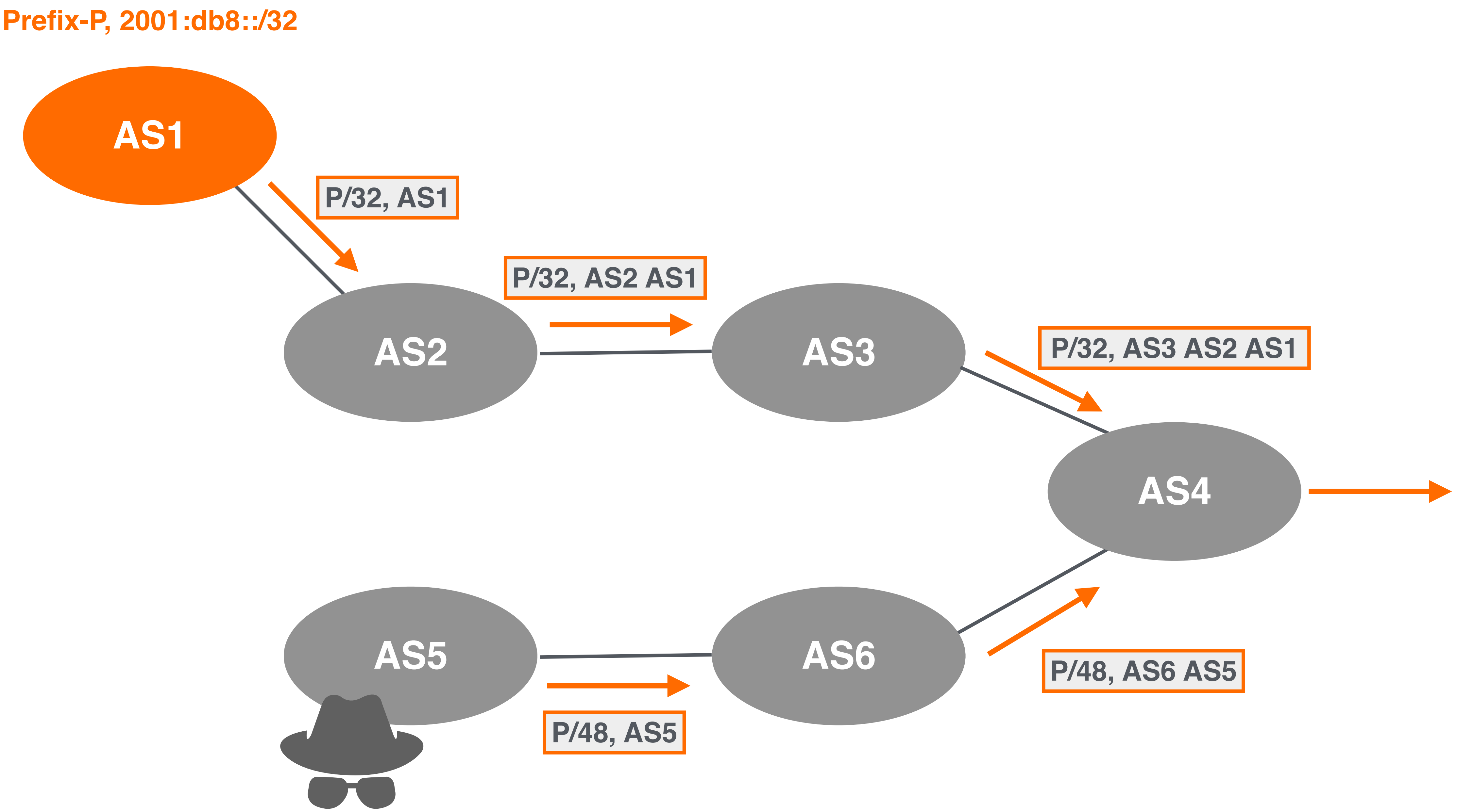
Resource
Public
Key
Infrastructure

Origin Hijack: Same Prefix



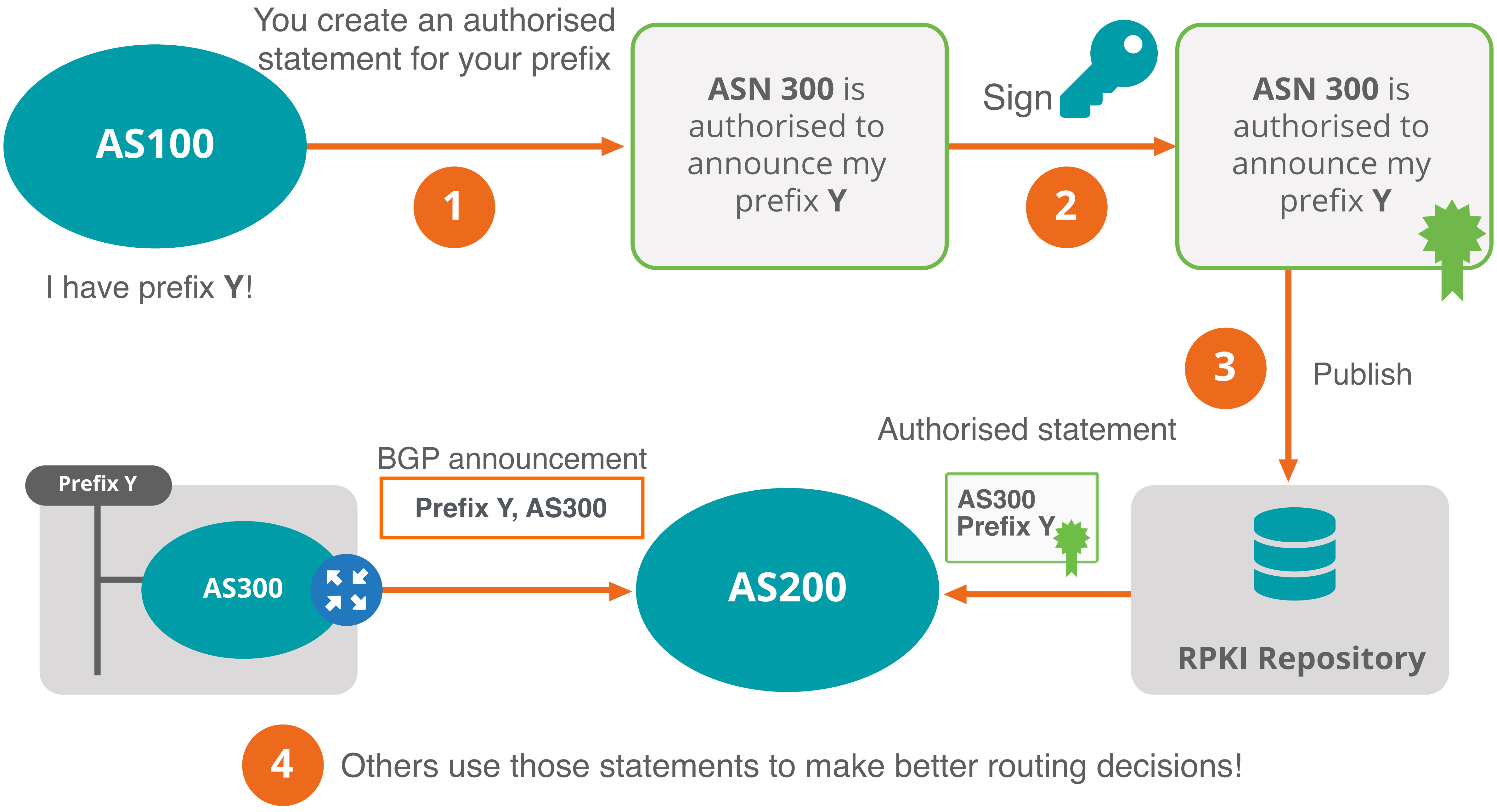
This is a **local hijack!**
Only some networks are affected based on BGP path selection process.

Origin Hijack: More Specific Prefix



This is a **global hijack!**
All traffic for more specific will be forwarded to the attacker’s network network.

How does it work?


You create an authorised statement for your prefix
AS100
I have prefix Y!
1
ASN 300 is authorised to announce my prefix Y
Sign
2
ASN 300 is authorised to announce my prefix Y
3
Publish
Authorised statement
BGP announcement
Prefix Y
AS300
Prefix Y, AS300
AS200
AS300
Prefix Y
RPKI Repository
4

Others use those statements to make better routing decisions!

Elements of RPKI

- RPKI system consists of two parts…

SIGNING

Create ROAs for your prefixes in the RPKI system

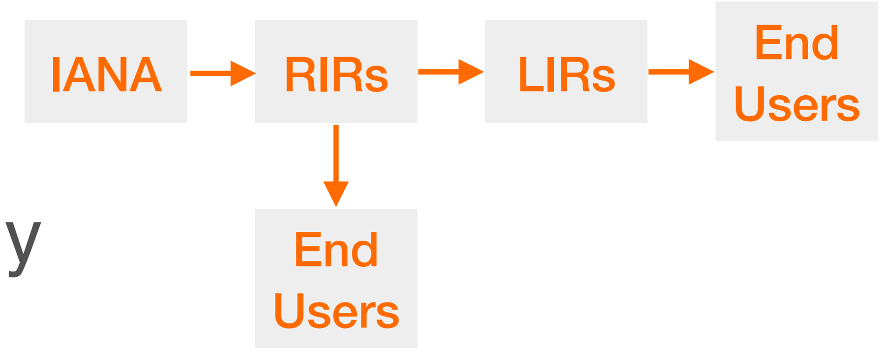
+

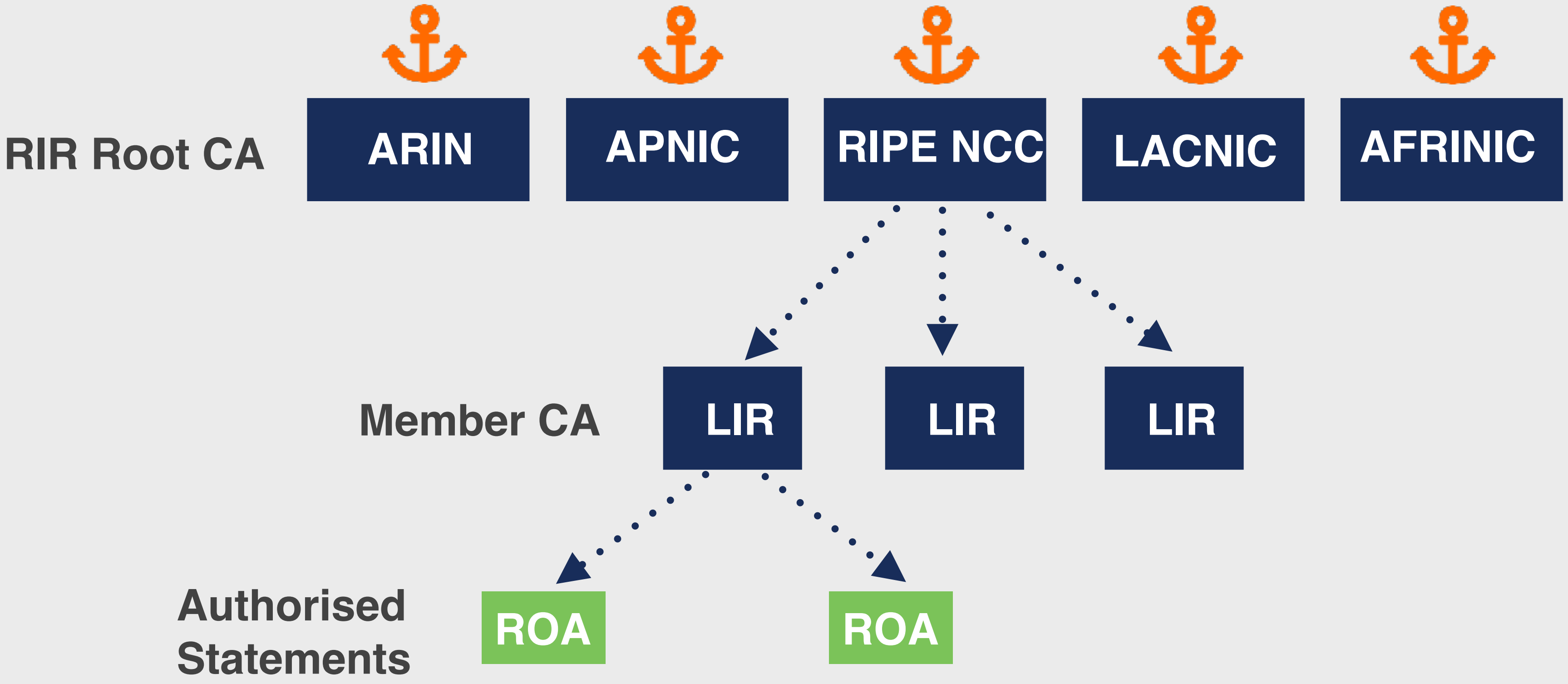
VALIDATION

Verify the information provided by others

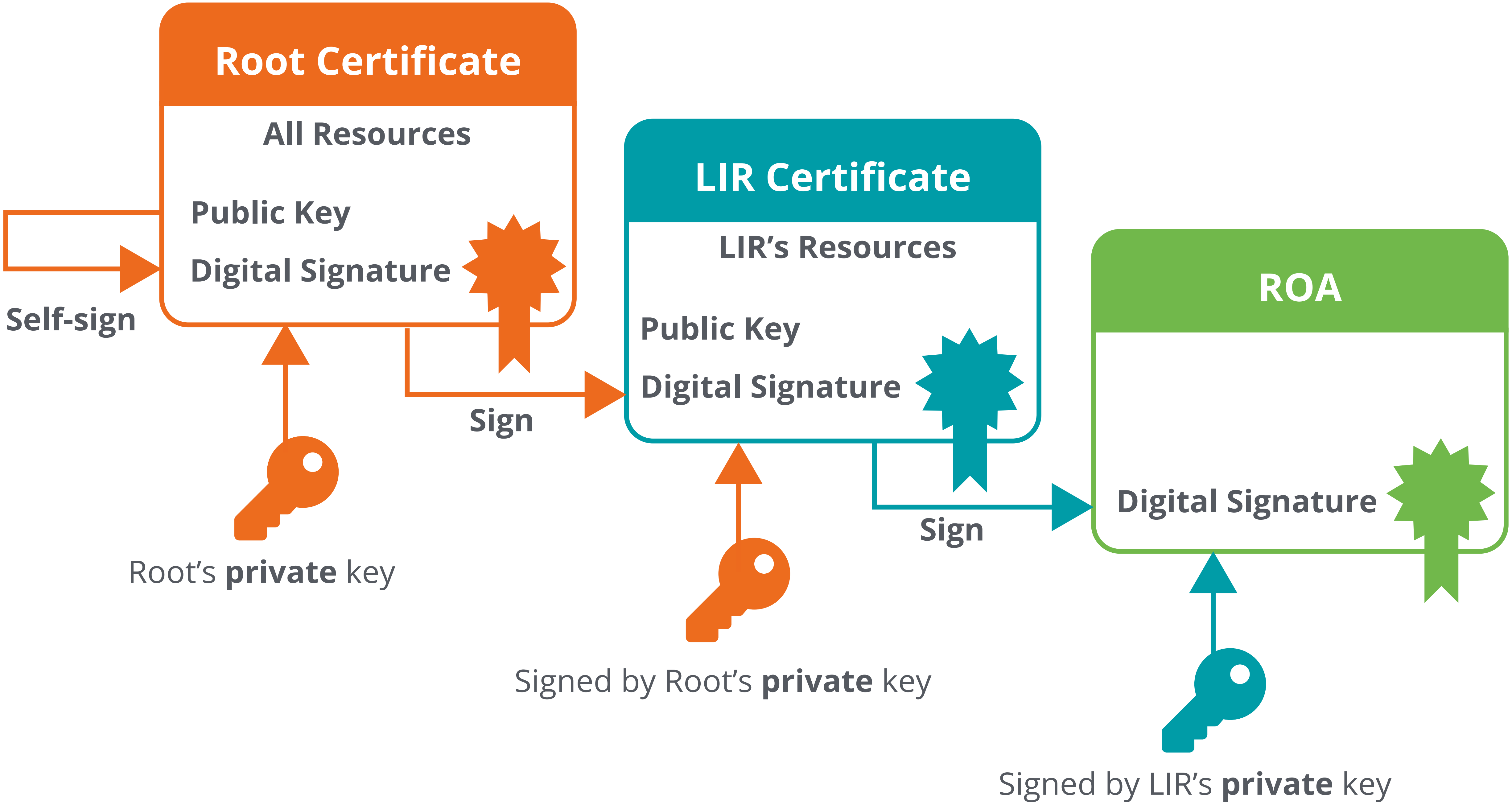
Trust in RPKI

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



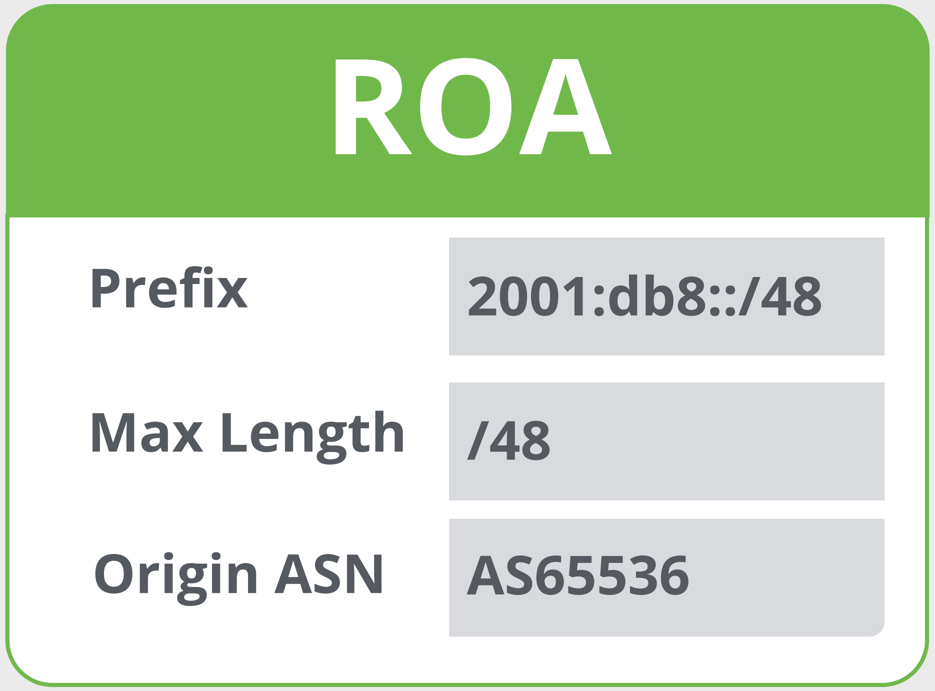


RPKI Chain of Trust



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

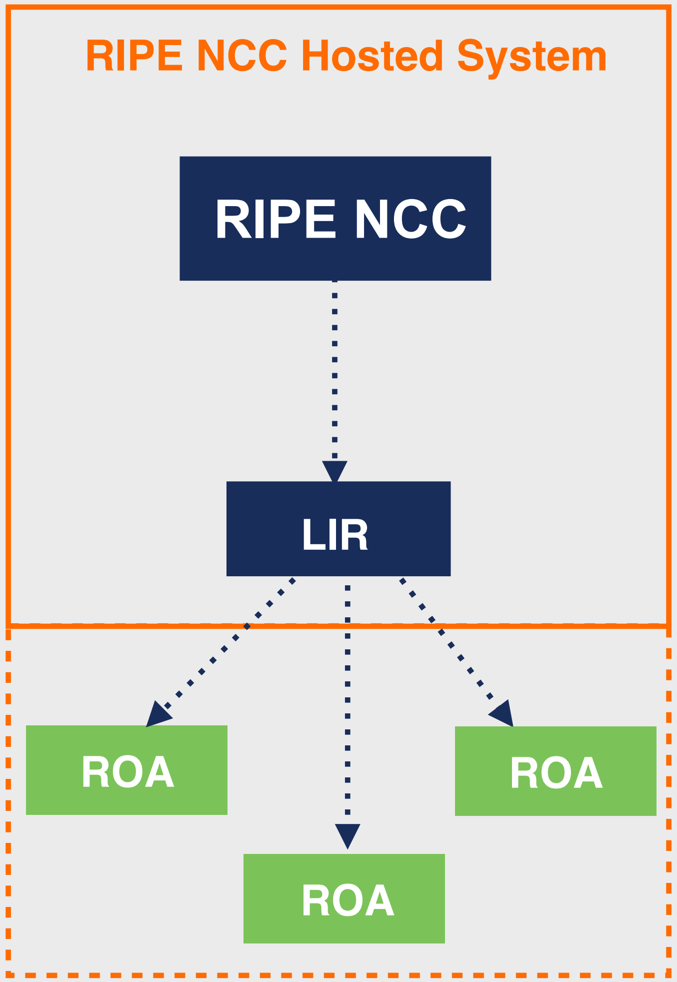


ROA

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

Hosted RPKI

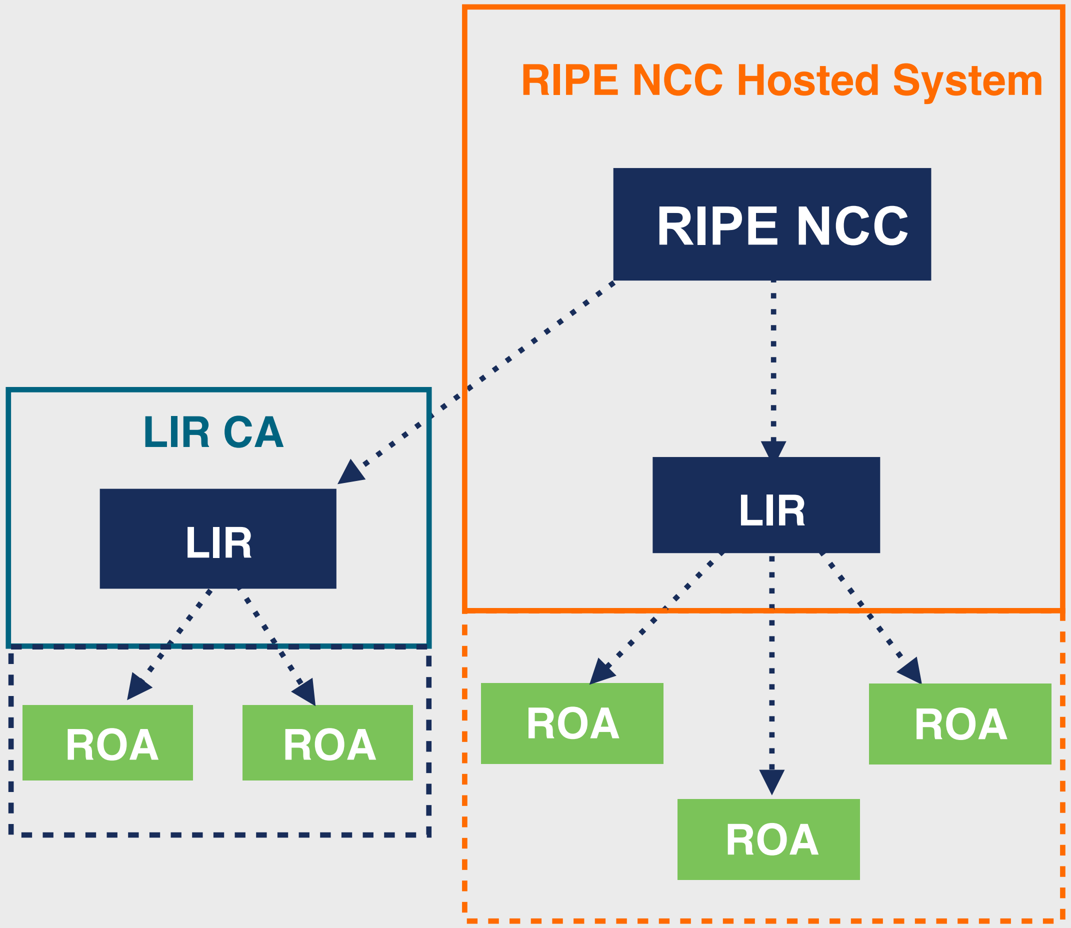
- ROAs are created and published using the **RIR's member portal**
- RIR hosts a CA (Certification Authority) for LIRs and signs all ROAs
- Automated signing and key rollovers



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

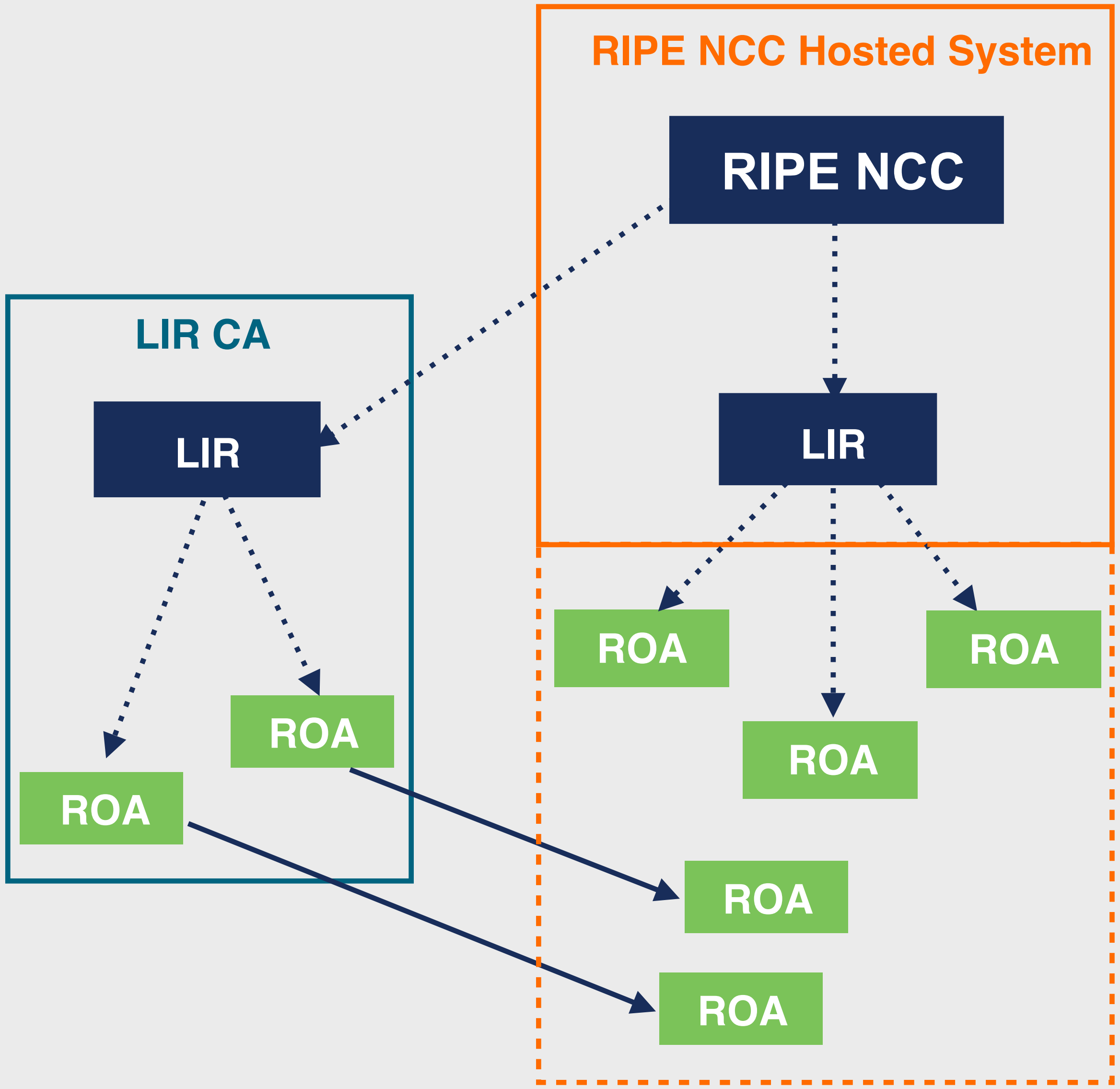
- Certificate Authority (CA) Software
  - **Krill** (NLnet Labs)
  - **rpkid** (Dragon Research Labs)



Publication as a Service

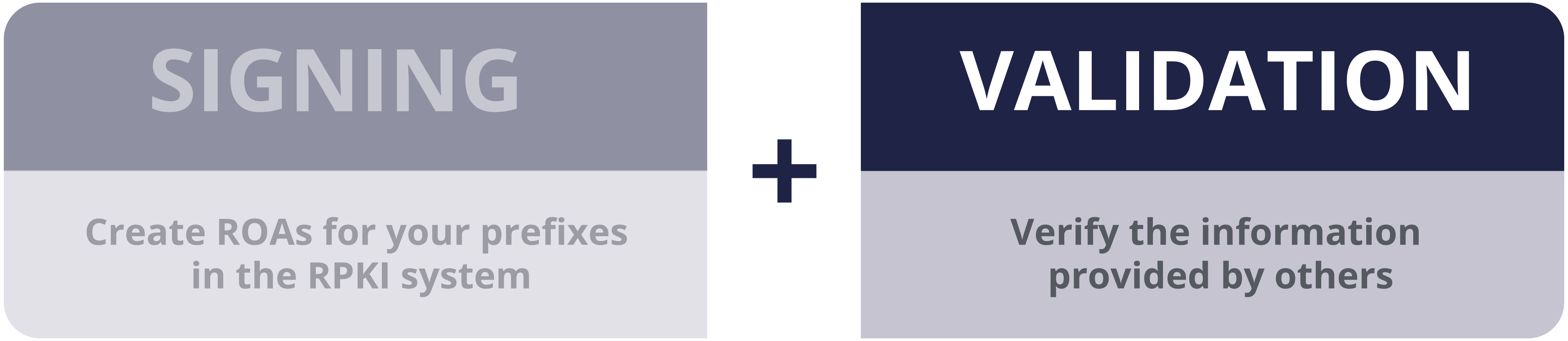
NEW!

- 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…



SIGNING

Create ROAs for your prefixes in the RPKI system

+

VALIDATION

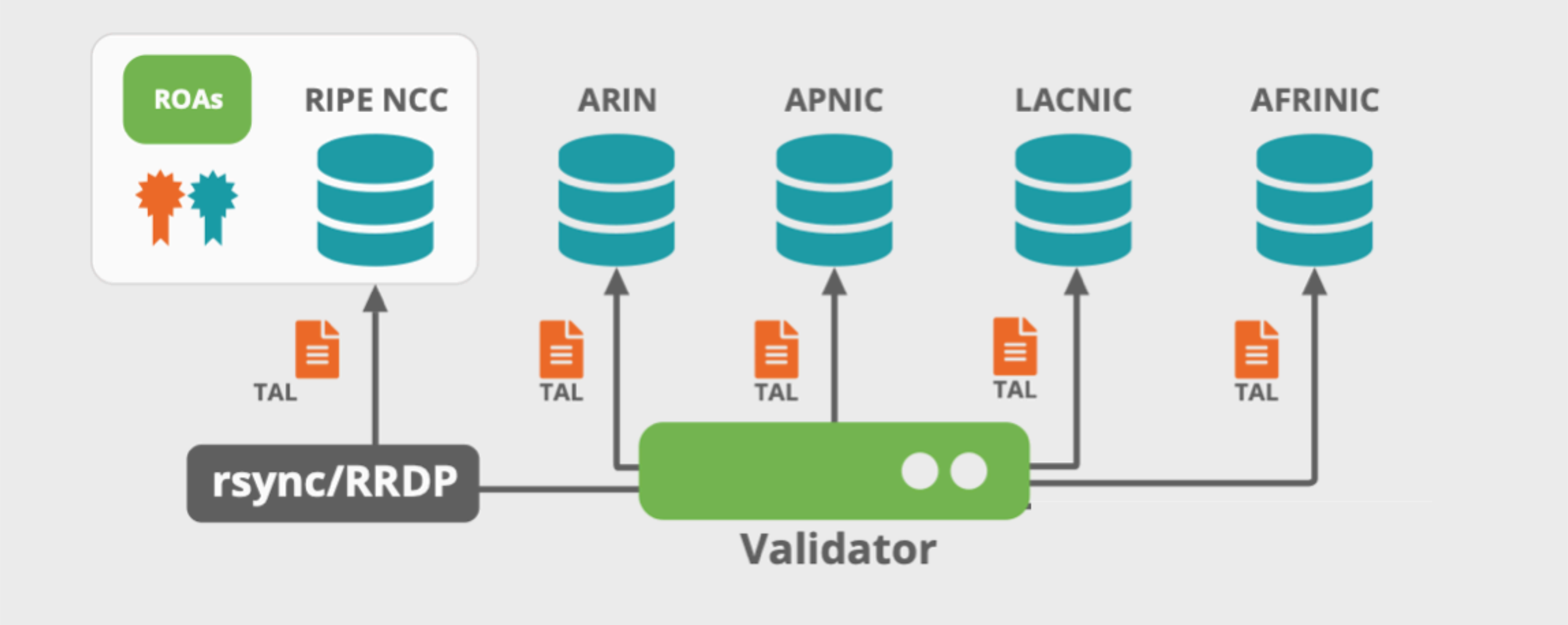
Verify the information provided by others

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

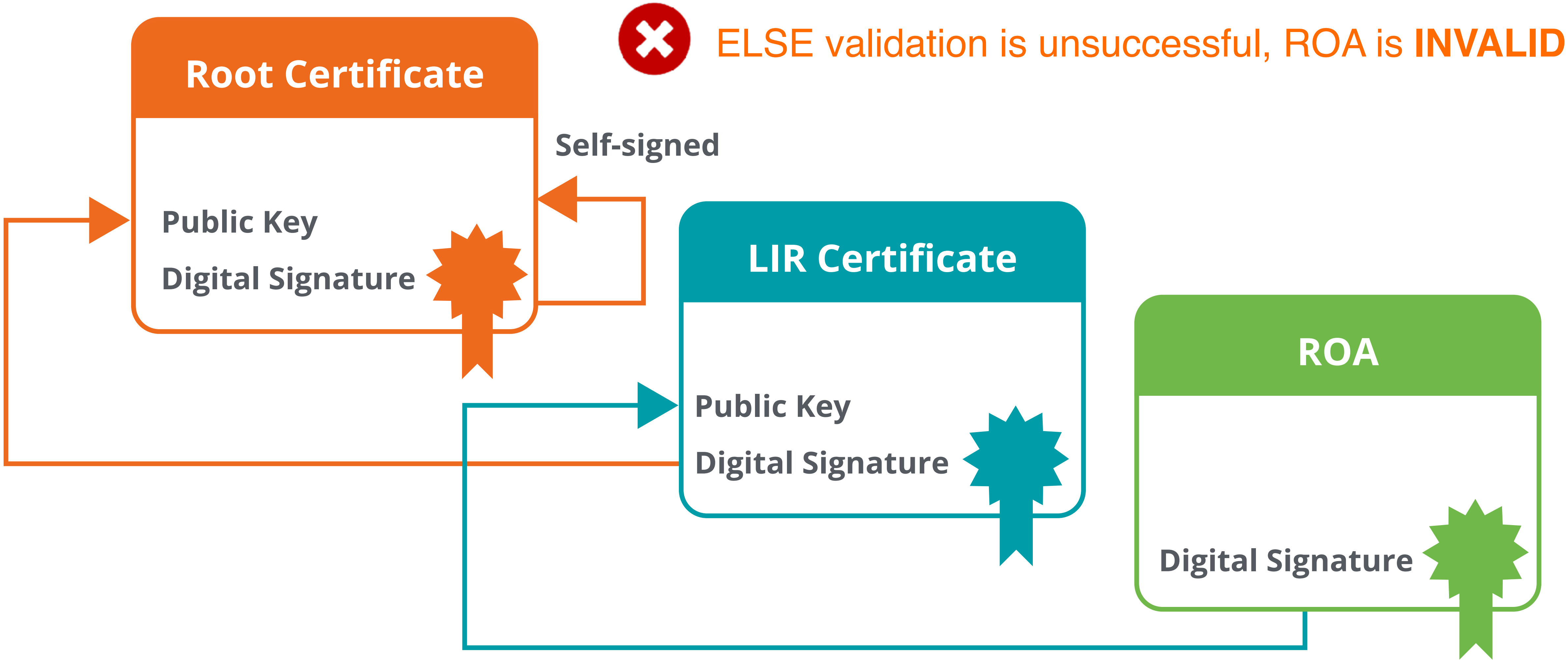
- Connects to RPKI repositories via rsync or RRDP protocol
- Uses TALs to connect to the repositories and download ROAs
- Validates chain of trust for all ROAs and associated CAs
- Creates a local “validated cache” with all the valid ROAs



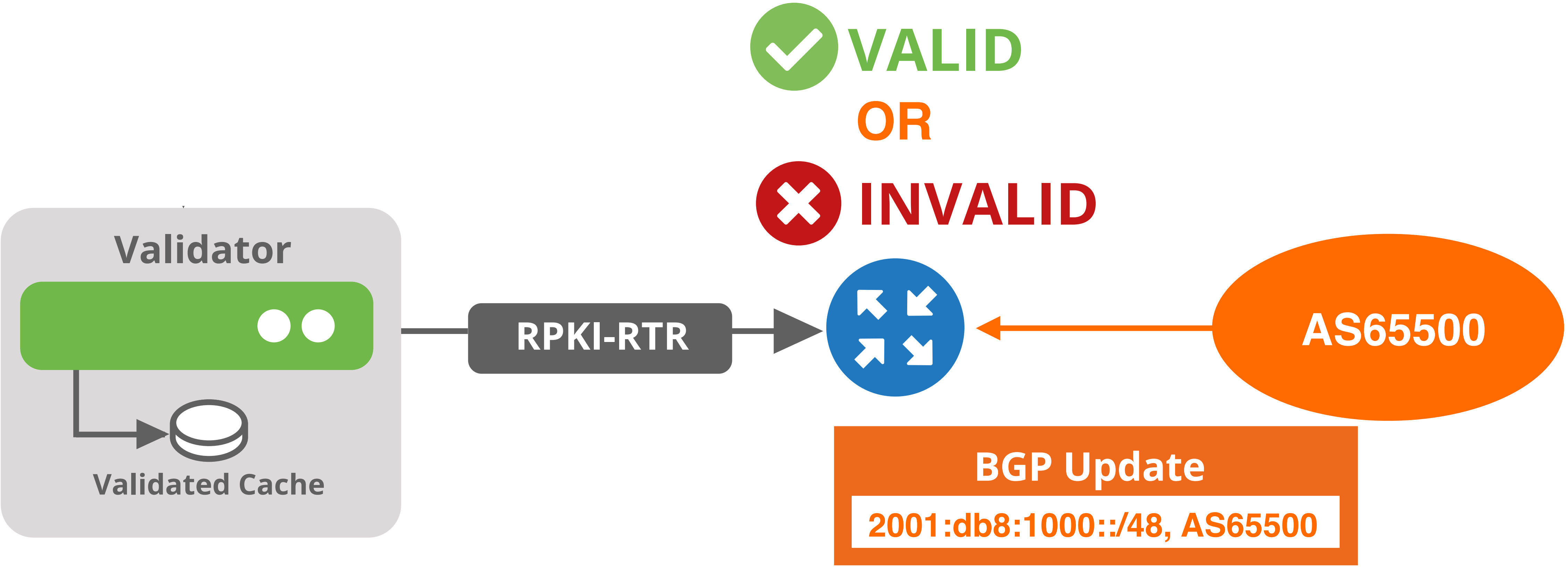
ROA Validation Process

✓ 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/cloudflare/cfrpki#octorpki

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

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

For more info…

https://rpki.readthedocs.io

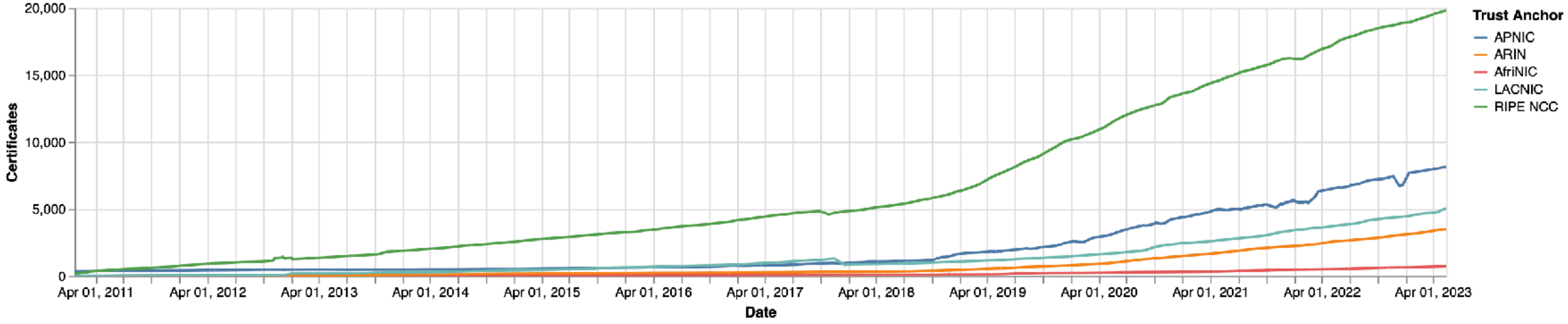
Run Different Validators

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

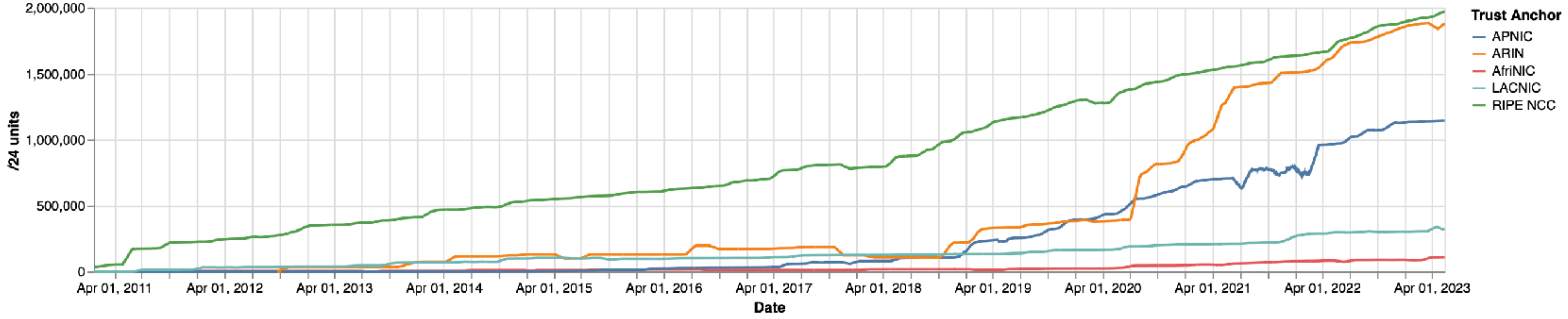
Source (13/5/23): https://rov-measurements.nlnetlabs.net/stats/

Steady growth: Adoption and ROAs

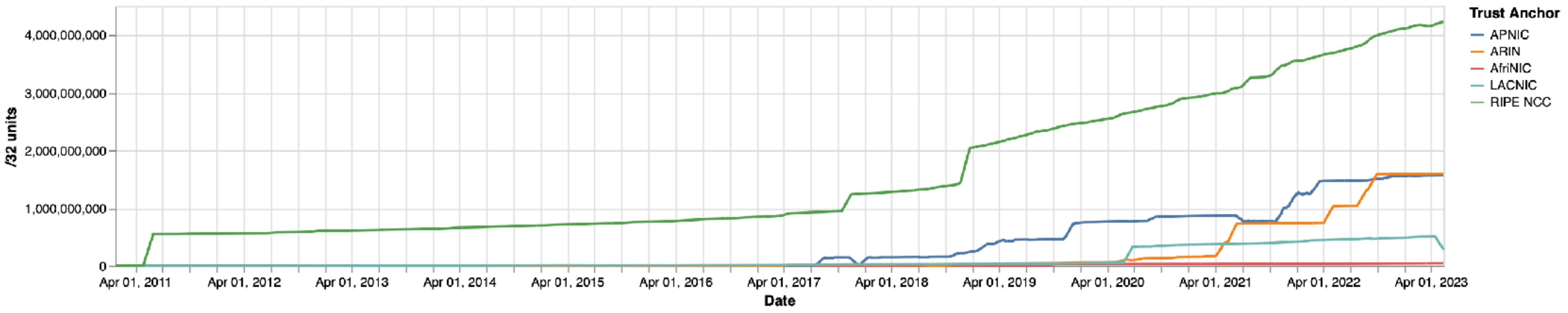
Number of Certificates



IPv4 address space in ROAs (/24s)



IPv6 address space in ROAs (/32s)



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

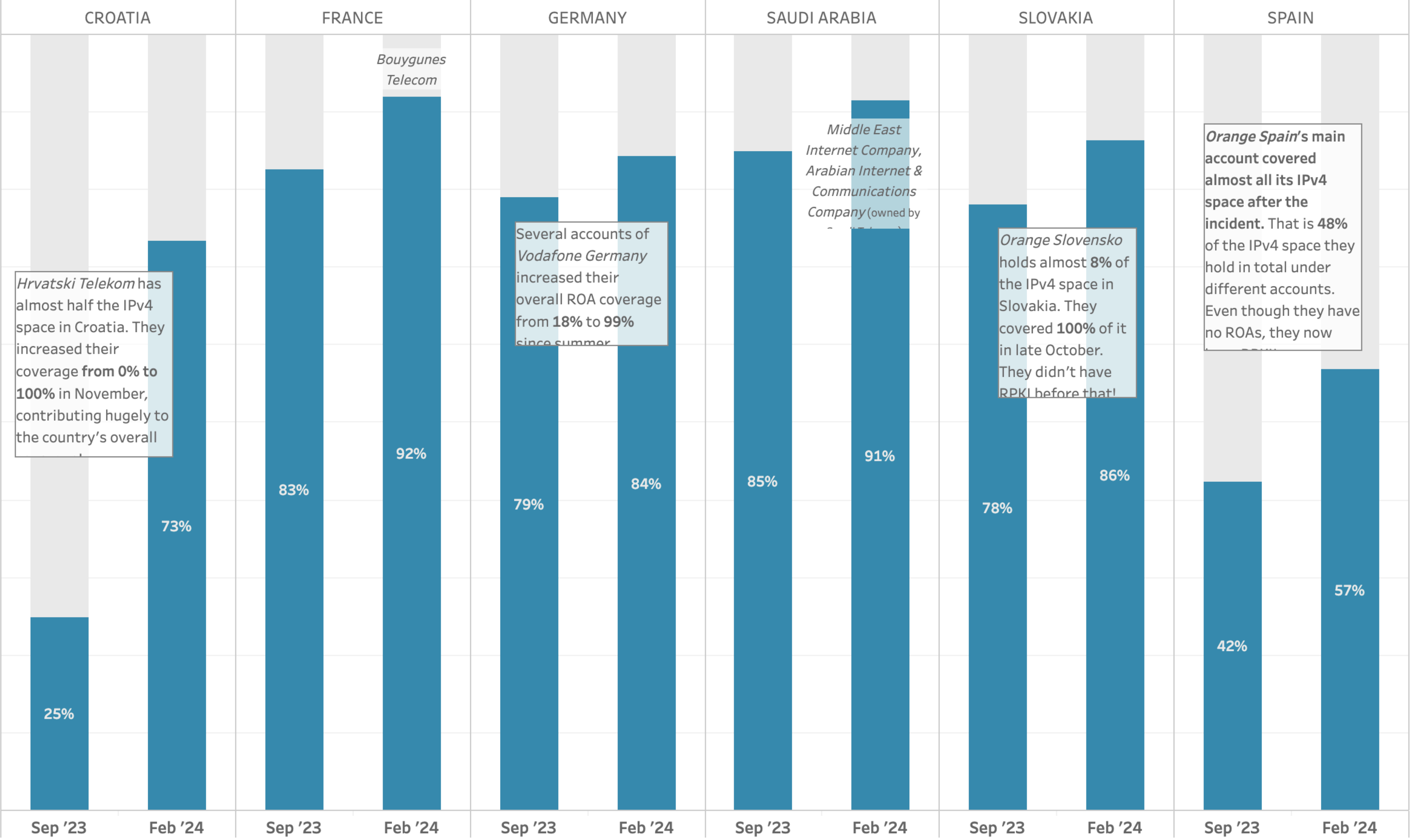
Adoption per RIR

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

September 2023 vs February 2024



Hrvatski Telekom has almost half the IPv4 space in Croatia. They increased their coverage **from 0% to 100%** in November, contributing hugely to the country's overall

Bouygunes Telecom

Several accounts of *Vodafone Germany* increased their overall ROA coverage from **18%** to **99%**

Middle East Internet Company, Arabian Internet & Communications Company (owned by

Orange Slovensko holds almost **8%** of the IPv4 space in Slovakia. They covered **100%** of it in late October. They didn't have

Orange Spain's **main account covered almost all its IPv4 space after the incident.** That is **48%** of the IPv4 space they hold in total under different accounts. Even though they have no ROAs, they now

Questions