RPKI at the root (of DNS)

Massimiliano Stucchi - ICANN Meeting

9th of March 2022

Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP)

BGP is one of the fundamental protocols that make the Internet work

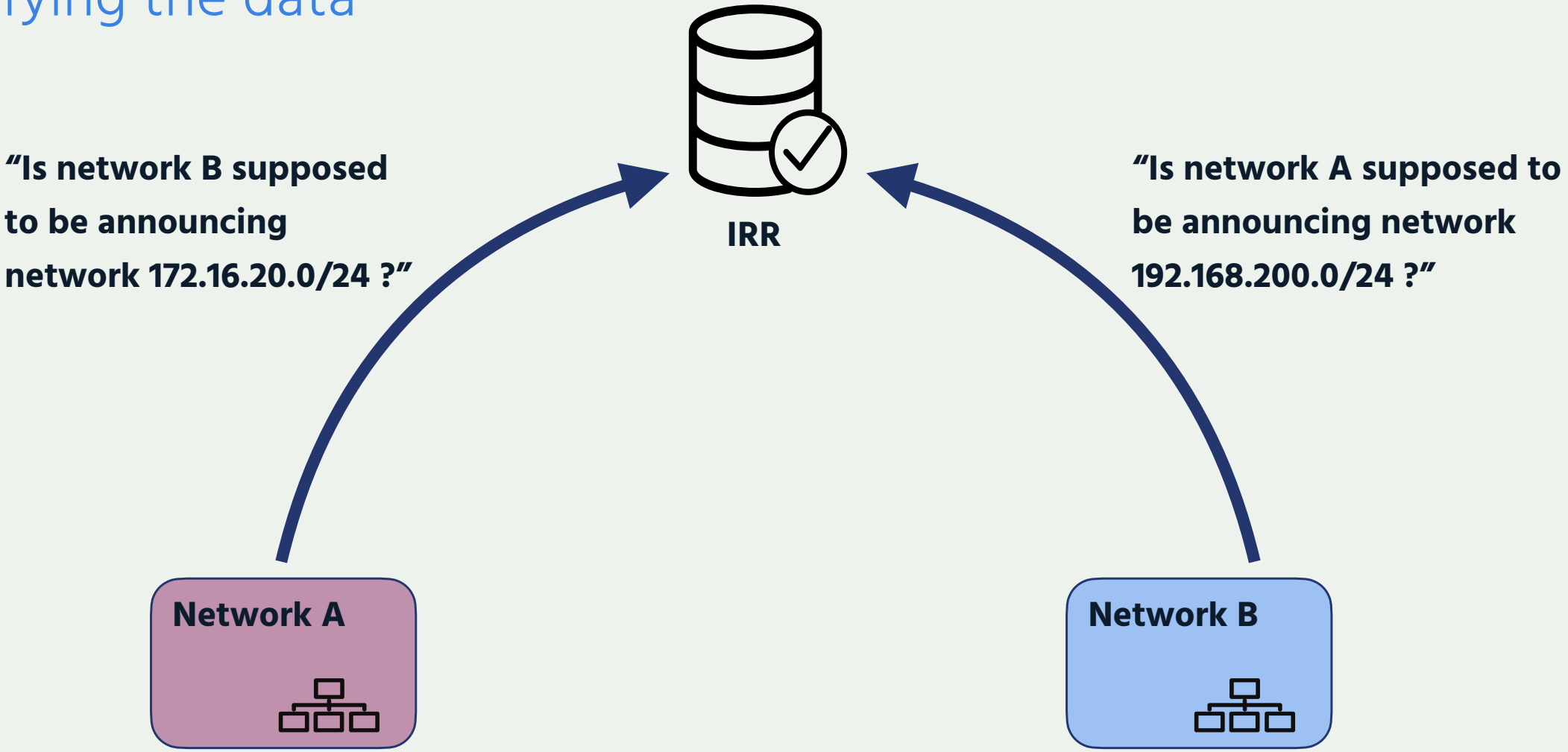
Used amongst Autonomous Systems to exchange routing information

Simple, yet complicated protocol

It works in clear-text, and requires “collaboration” between BGP speakers


Hi! My network is
192.168.200.0/24
Nice to meet you!
My network is
172.16.20.0/24
Network A
Network B

Verifying the data



Problem Statement

Some Internet Routing Registry (IRR) data cannot be fully trusted

- Accuracy
- Incomplete data
- Lack of maintenance

Not every Regional Internet Registry (RIR) has an IRR

- Third party databases need to be used (RADB, Operators)
- No verification of who holds IPs/ASNs

RPKI

Resource Public Key Infrastructure

Ties IP addresses and ASNs to public keys

Follows the hierarchy of the registries

Authorised statements from resource holders

- “ASN X is authorised to announce my Prefix Y”
- Signed, holder of Y

A bit of history

Operated since 2008 by all RIRs

- Community-driven standardisation (IETF)

Adds crypto-security to IPs and ASNs

- Provides **data you can trust**

RPKI

A security framework for verifying the association between resource holders and their Internet resources

Attaches digital certificates to network resources upon request that lists all resources held by the member

- AS Numbers
- IP Addresses

Operators associate those two resources

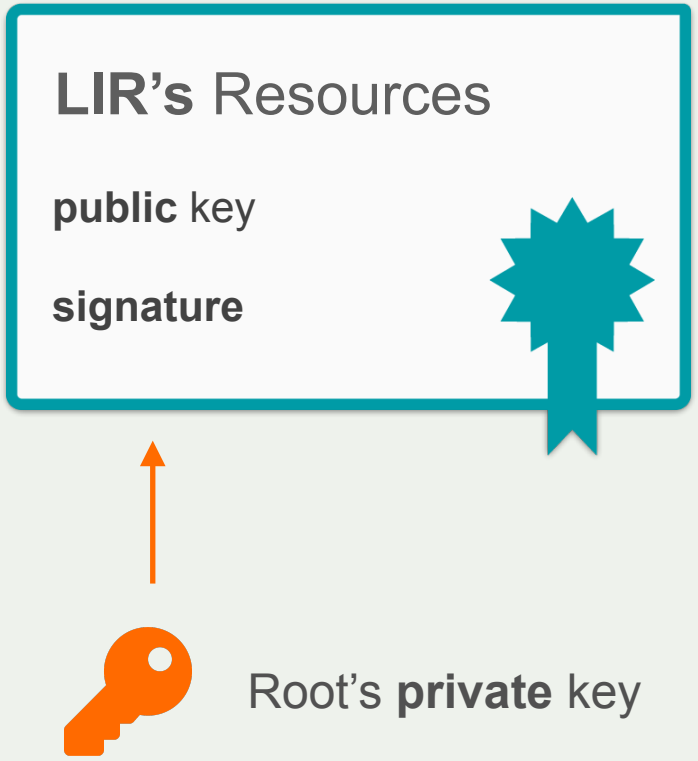
- Route Origin Authorisations (ROAs)

RPKI Chain of Trust

RIPE NCC Root Certificate

Self-signed

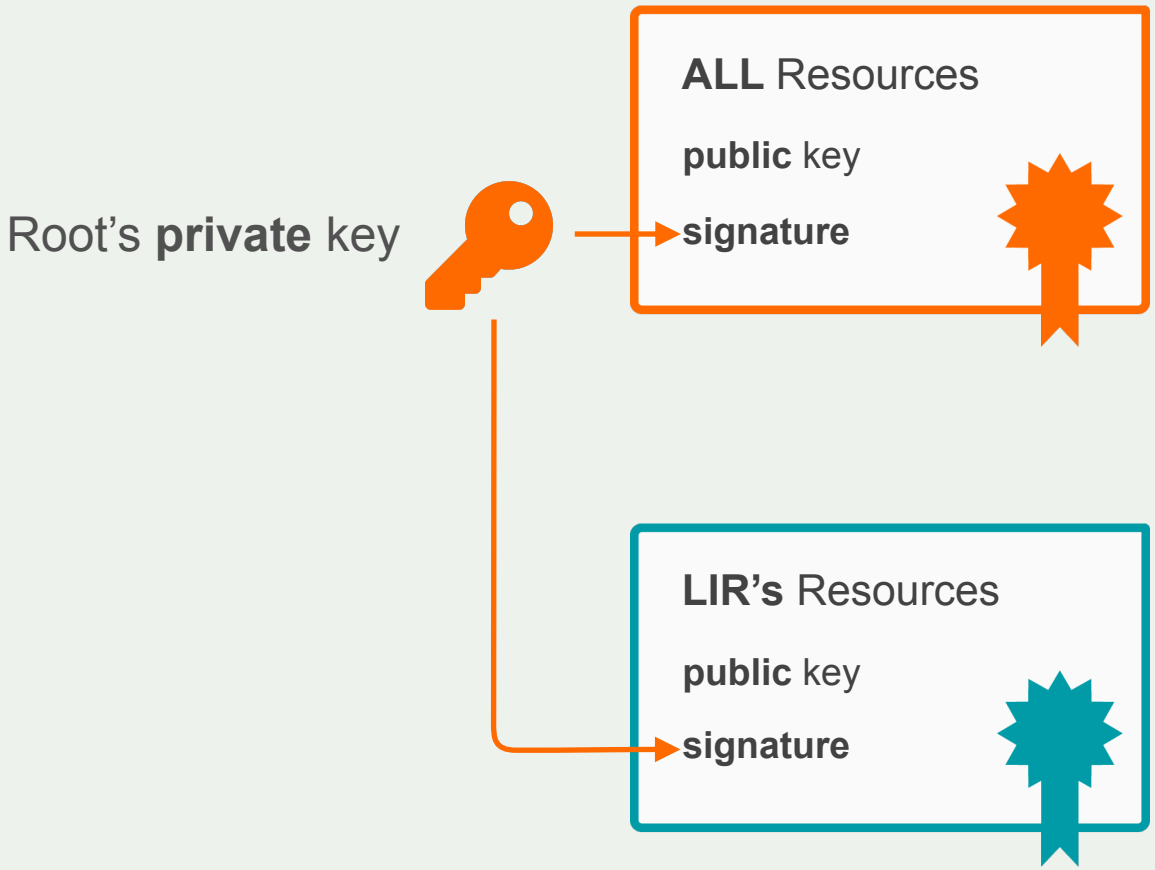
RPKI Chain of Trust



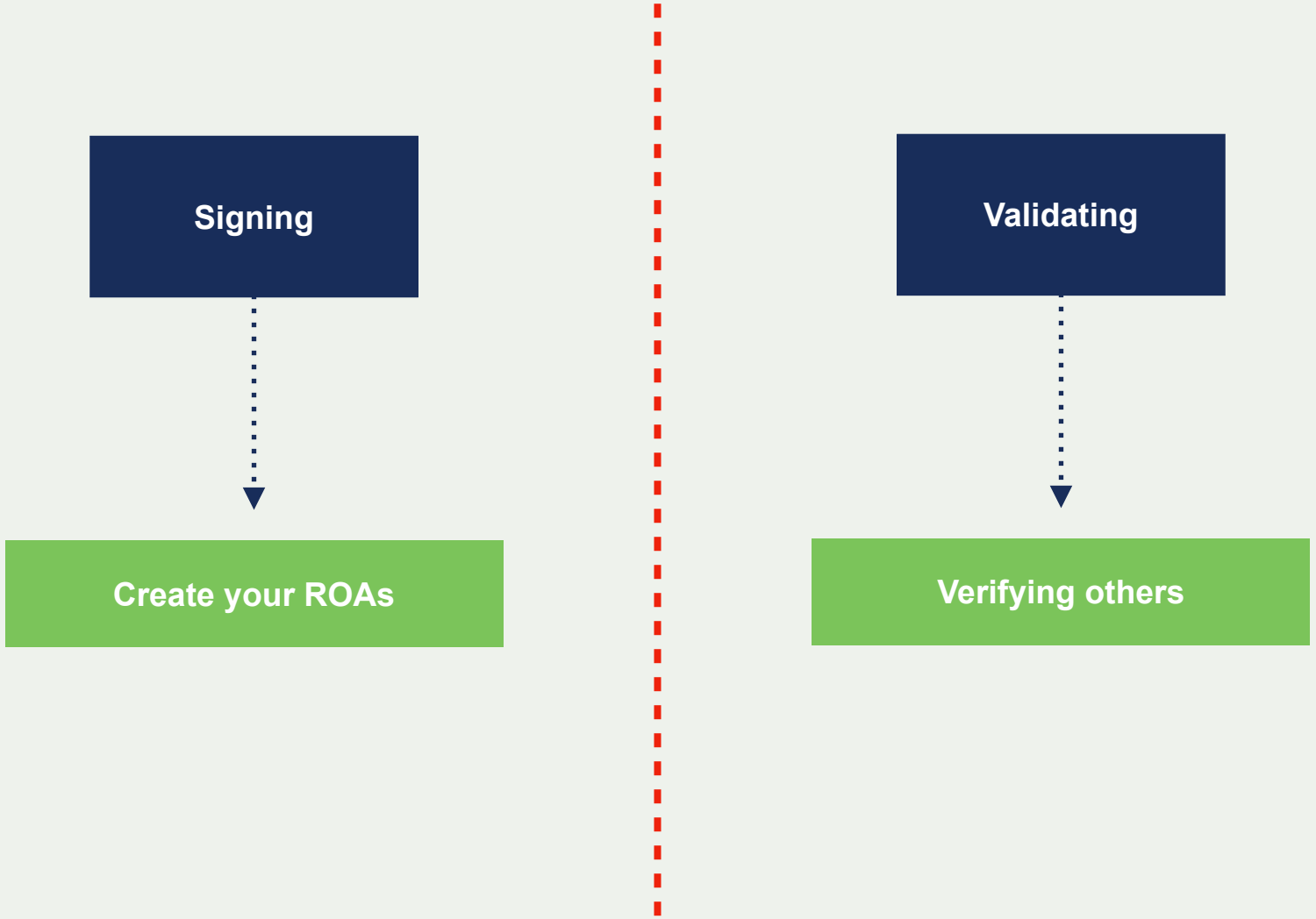
LIR Certificate

Signed by the Root private key

RPKI Chain of Trust



Two elements of RPKI



ROAs

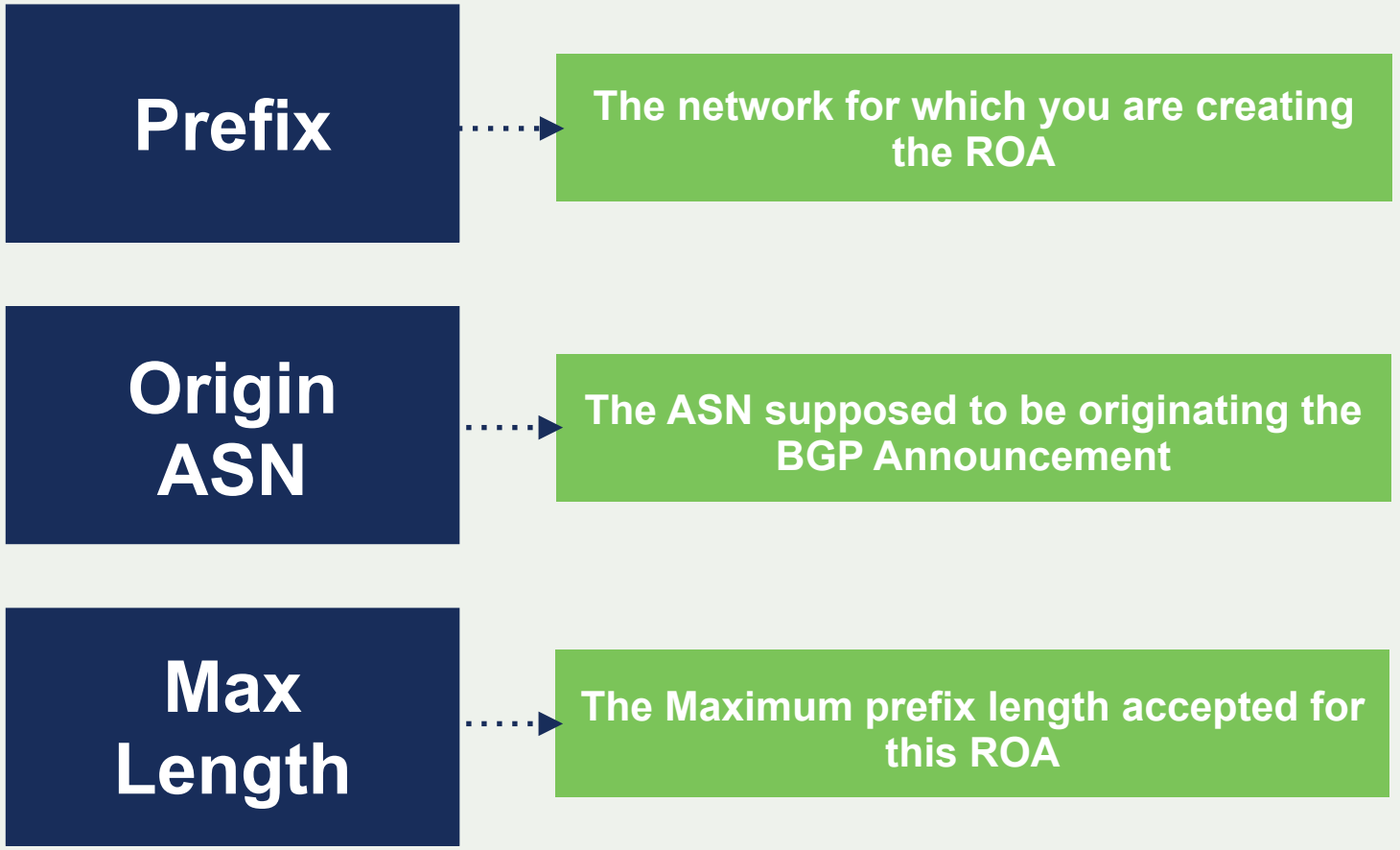
ROA (Route Origin Authorisation)

Network operators can create a ROA for each one of their resources (IP address ranges)

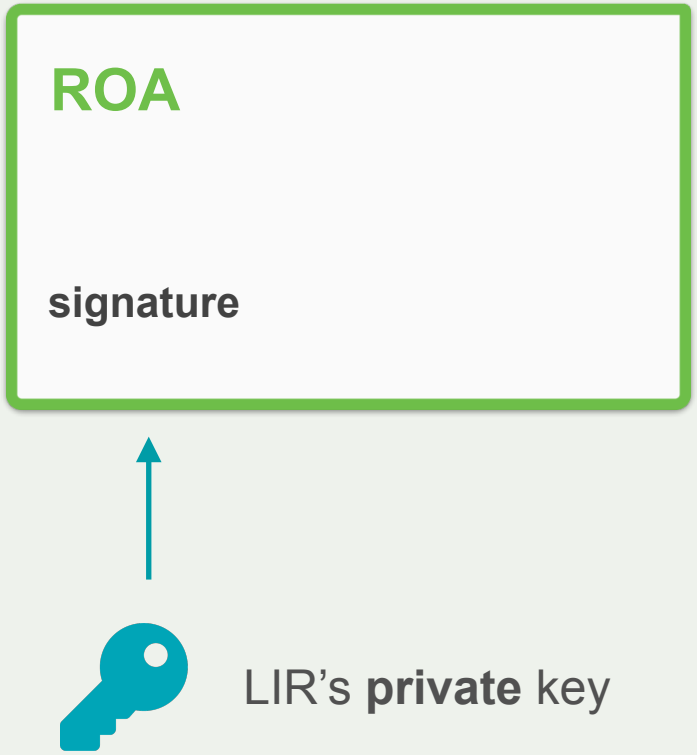
Multiple ROAs can be created for an IP range

ROAs can overlap

What is in a ROA ?



Route Origin Authorisation

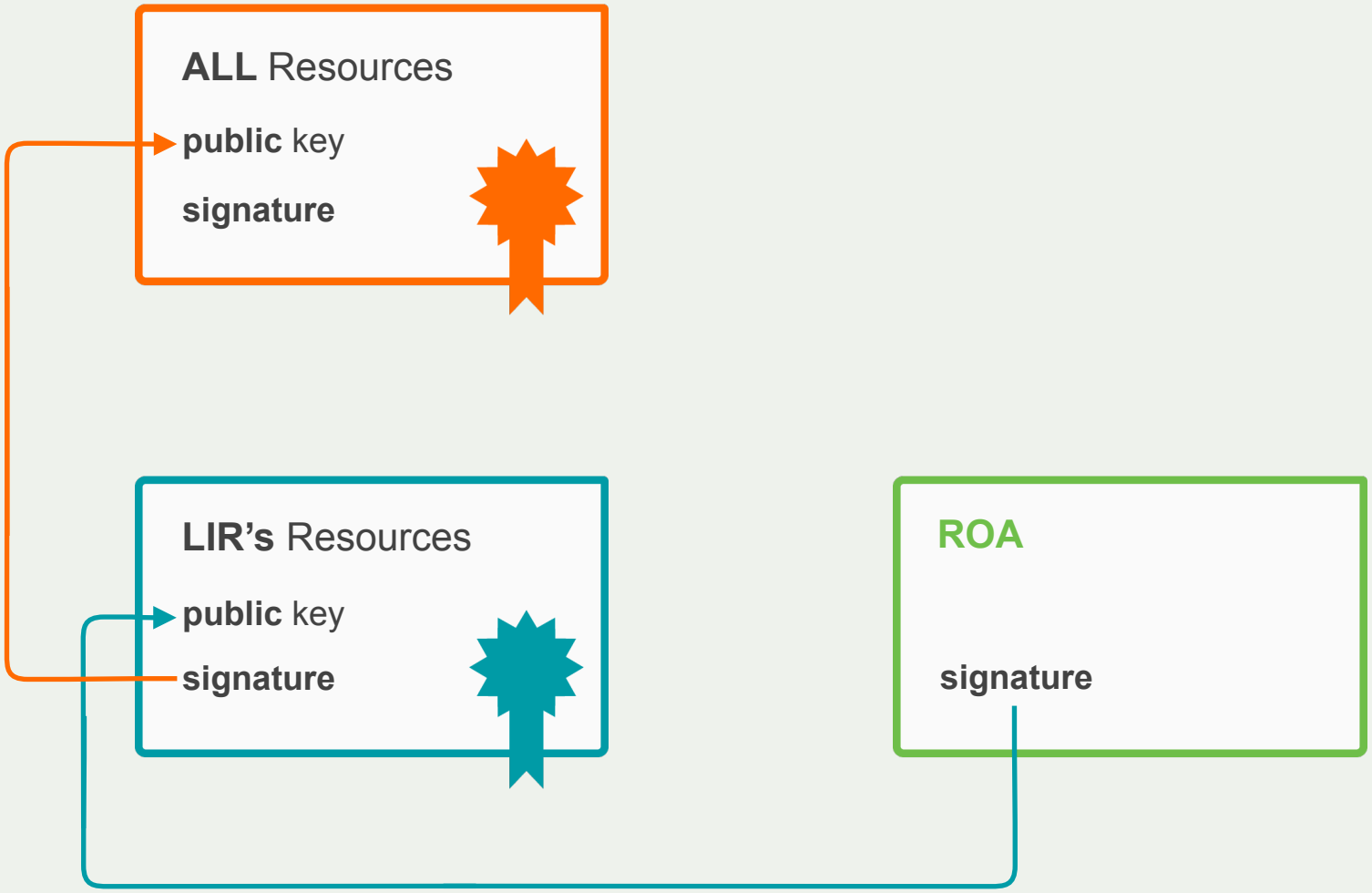


Prefix

is authorised to be announced by

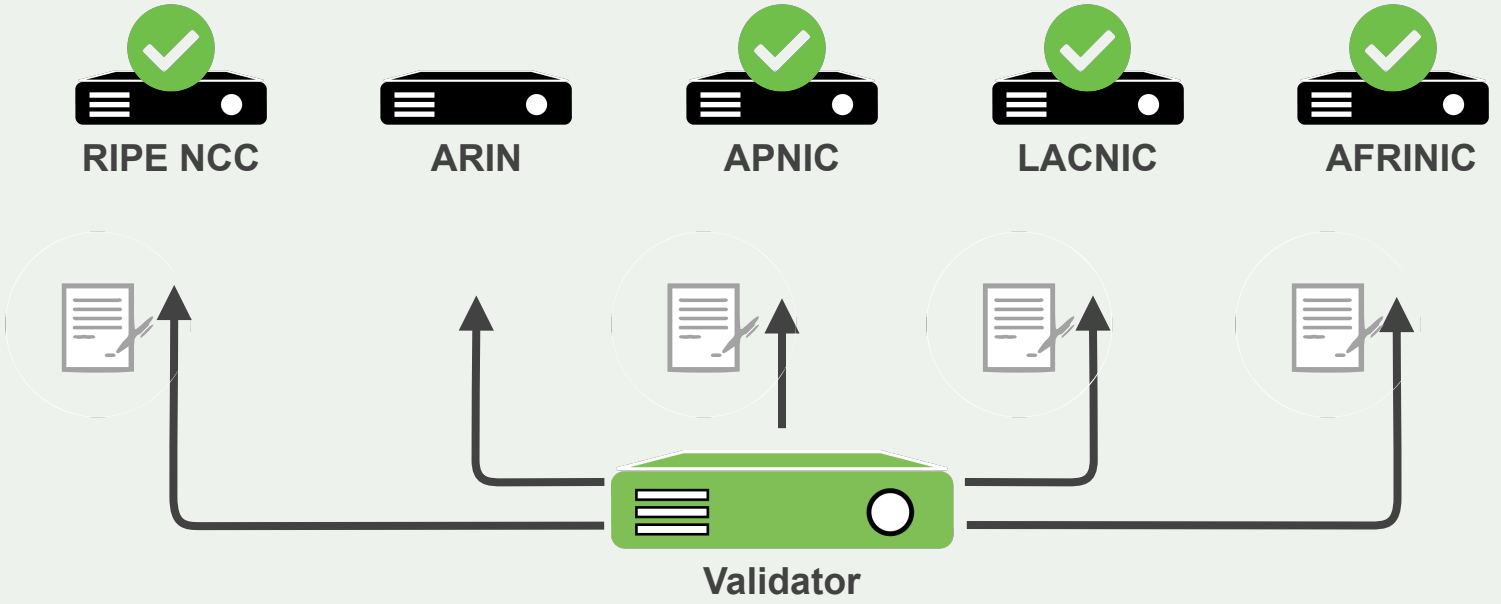
AS Number

RPKI Chain of Trust

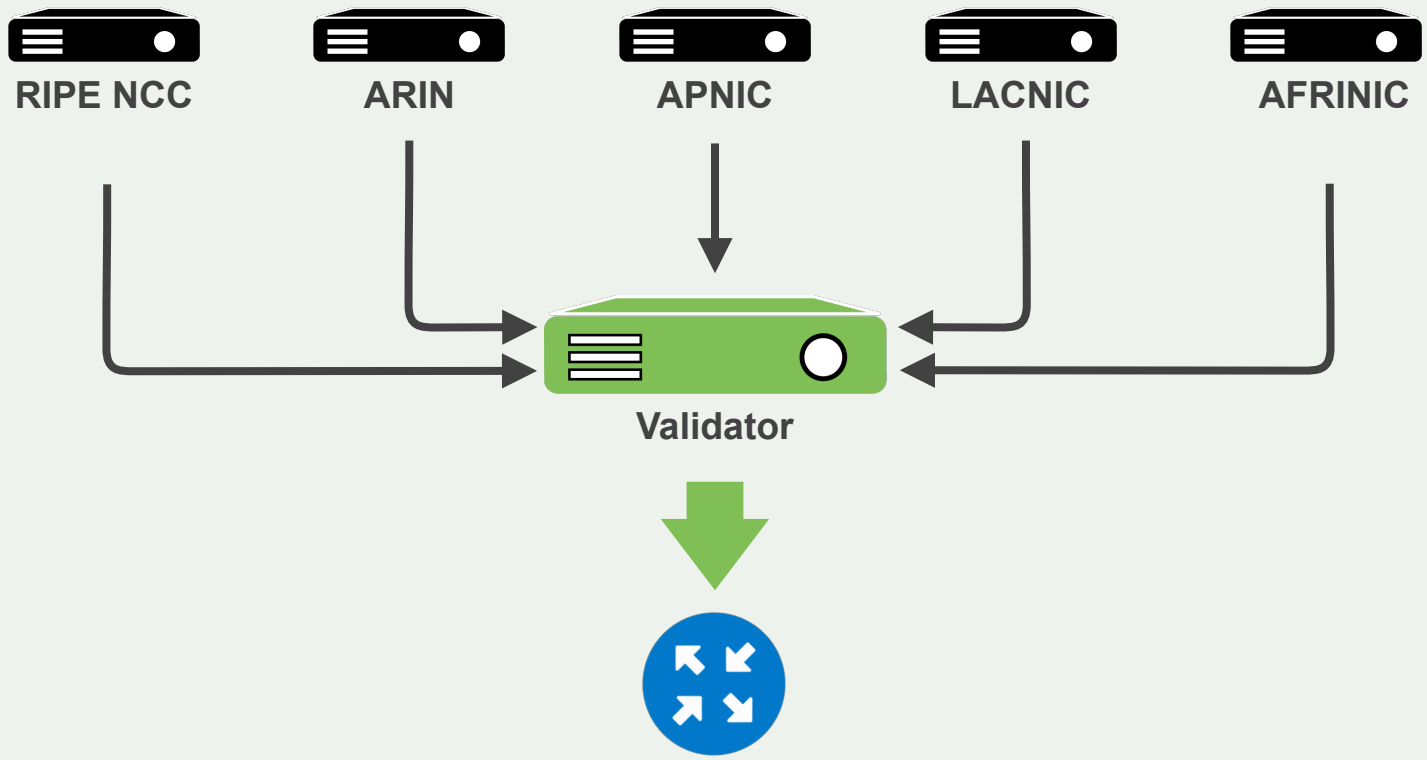


RPKI Validation

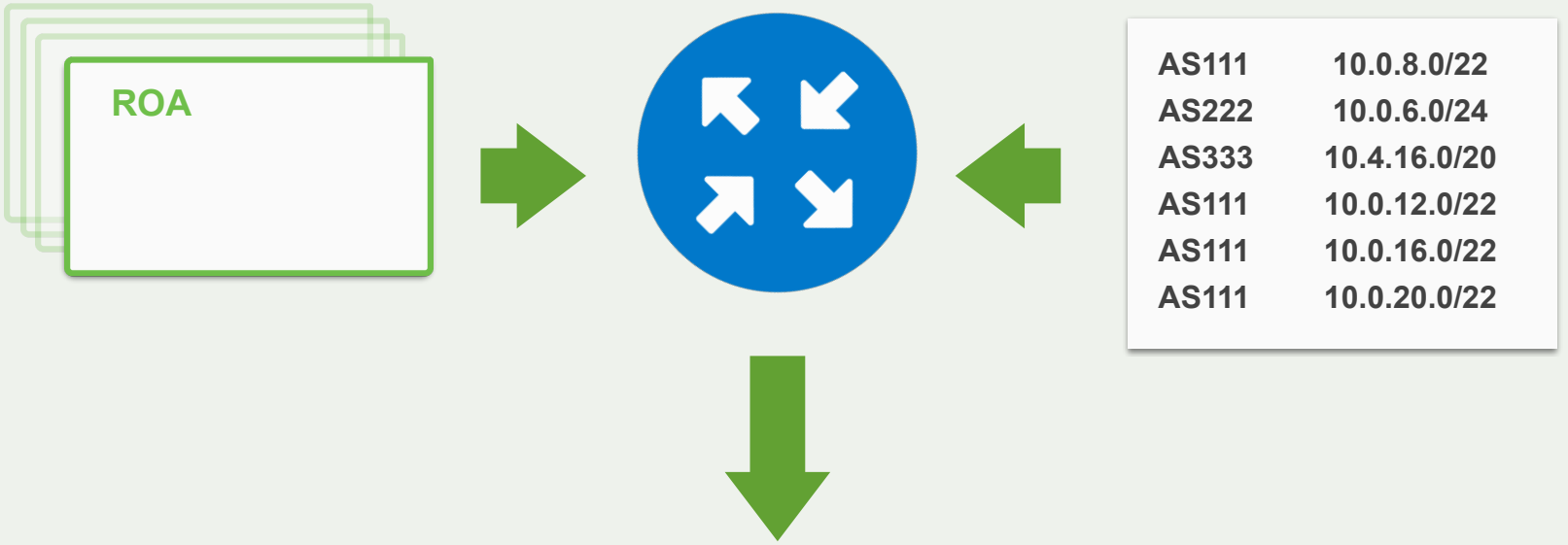
Trust Anchor Locator (TAL)



Relying Party



Relying Party



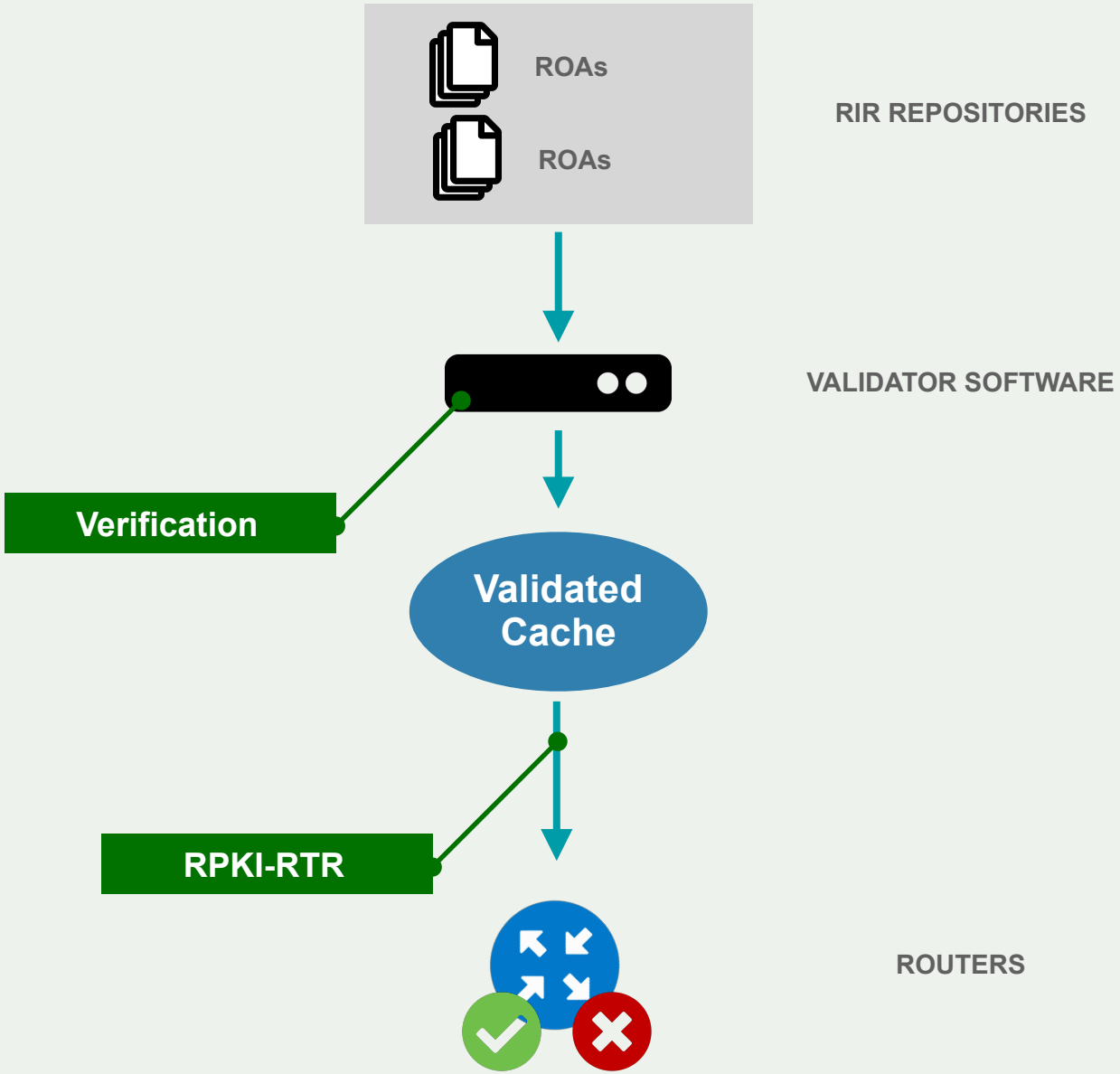
ROA Validation

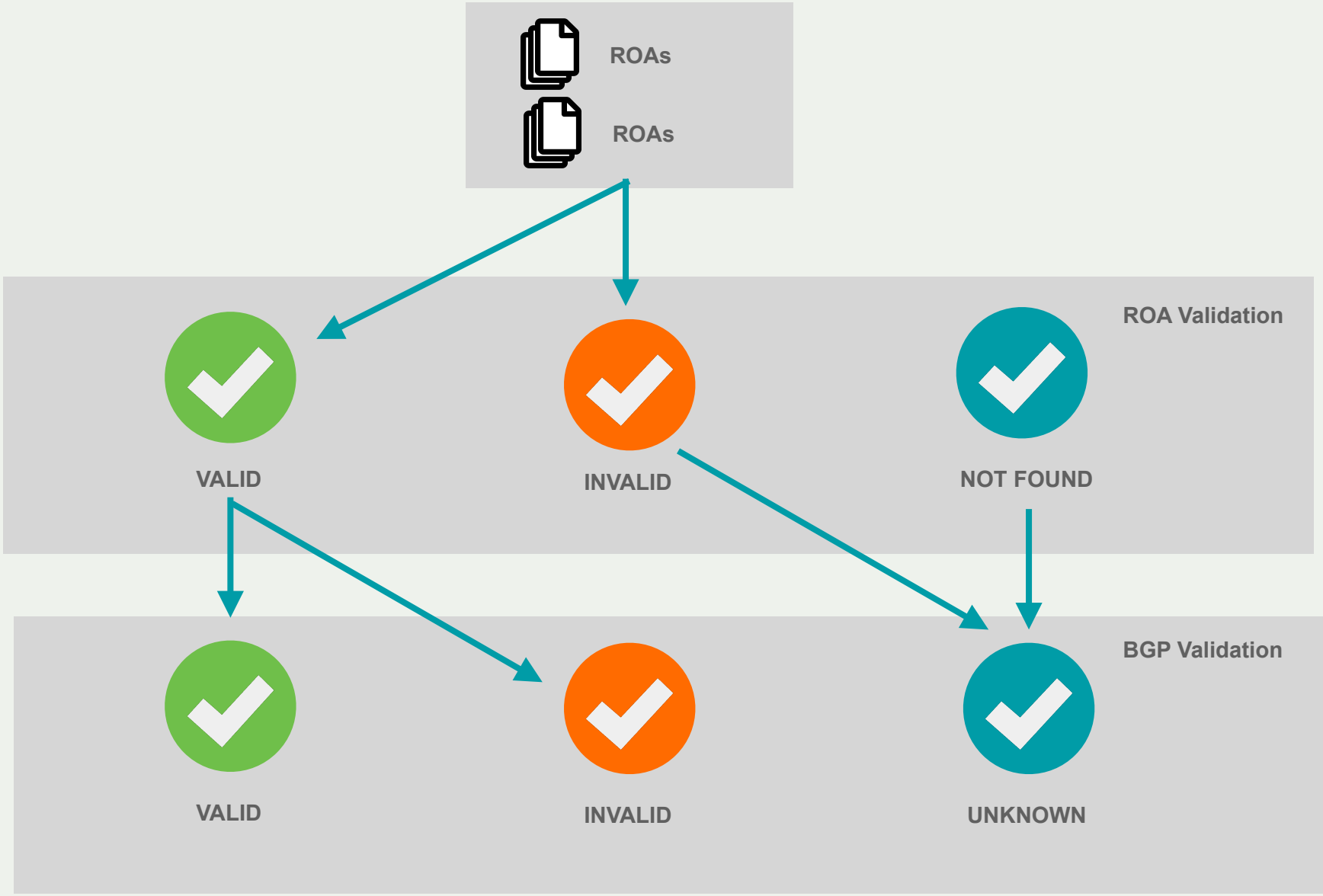
Routers receive data from the validated cache via RPKI-RTR

Based on this and on BGP announcements, you have to make decisions

- Accept or discard the BGP Announcement
- As temporary measure, you could influence other attributes, such as Local Preference

RPKI-RTR


ROAs
ROAs
RIR REPOSITORIES
VALIDATOR SOFTWARE
Verification
Validated Cache
RPKI-RTR
ROUTERS


ROAs
ROAs
ROA Validation
VALID
INVALID
NOT FOUND
BGP Validation
VALID
INVALID
UNKNOWN

RPKI DNS Statistics

“How many of the authoritative DNS Servers for TLDs and ccTLDs are in networks covered by ROAs ?”

6927 Nameservers
on IPv6

7571 Nameservers
on IPv4

Measurements

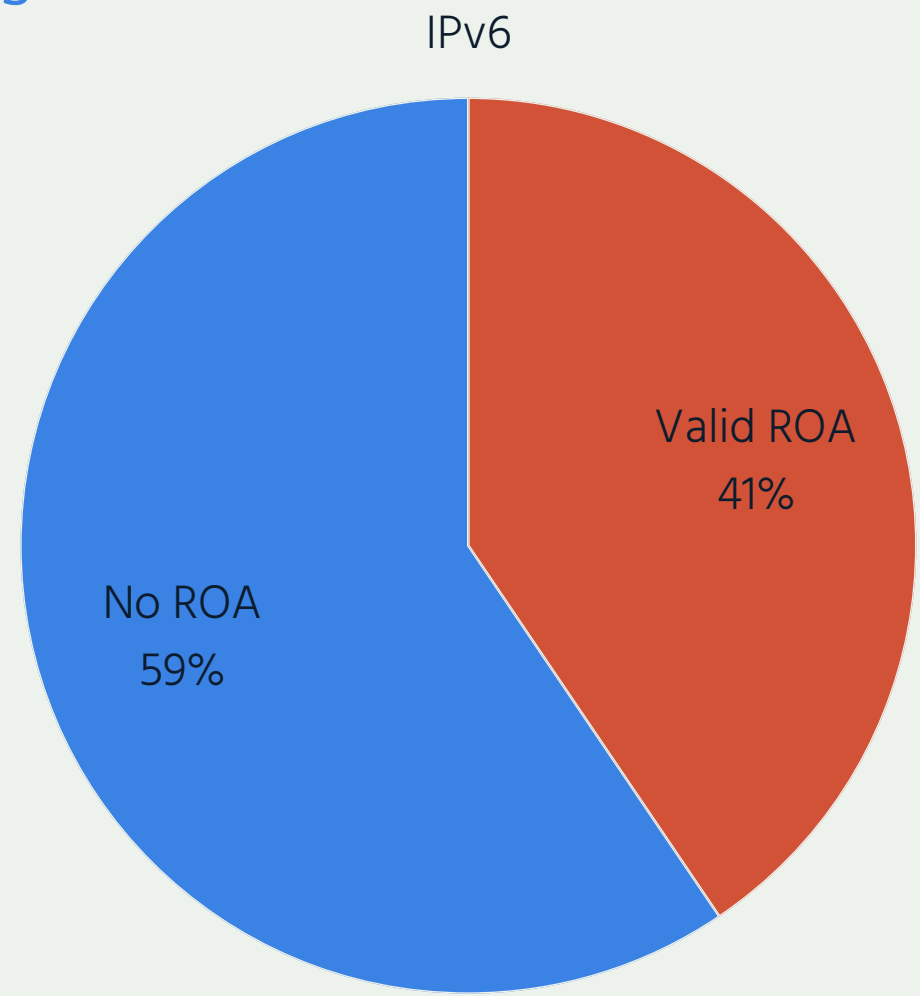
We checked, for every TLD:

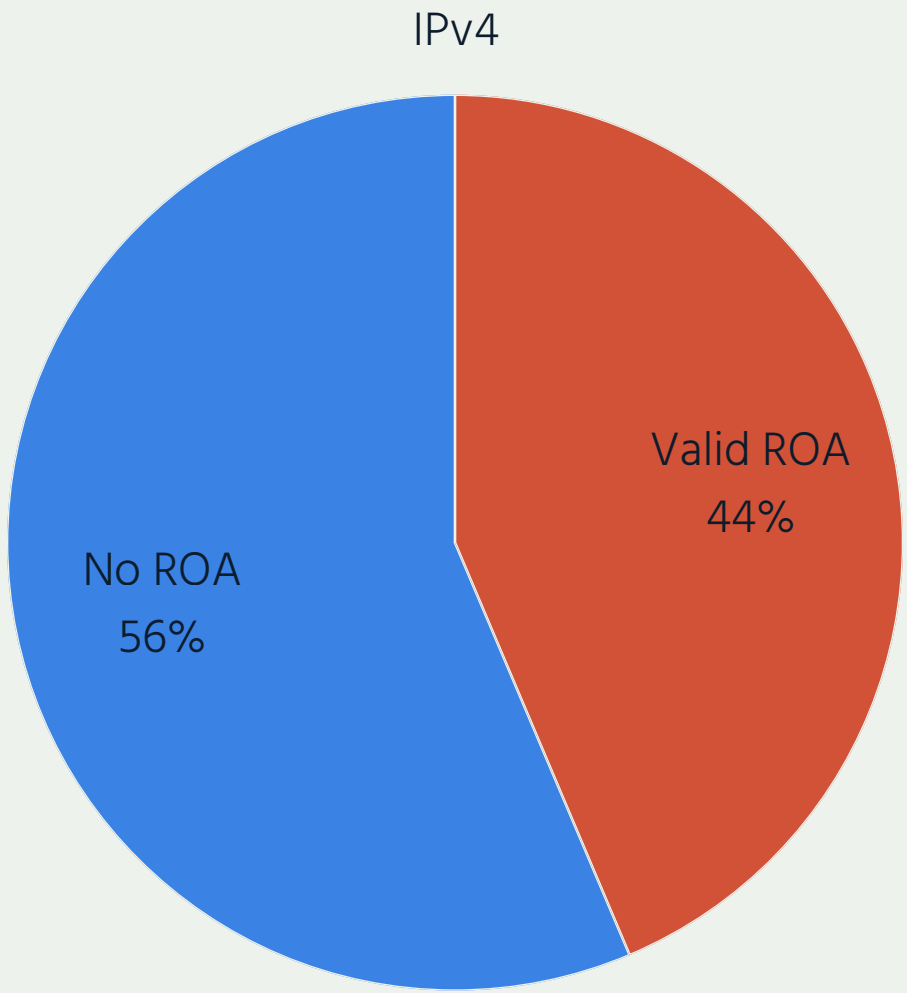
All the name servers listed as authoritative

For each one of these we checked every BGP announcement and its status

We picked only the Valid and Unknown

ROAs



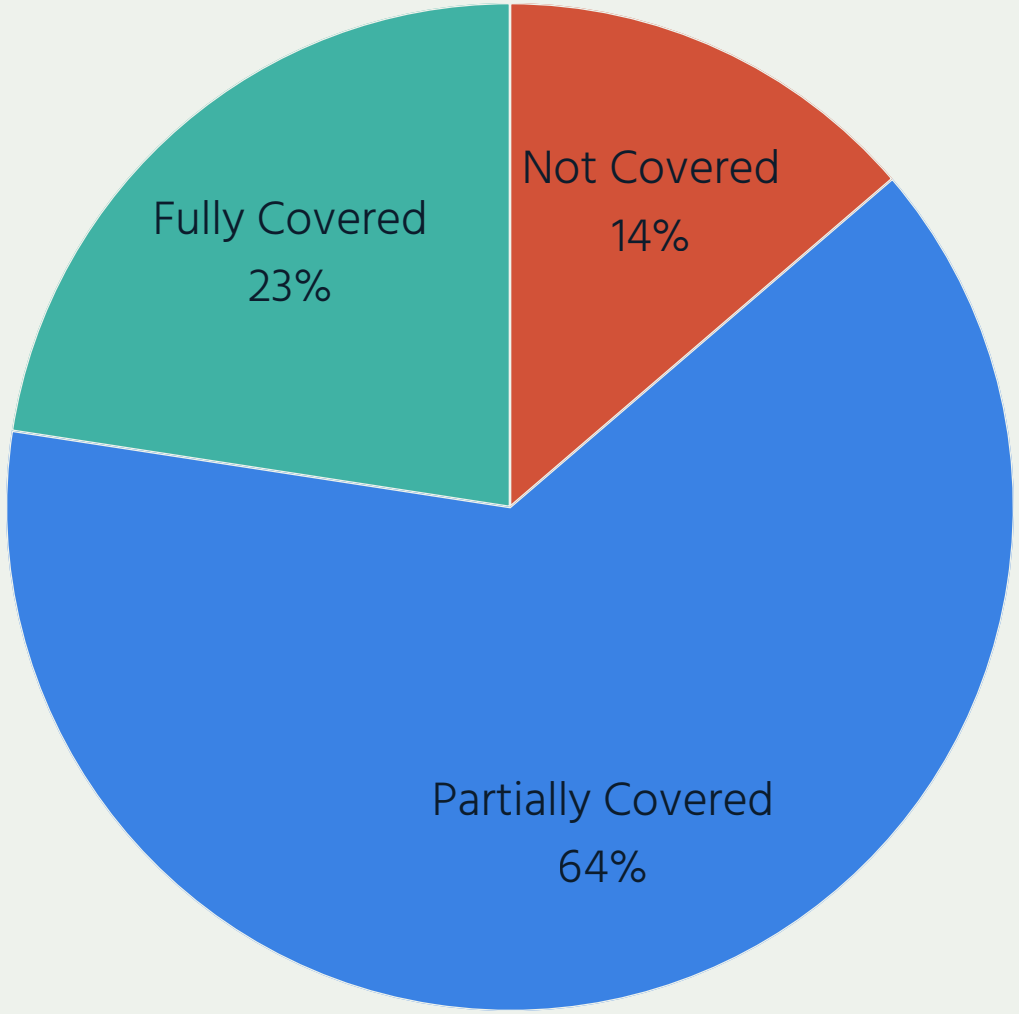


ccTLDs

"Fully Covered" means **every** BGP announcement has a covering ROA

"Partially Covered" means **at least one** BGP announcement is **missing** a covering ROA

"Not Covered" means **no** BGP announcement has a covering ROA

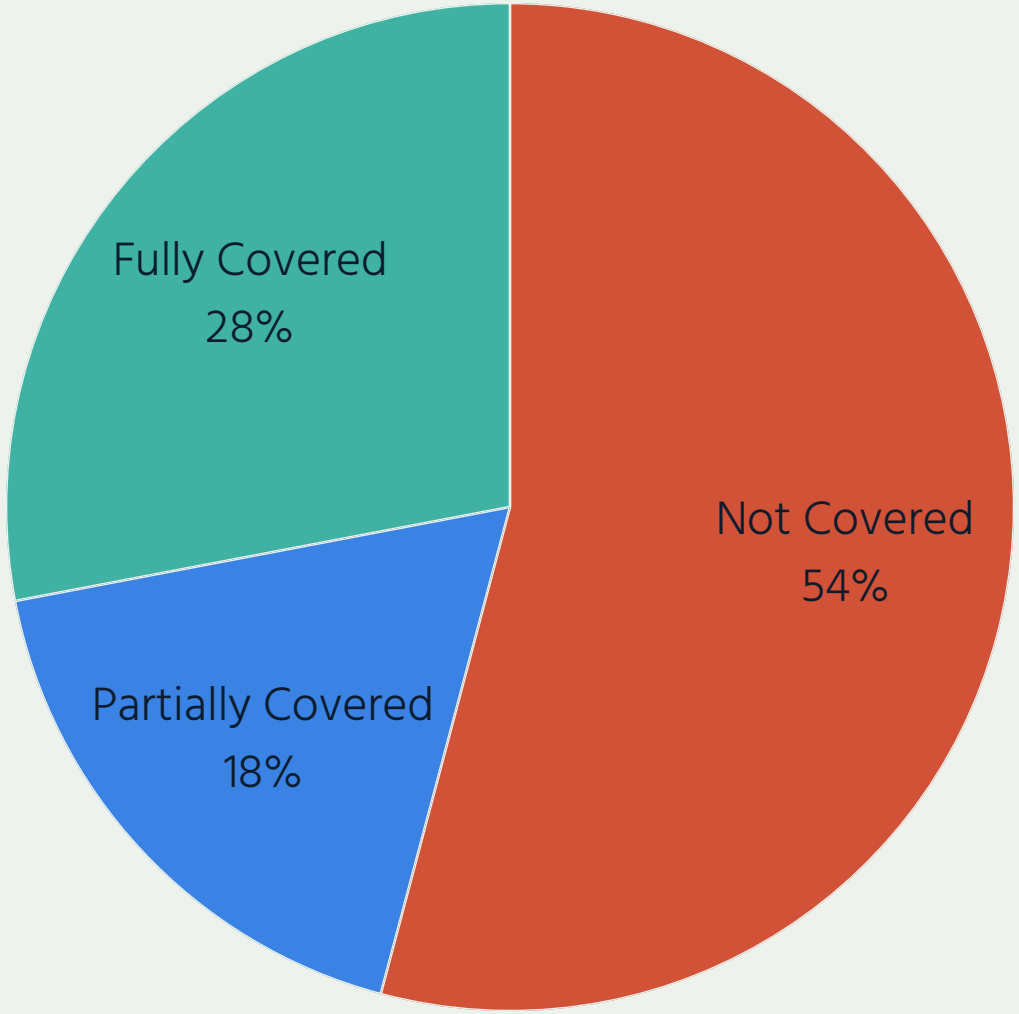


Other TLDs

"Fully Covered" means **every** BGP announcement has a covering ROA

"Partially Covered" means **at least one** BGP announcement is **missing** a covering ROA

"Not Covered" means **no** BGP announcement has a covering ROA



What could be done ?

Actions

Talk to your network engineers or network operators and ask them to create ROAs

Prepare your network to validate ROAs (ROV)

Join MANRS (Mutually Agreed Norms for Routing Security) - manrs.org

Possible Challenges

Legacy space

Routers not capable of doing ROV

Network operator not willing to set up ROV

Questions ?

stucchi@isoc.org

@stucchimax (twitter, telegram)

Merci.

Rue Vallin 2
CH-1201 Geneva
Switzerland

11710 Plaza America Drive
Suite 400
Reston, VA 20190, USA

Rambla Republica de Mexico 6125
11000 Montevideo,
Uruguay

66 Centrepoint Drive
Nepean, Ontario, K2G 6J5
Canada

Science Park 400
1098 XH Amsterdam
Netherlands

3 Temasek Avenue, Level 21
Centennial Tower
Singapore 039190