RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Resource Public Key Infrastructure

The PKI that makes the routing on the Internet more secure

Ondřej Caletka | 1 December 2025

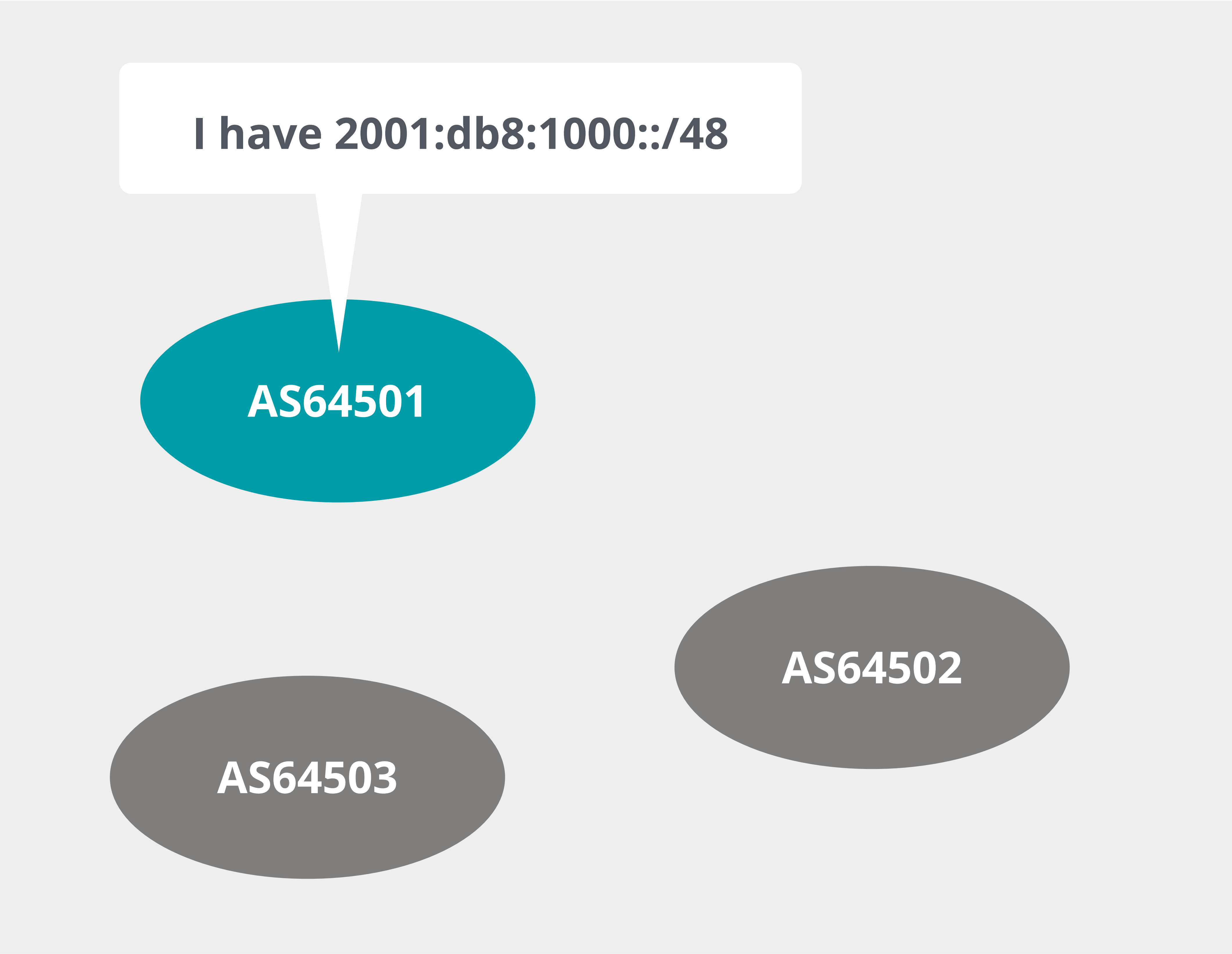
RIPE NCC Learning & Development

The Need for BGP Security

Is BGP Secure?

In theory:

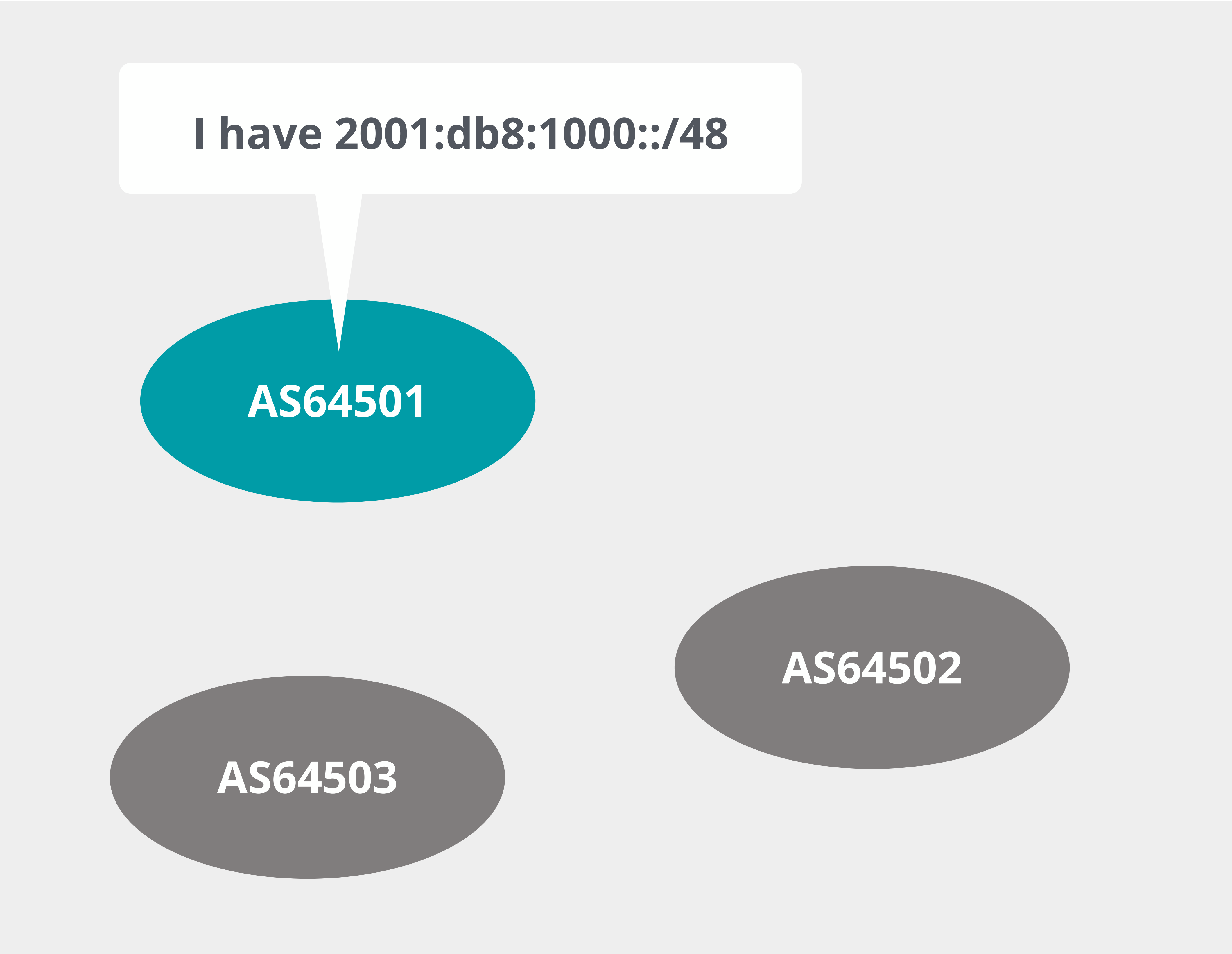
Only the legitimate resource holder should be announcing the prefix



Is BGP Secure?

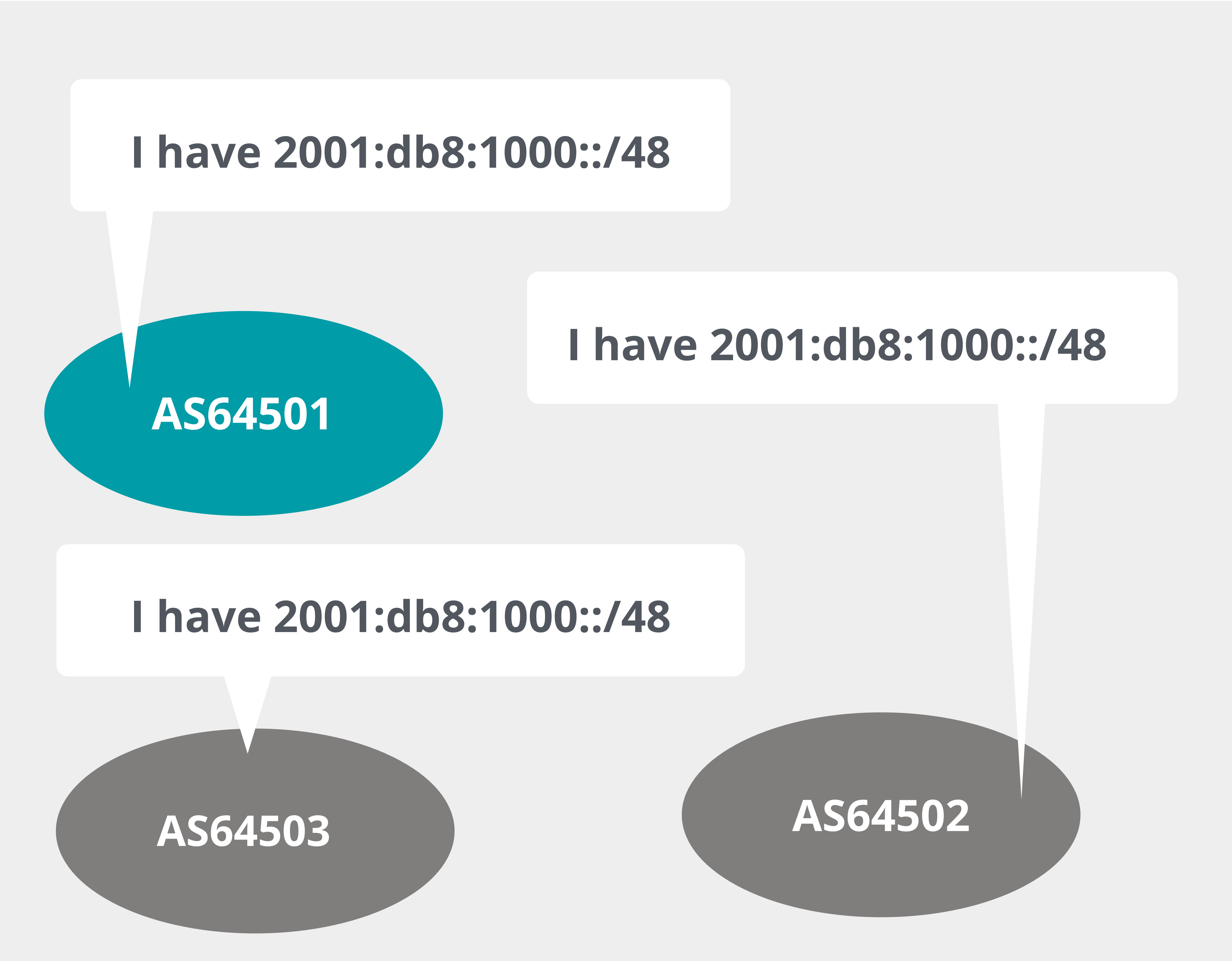
In theory:

Only the legitimate resource holder should be announcing the prefix



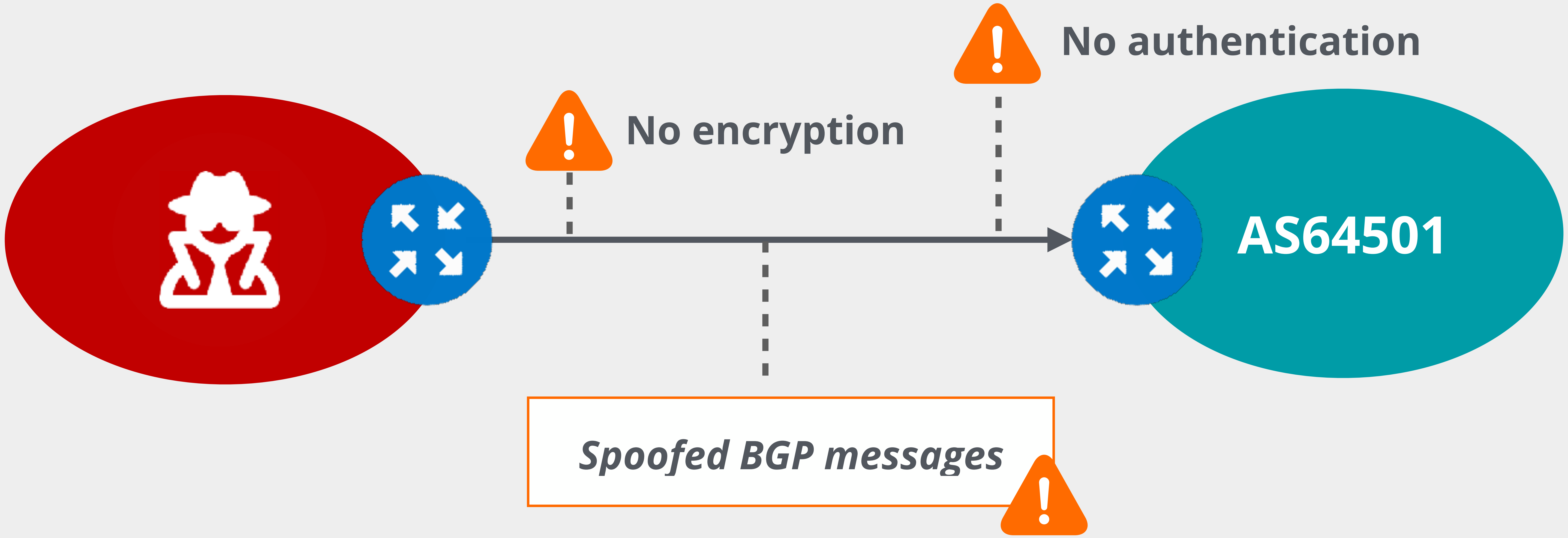
In practice:

Any AS can announce any prefix


I have 2001:db8:1000::/48
I have 2001:db8:1000::/48
AS64501
I have 2001:db8:1000::/48
AS64503
AS64502

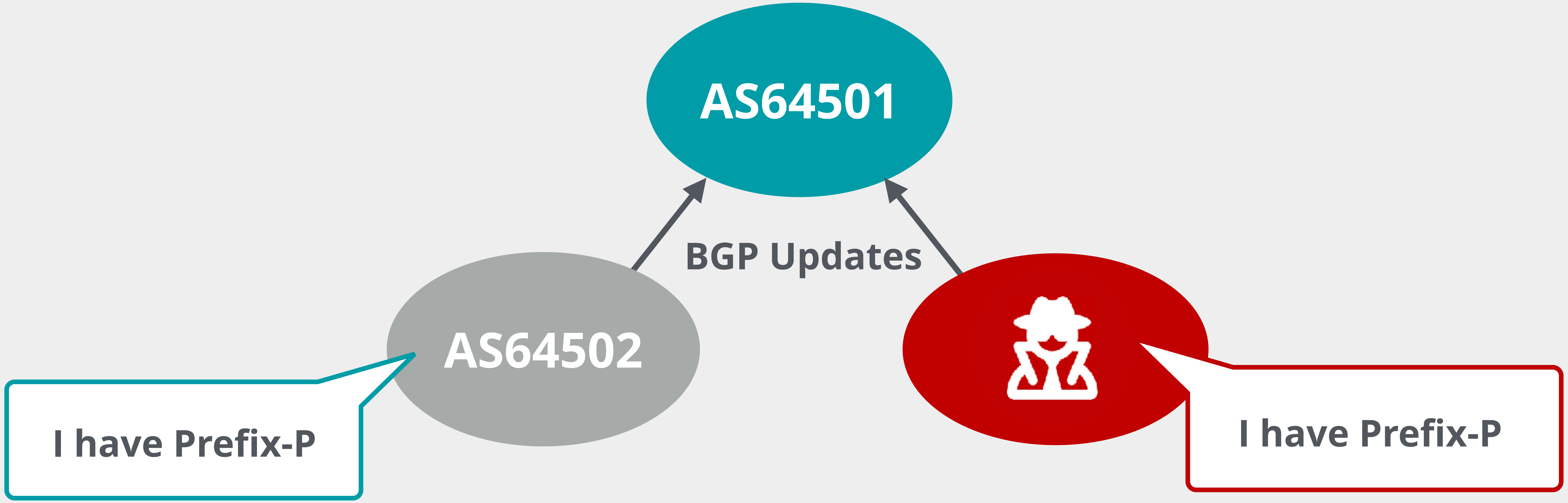
No Encryption or Authentication

- BGP **does not** have a built-in authentication mechanism
- BGP provides **no integrity** or **confidentiality**
- BGP messages do not use a freshness service and can be replayed



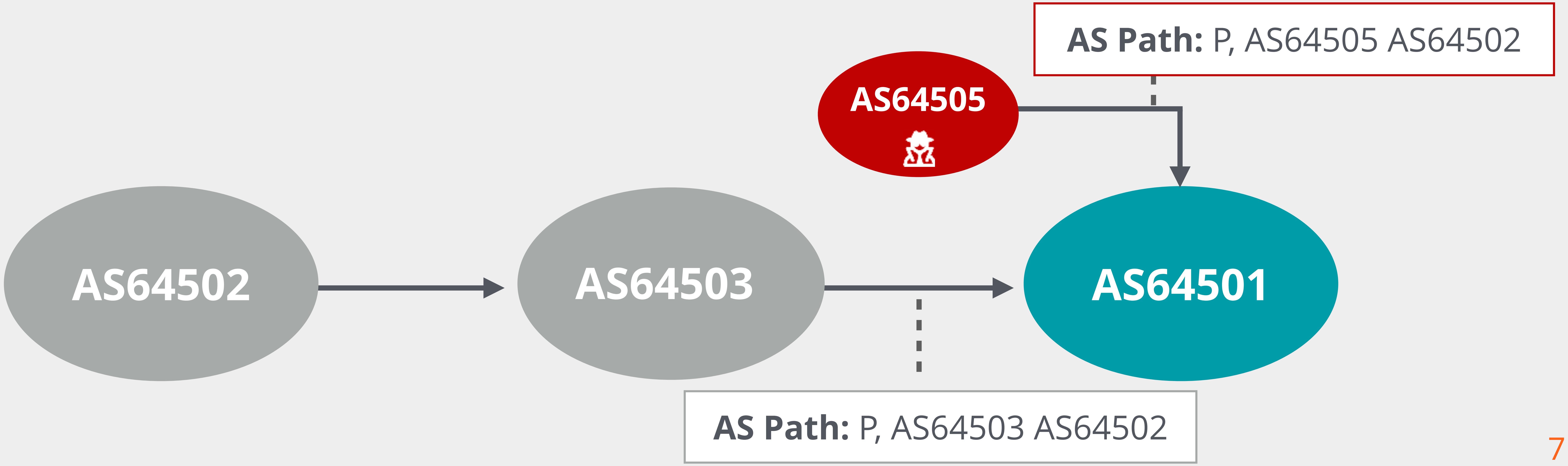
No Origin Validation

- BGP does not have a validity check for propagated routes
  - **Any AS can announce any prefix**



No Authentication of AS Path

- AS path attribute received in BGP update can not be validated
- Anyone can alter the path and prepend any ASN to the AS path

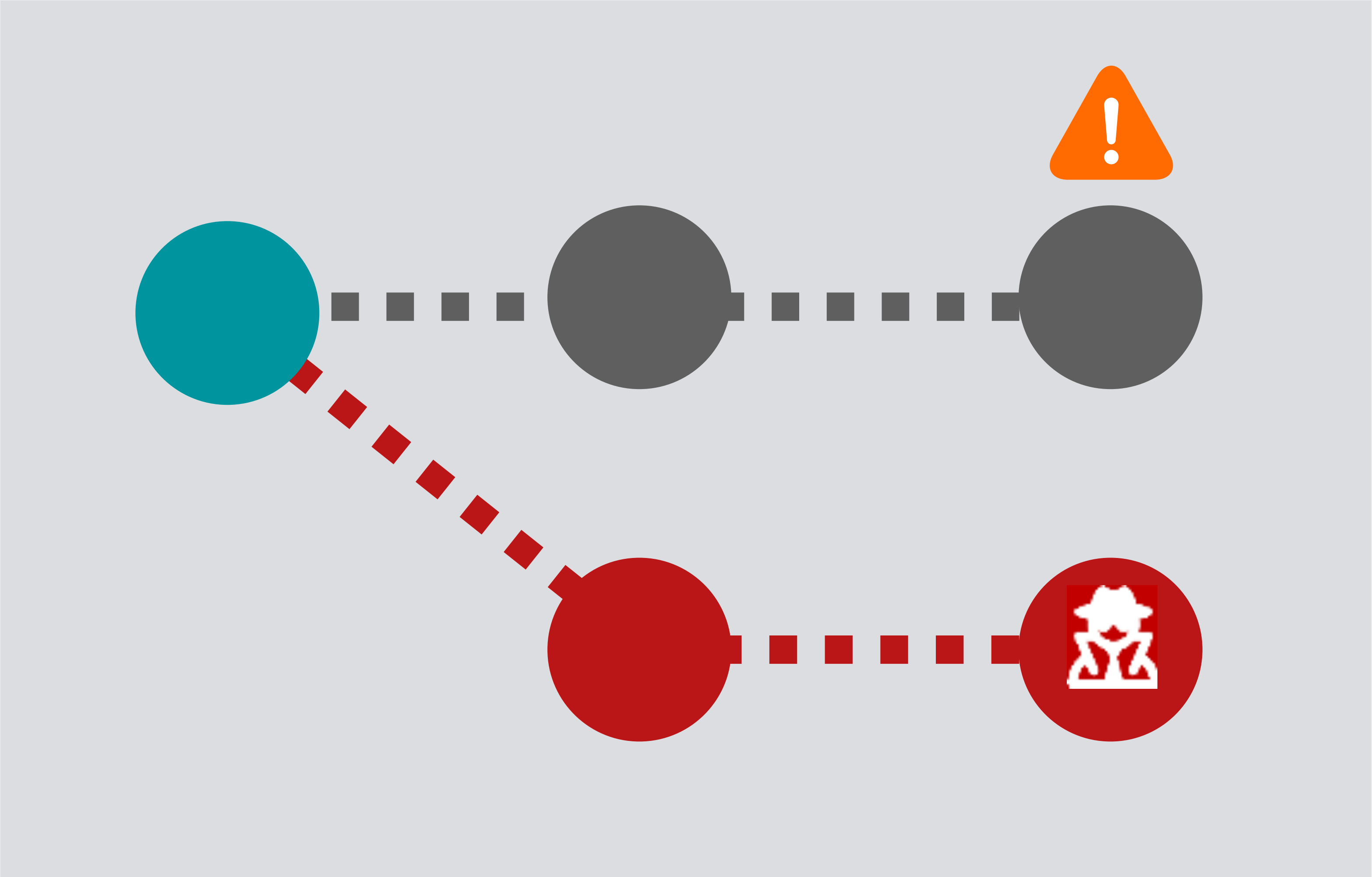

AS Path: P, AS64505 AS64502
AS64505
AS64502
AS64503
AS64501
AS Path: P, AS64503 AS64502

BGP Incidents

BGP Route Manipulation Attacks

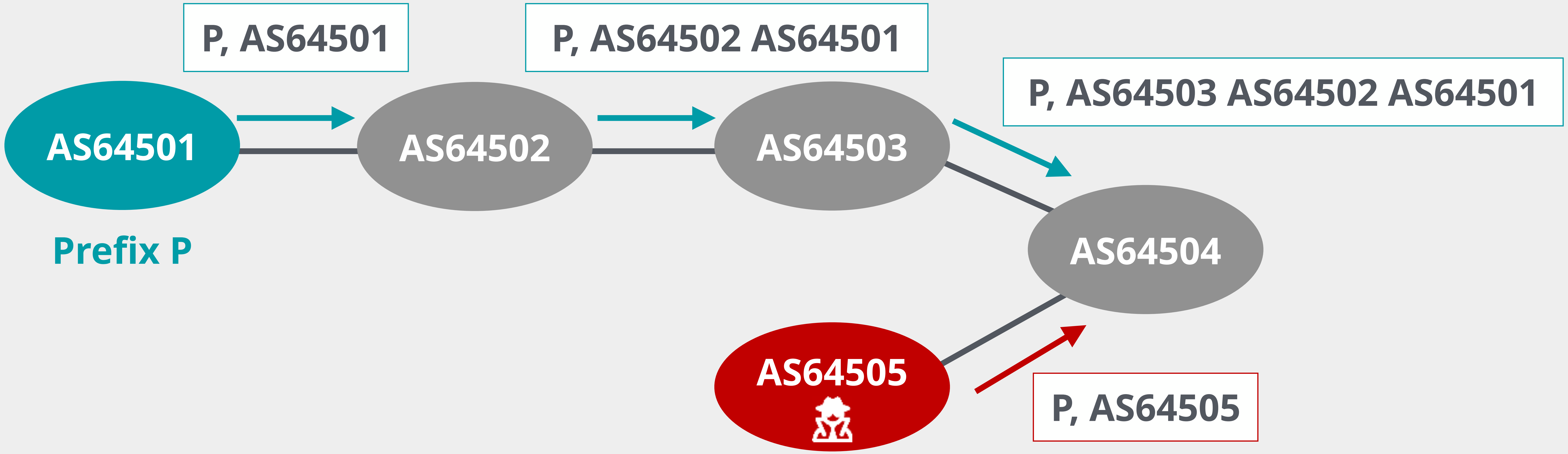
- Attacker can:
  - **Inject bogus routes** into BGP tables
  - **Reroute packets** based on their intentions
  - **Prevent traffic** from reaching the intended destination

- Can be classified as:
  - **BGP Origin Hijacks**
  - **BGP Path Hijacks**
  - **BGP Route Leaks**



BGP Origin Hijack

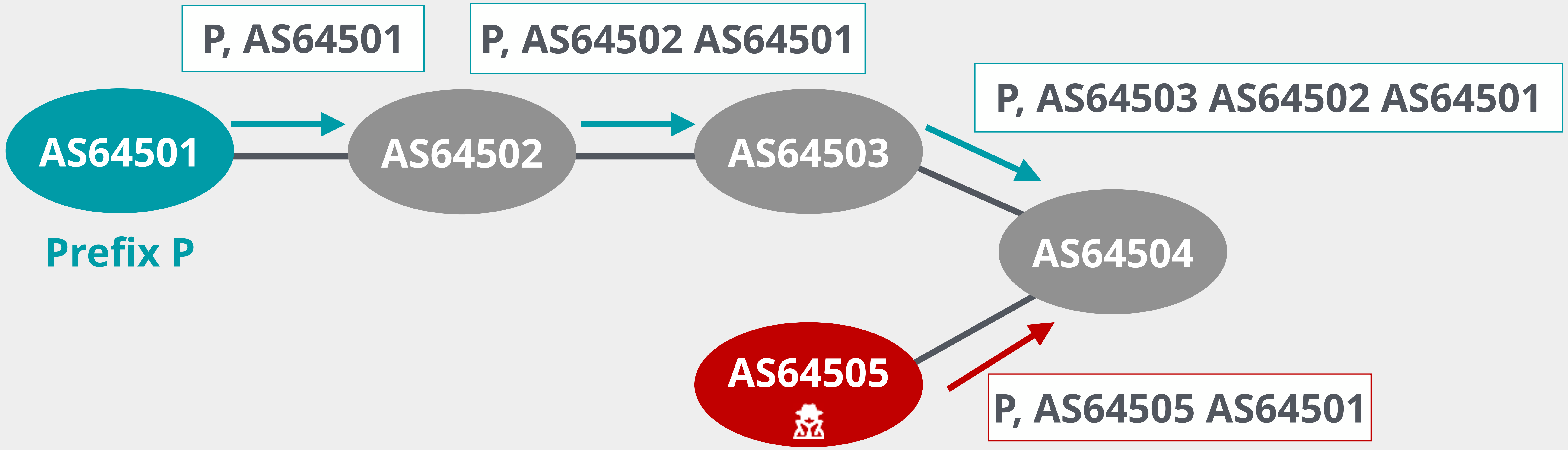
- The hijacking AS:
  - Abuses mutual trust between ASes
  - Originates a prefix **that it is not authorised to originate**
- Difficult to say whether it is an accident or an attack
- Traffic lost or received by attacker (eavesdrop)



ROUTE MANIPULATION

BGP Path Hijack

- No verification of path attributes in received BGP updates
- Hijacker can modify the AS Path and **redirect traffic**
- **Traffic lost** or **eavesdropped/modified** (adds latency)



ROUTE MANIPULATION

BGP Route Leak

- Propagating of a route beyond its intended scope
- Defined in RFC 7908
- **Traffic lost** or **rerouted** (adds latency, capacity issues)

YouTube vs. Pakistan Telecom, 2008

- YouTube used /22
- Pakistan Telecom leaked Null route /24
- **More specific prefix** won, YouTube fought back
- Eventually, the hijack stopped

YouTube Hijacking: A RIPE NCC RIS case study

BGP Incidents in Q1 2025

BGP route leaking ASes	Q1 2025	BGP hijacking ASes
1 899	January	8 968
1 921	February	8 063
1 883	March	8 490

Source:

https://blog.qrator.net/en/q1-2025-ddos-bots-and-bgp-incidents-statistics-and_211

Internet Routing Registries

First attempt to secure the routing

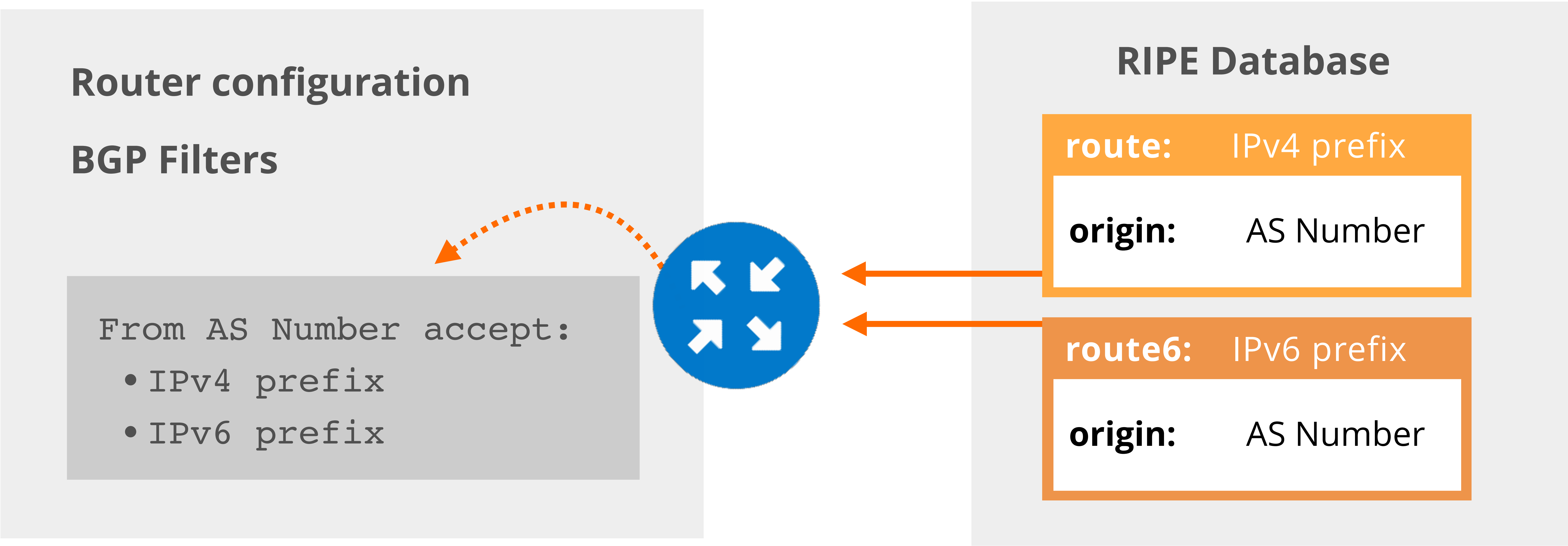
Internet Routing Registry

- Composed by many databases:
  - RIPE NCC, APNIC, RADB, JPIRR, Level3, NTTCom, etc.
- Uses **Whois protocol** and **RPSL language**
- Their information can be used to:
  - Automation of **creating BGP filters**
  - Provide global view of routing policies
  - Network troubleshooting

Source: **http://www.irr.net**

ROUTE(6) objects in the IRR

- Contains routing information for IPv4/IPv6 address space
- **Specifies from which AS a certain prefix may be originated**
- Used for creating BGP filters



Router configuration

BGP Filters

```
From AS Number accept:
 • IPv4 prefix
 • IPv6 prefix
```

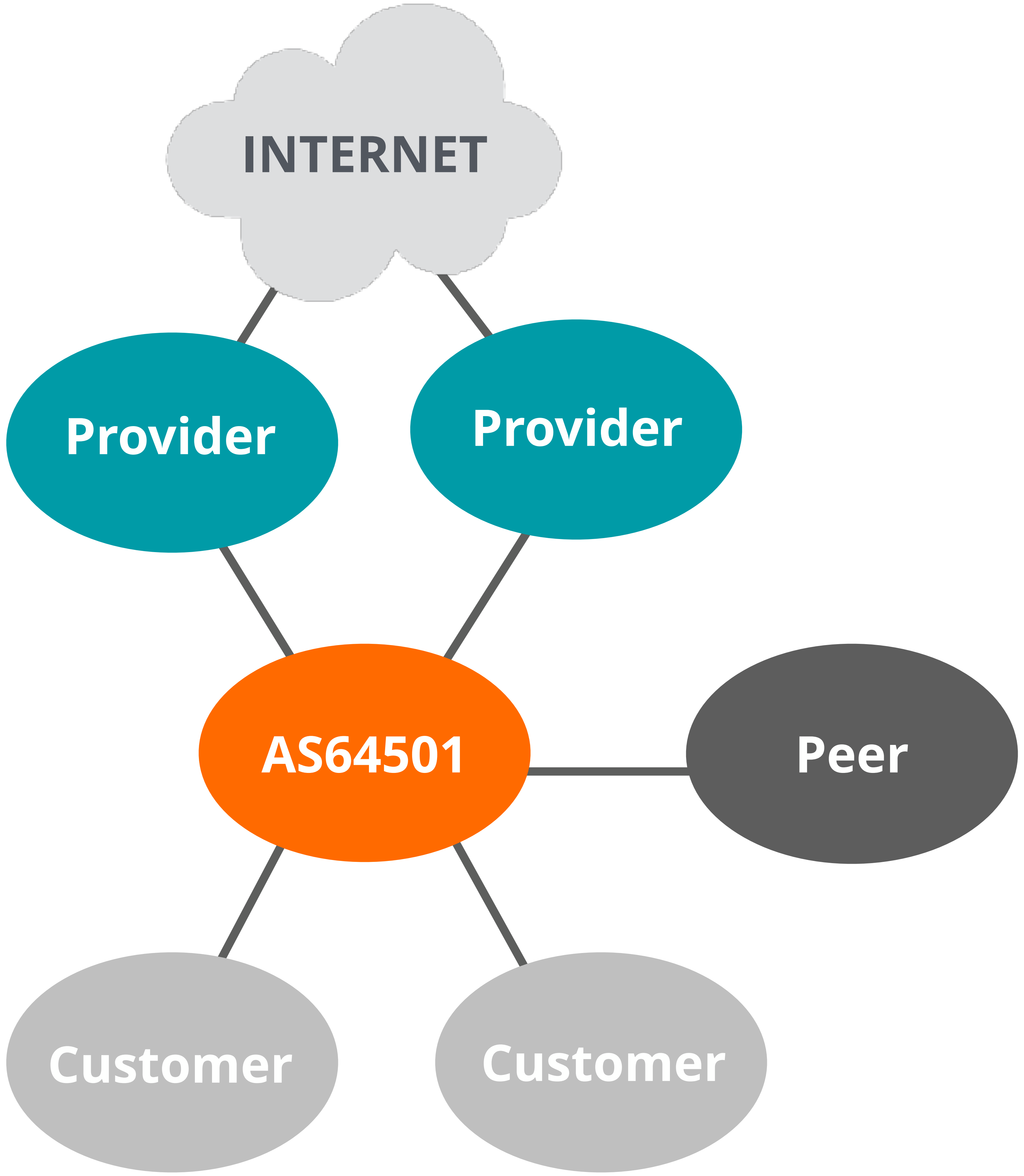
RIPE Database

route: IPv4 prefix
origin: AS Number

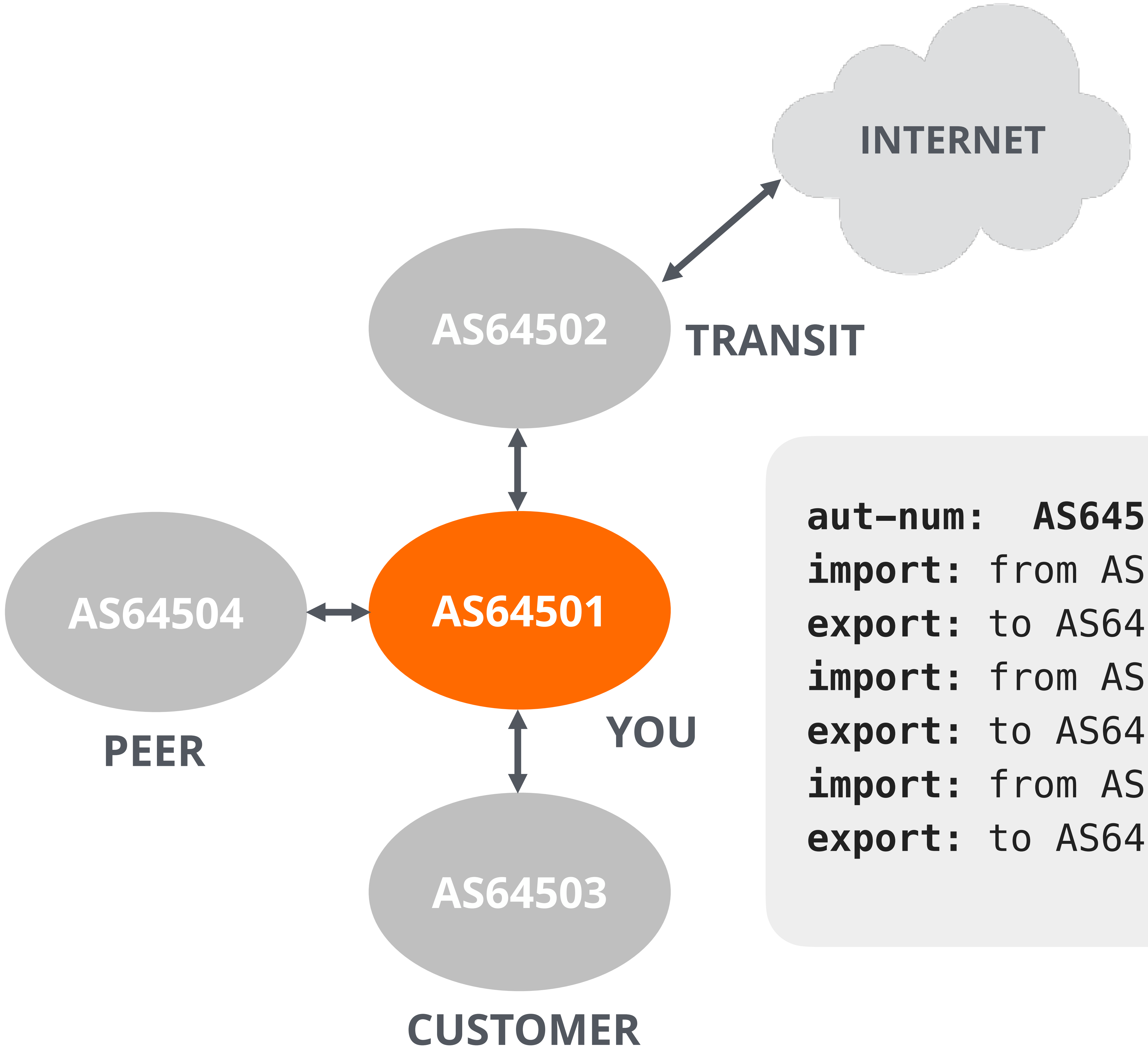
route6: IPv6 prefix
origin: AS Number

BGP Routing Policy

- **Who are your BGP peers? Which ASes do you peer with?**
- **What is your BGP relationship with them?**
  - Customer, Provider, Peer
- **Which routing decisions have you made?**
  - Which prefixes to accept
  - Which prefixes to announce
  - Which prefixes will be preferred in case of multiple routes



Routing Policy Example



```
aut-num:  AS64501
import: from AS64502 accept ANY
export: to AS64502 announce AS64501 AS64503
import: from AS64503 accept AS64503
export: to AS64503 announce ANY
import: from AS64504 accept AS64504
export: to AS64504 announce AS64501 AS64503
```

The Limits of the IRR system

- Multiple databases, **stale data**, limited **holdership checks**
- It is still widely used

You download **plaintext** data from **random sources** on the Internet and put them into the configuration of your routers to **make the Internet more secure.** What could possibly go wrong?

Resource Public Key Infrastructure

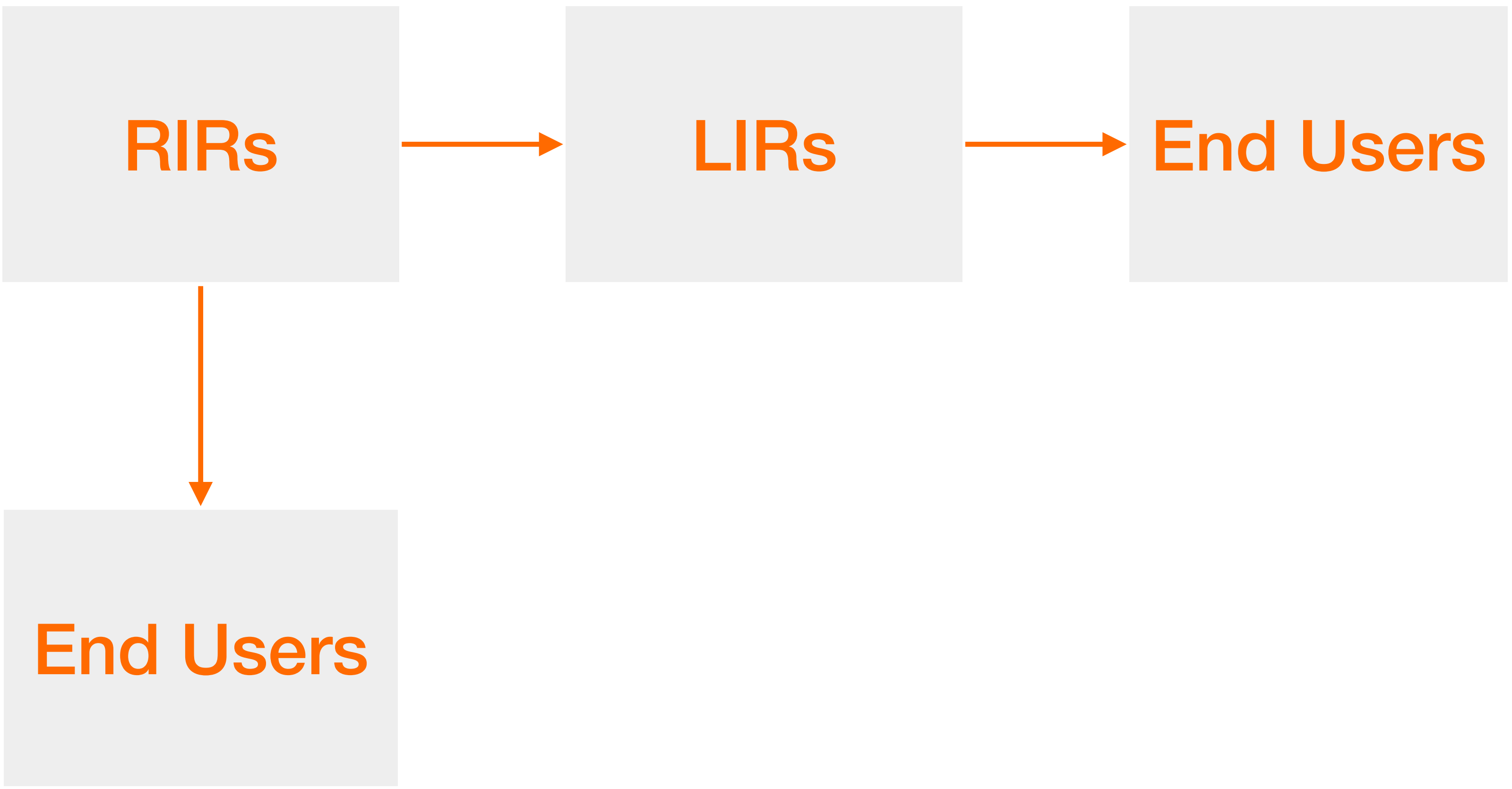
Putting cryptography into Internet registries

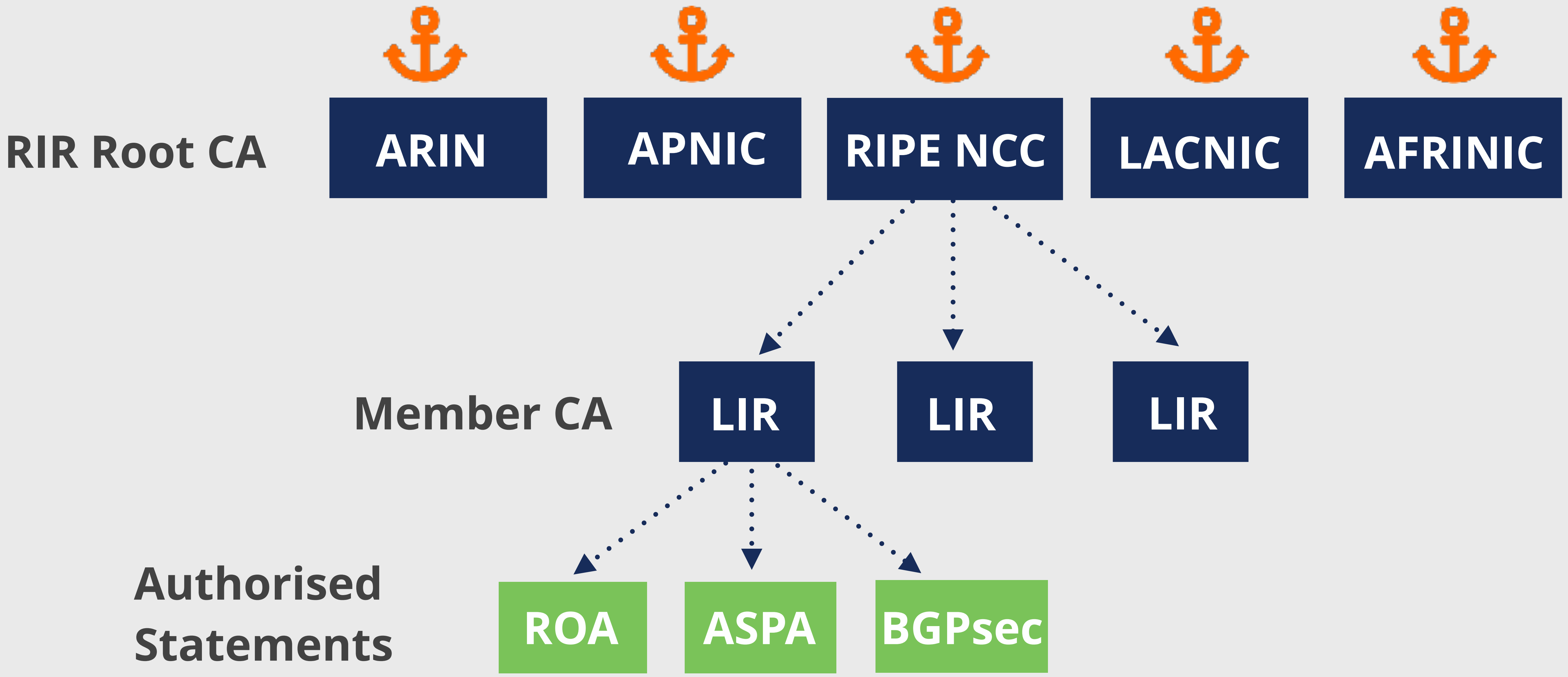
What is RPKI?

- A security framework for the Internet
- **Verifies the association between resource holders and their resources**
  - Attaches digital **certificate** to IP addresses and AS numbers
  - Does not contain other information about the holders (no PII)
- Growing list of use cases:
  - **BGP Origin Validation** (BGP OV)
  - **Autonomous System Provider Authorization** (ASPA)
  - BGPsec

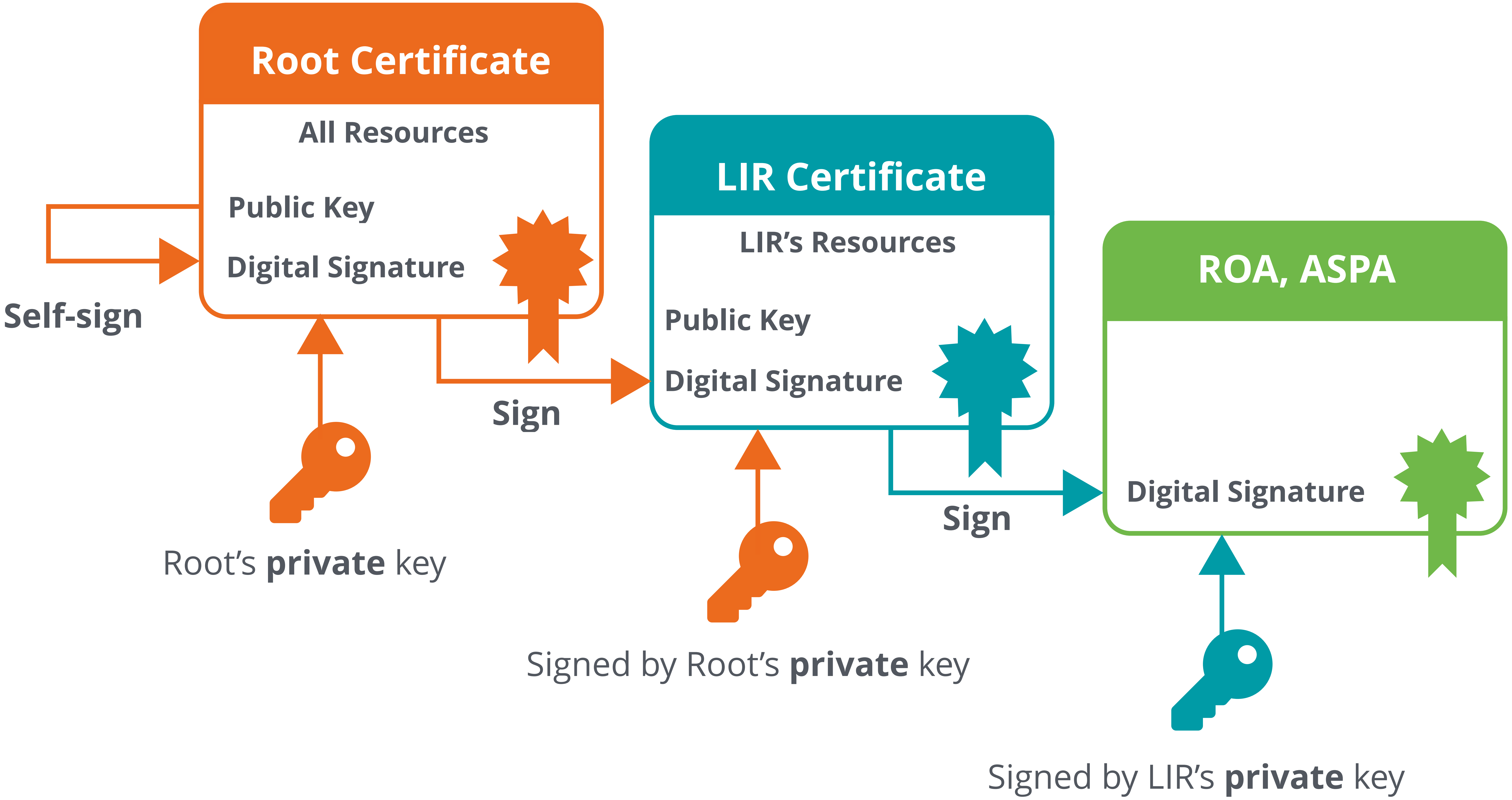
Trust in RPKI

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





RPKI Chain of Trust



Root Certificate

All Resources

Public Key

Digital Signature

Self-sign

Root's **private** key

Sign

LIR Certificate

LIR's Resources

Public Key

Digital Signature

Signed by Root's **private** key

Sign

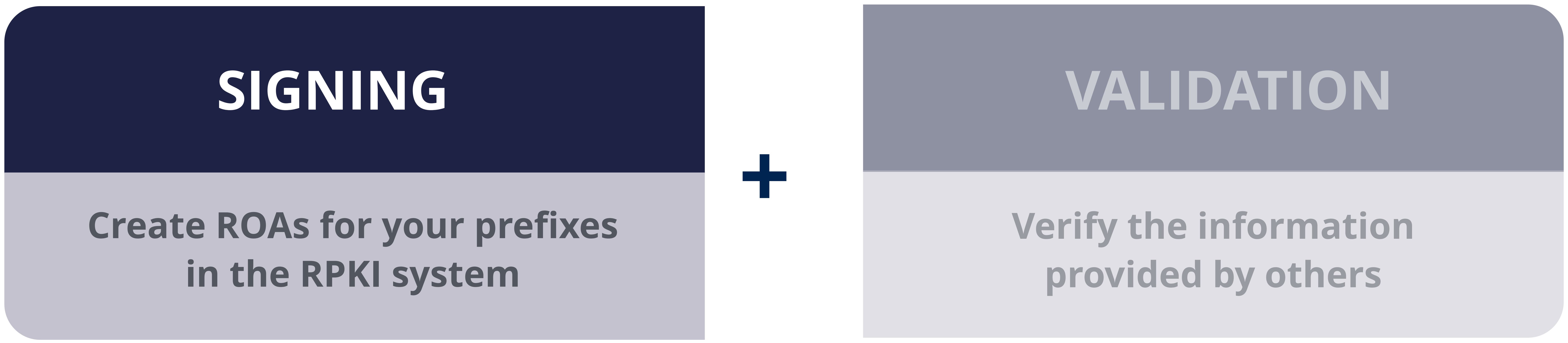
ROA, ASPA

Digital Signature

Signed by LIR's **private** key

Elements of RPKI Origin Validation

- The RPKI system consists of two parts:



SIGNING

Create ROAs for your prefixes in the RPKI system

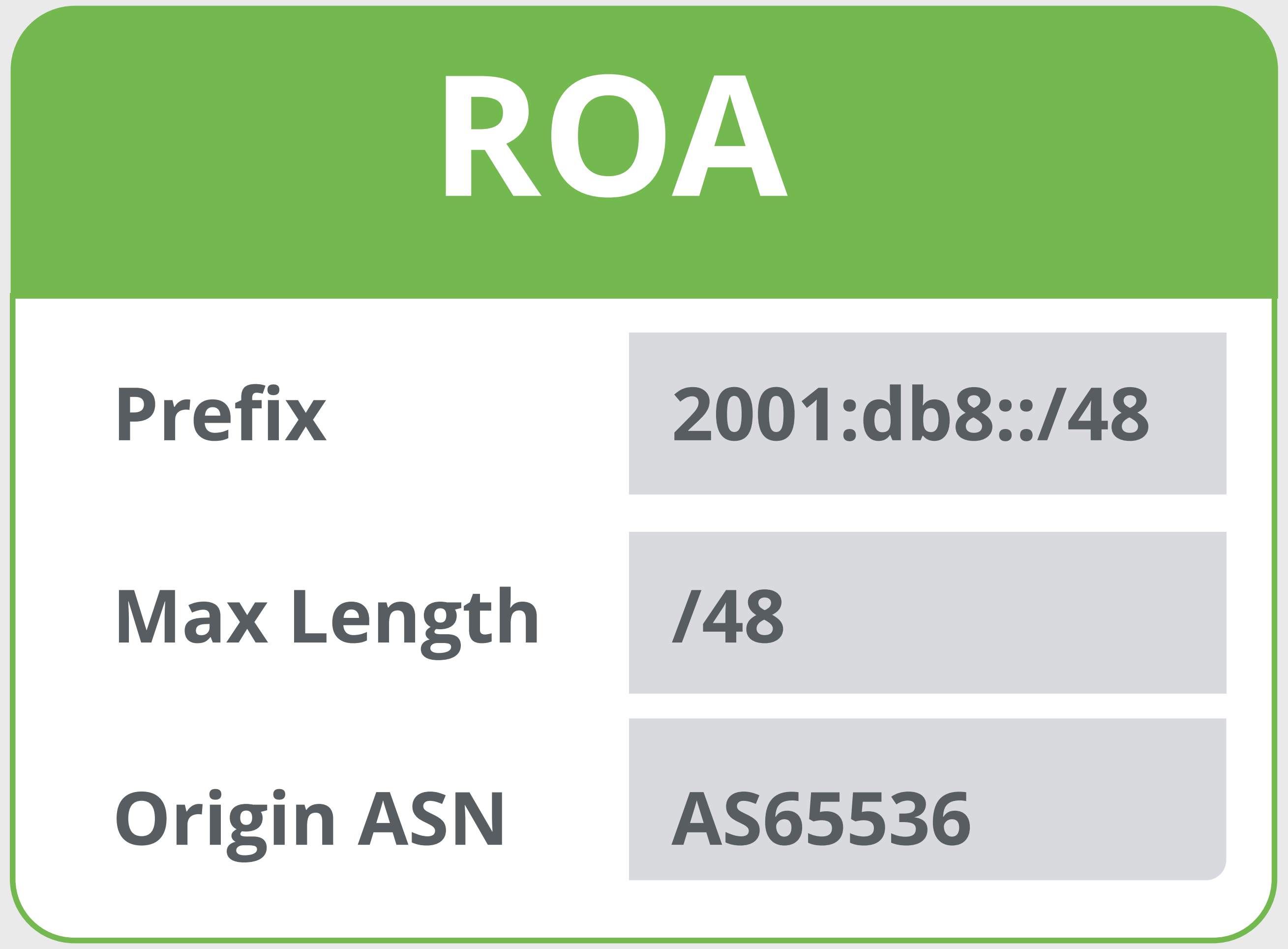
+

VALIDATION

Verify the information provided by others

What is Route Origin Authorization

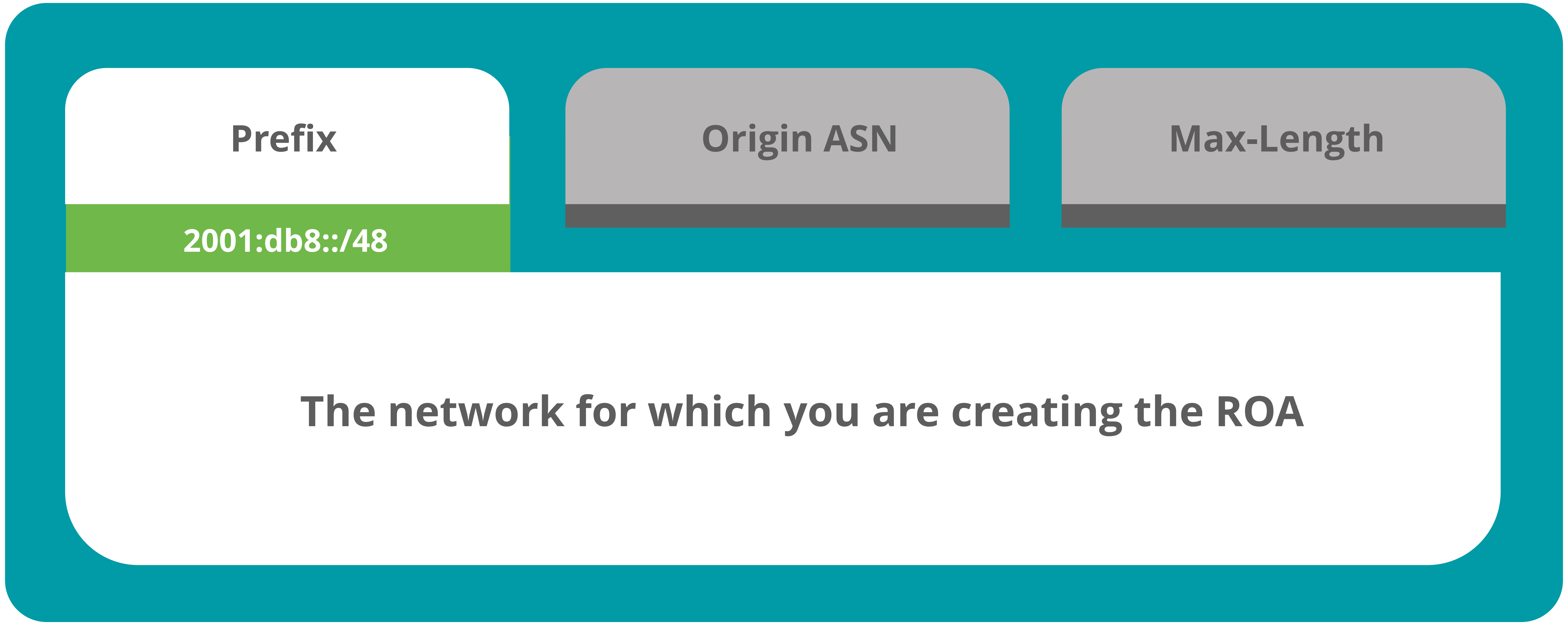
- An **authorised statement** from a resource holder
  - states that a certain prefix can be originated by a certain AS
- Contains a list of IP address prefixes and an AS number
- Multiple ROAs can exist for the same prefix
- ROAs can overlap



ROA

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

What is in a ROA?



Prefix

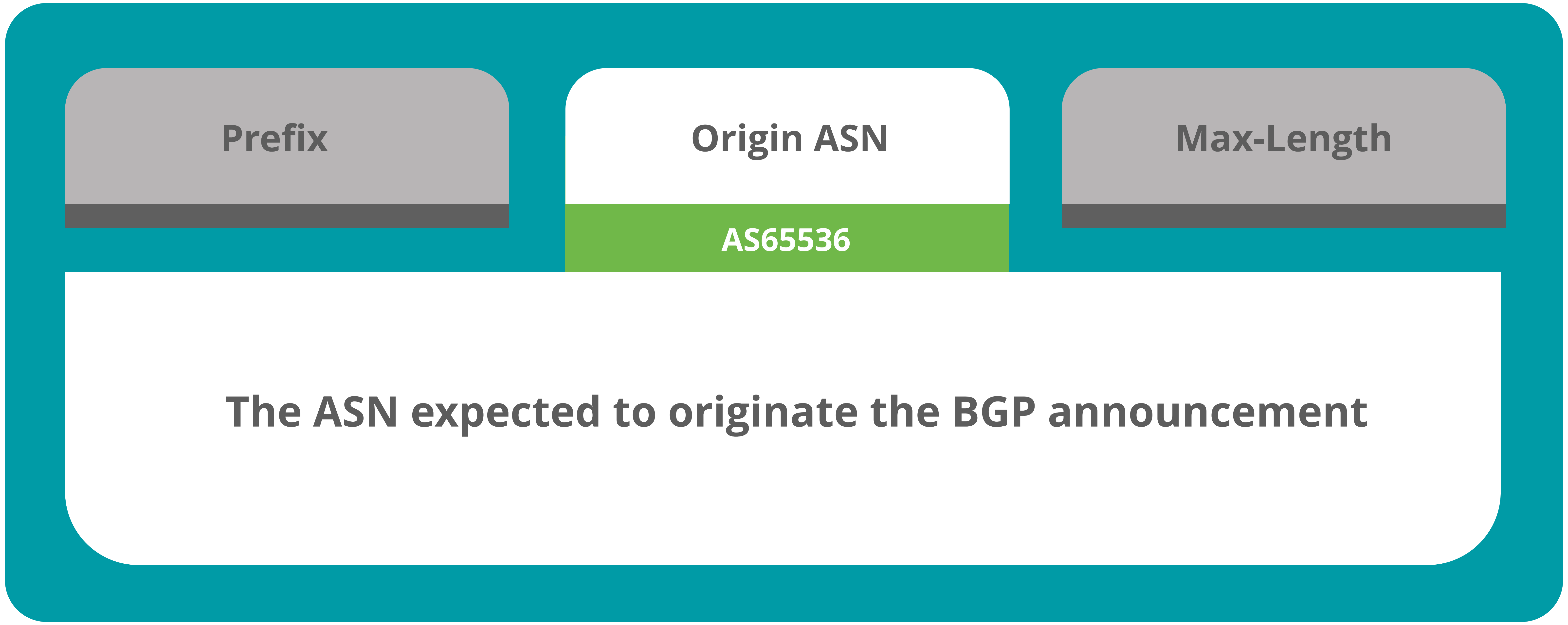
2001:db8::/48

Origin ASN

Max-Length

The network for which you are creating the ROA

What is in a ROA?



Prefix

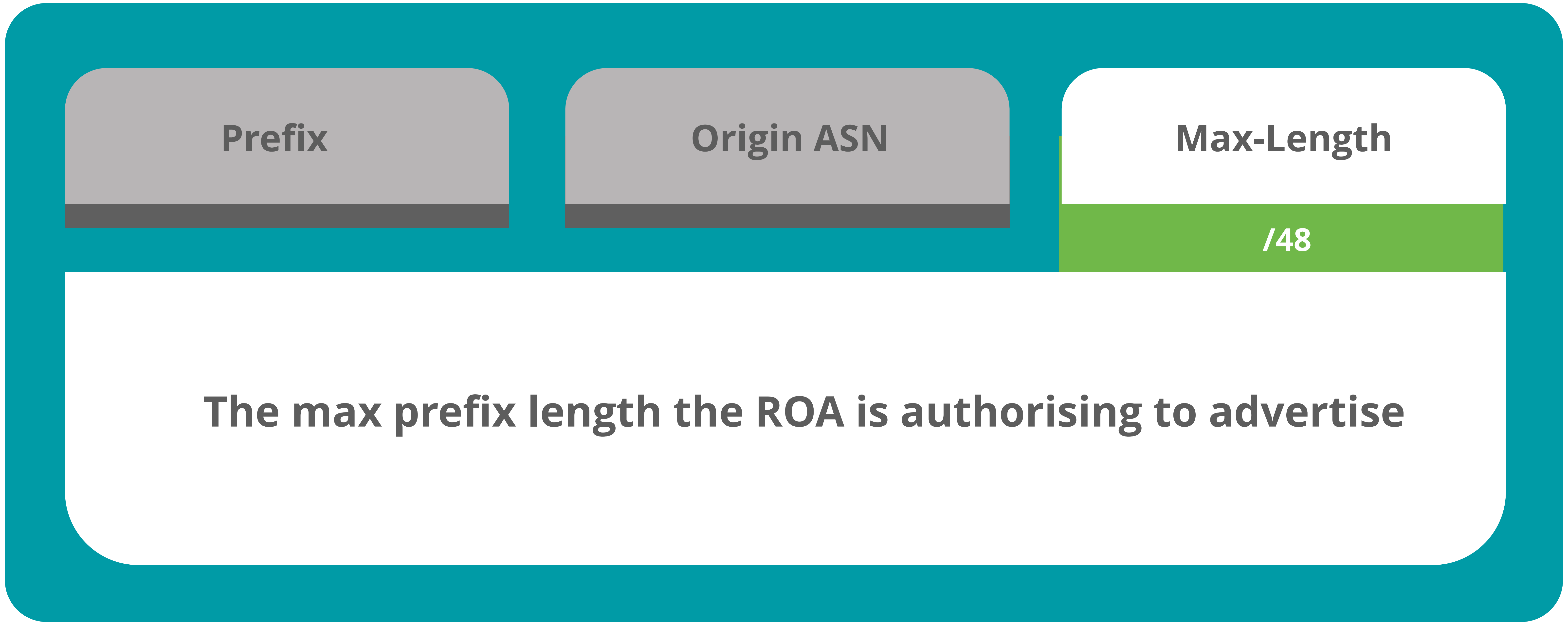
Origin ASN

Max-Length

AS65536

The ASN expected to originate the BGP announcement

What is in a ROA?



Prefix

Origin ASN

Max-Length

/48

The max prefix length the ROA is authorising to advertise

Max-Length

RIPE NCC (AS3333) has an IP address allocation

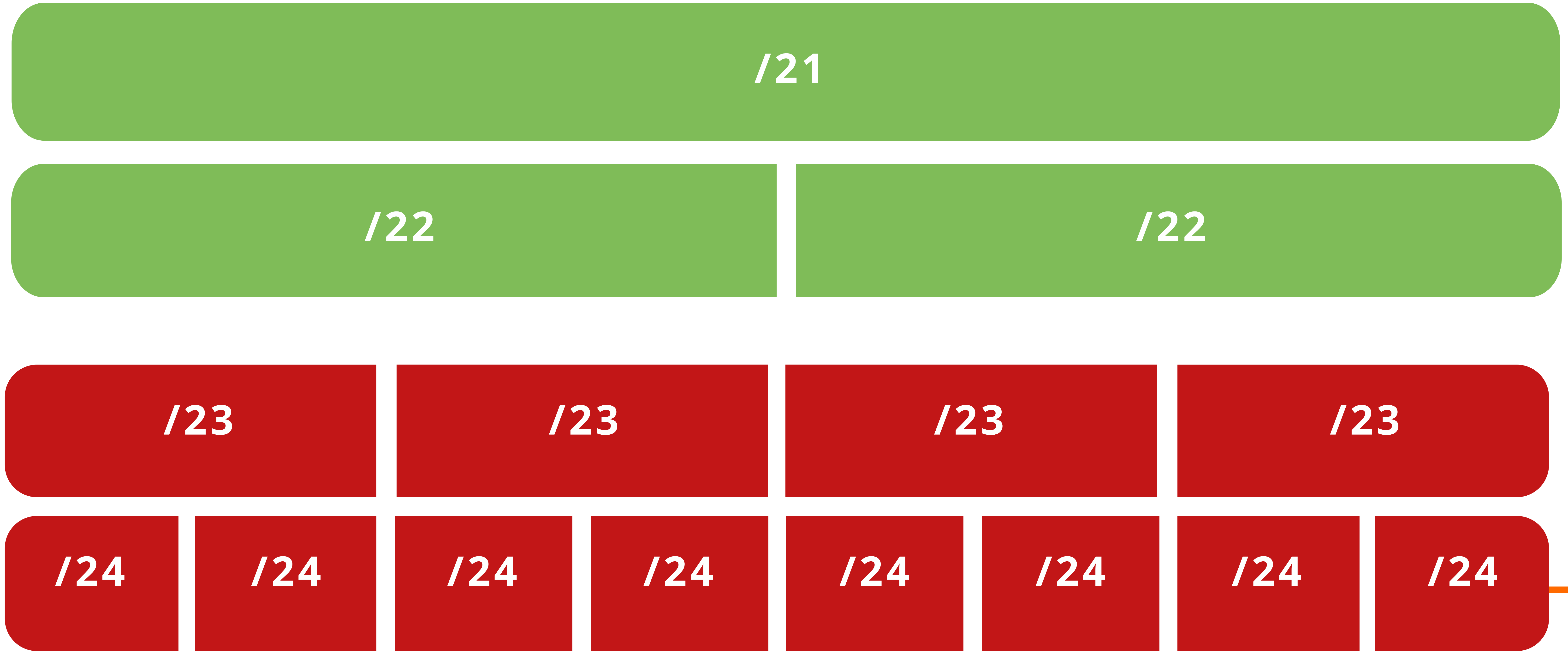
193.0.0.0/21

RIPE NCC creates this ROA

ROA

Prefix	193.0.0.0/21
Max Length	/22
Origin ASN	AS3333

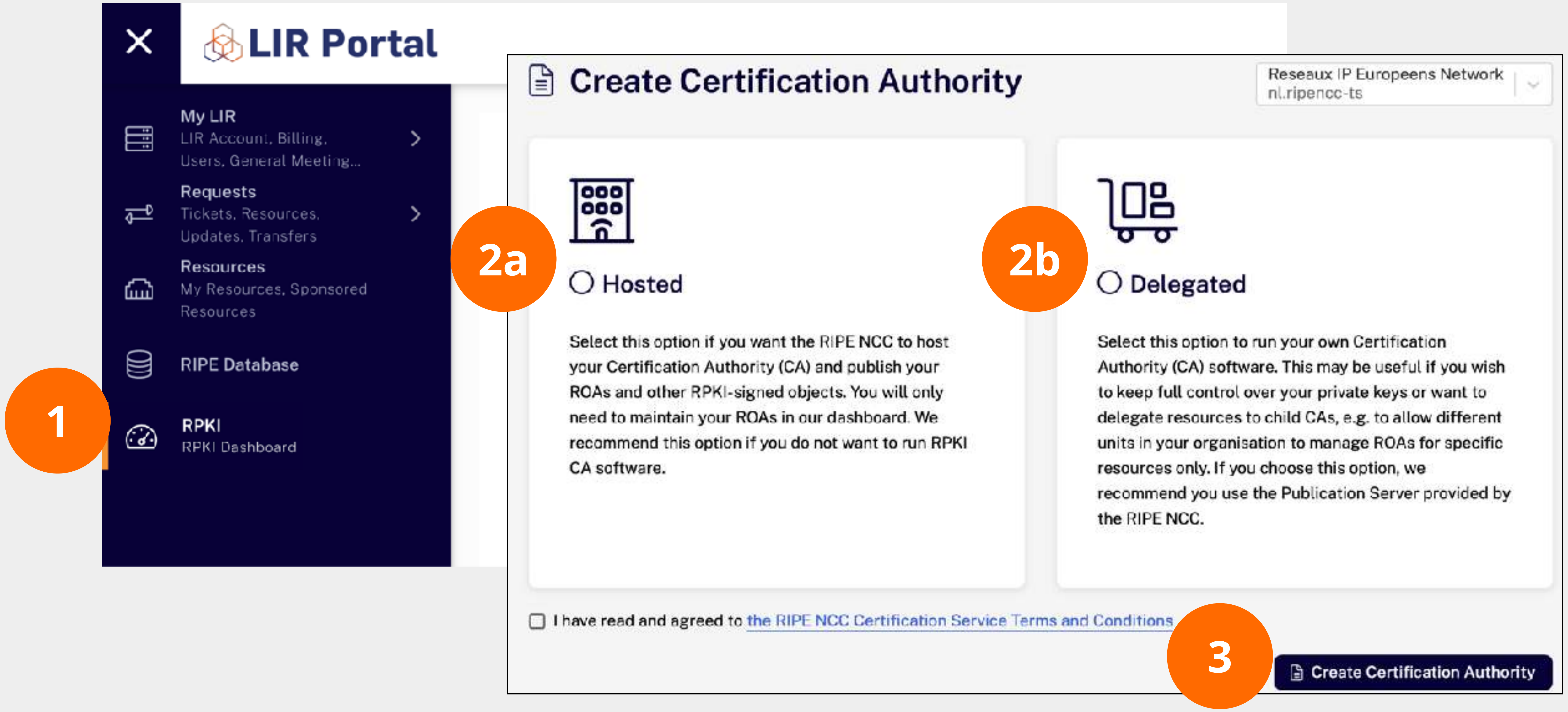
According to the ROA:



Any other more specific announcements are unauthorised by the ROA

Creating ROAs the easy way

- Login to the LIR Portal (my.ripe.net)
- Go to the RPKI Dashboard
- Choose the RPKI model you would like to use


LIR Portal
My LIR
LIR Account, Billing, Users, General Meeting...
Requests
Tickets, Resources, Updates, Transfers
Resources
My Resources, Sponsored Resources
RIPE Database
RPKI
RPKI Dashboard
1
Create Certification Authority
Reseaux IP Europeens Network
nl.ripencc-ts
2a
○ Hosted
2b
○ Delegated
3
Create Certification Authority

Select this option if you want the RIPE NCC to host your Certification Authority (CA) and publish your ROAs and other RPKI-signed objects. You will only need to maintain your ROAs in our dashboard. We recommend this option if you do not want to run RPKI CA software.

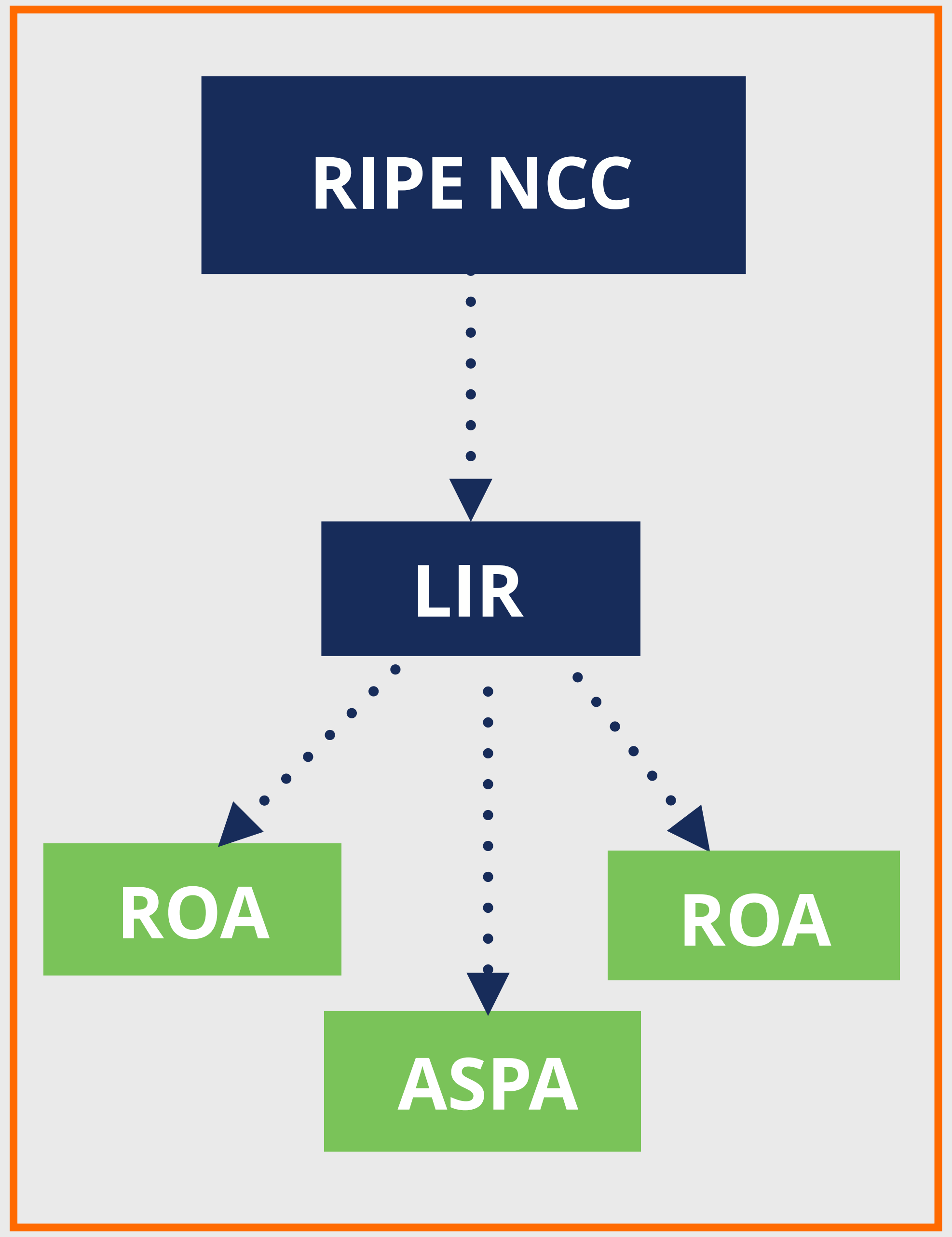
Select this option to run your own Certification Authority (CA) software. This may be useful if you wish to keep full control over your private keys or want to delegate resources to child CAs, e.g. to allow different units in your organisation to manage ROAs for specific resources only. If you choose this option, we recommend you use the Publication Server provided by the RIPE NCC.

□ I have read and agreed to the RIPE NCC Certification Service Terms and Conditions

Hosted RPKI

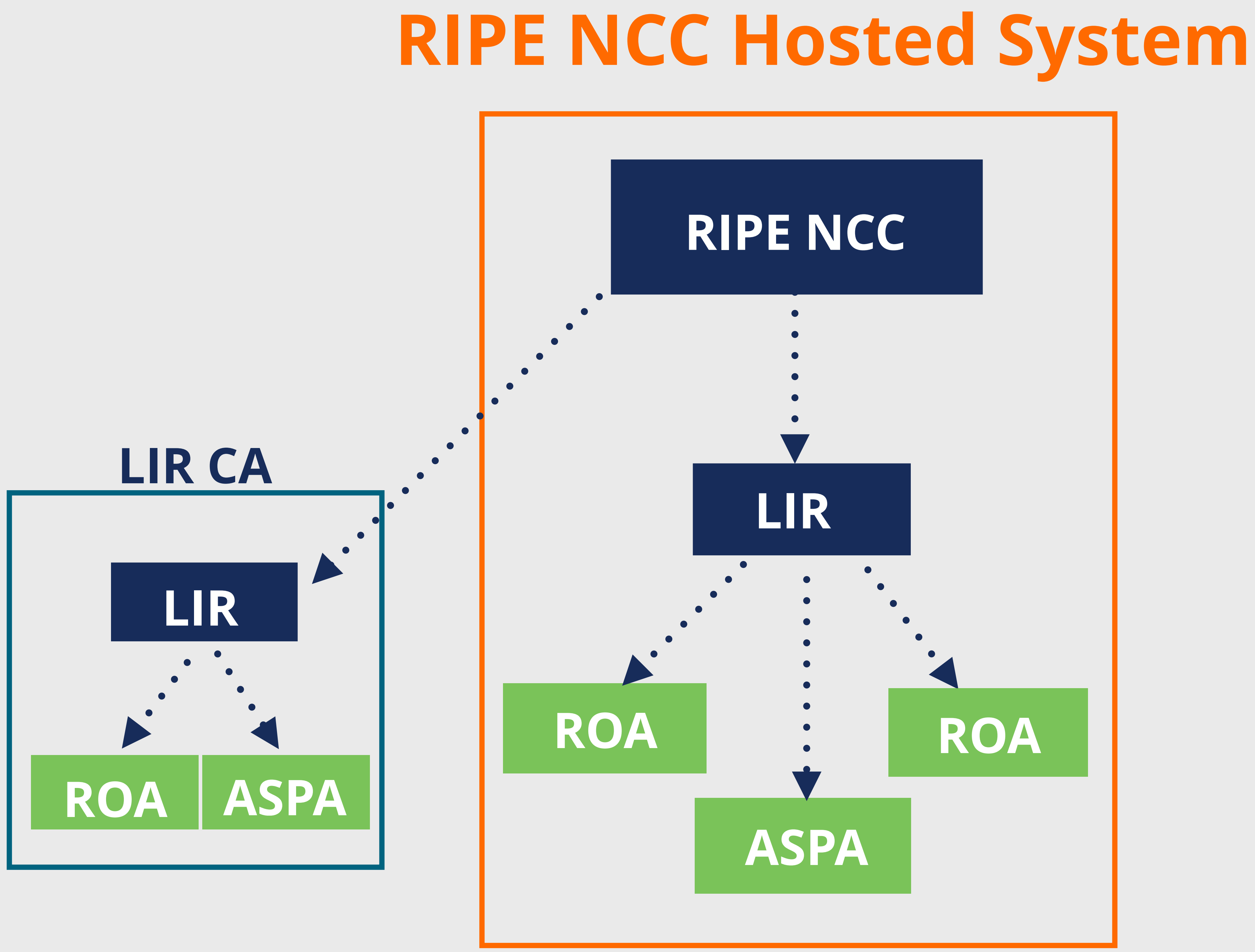
- ROAs and other objects are created and published using the **RIR's member portal**
- RIR hosts a CA for LIRs and signs all ROAs
- Automated **signing and key rollovers**
- Useful for most holders

RIPE NCC Hosted System



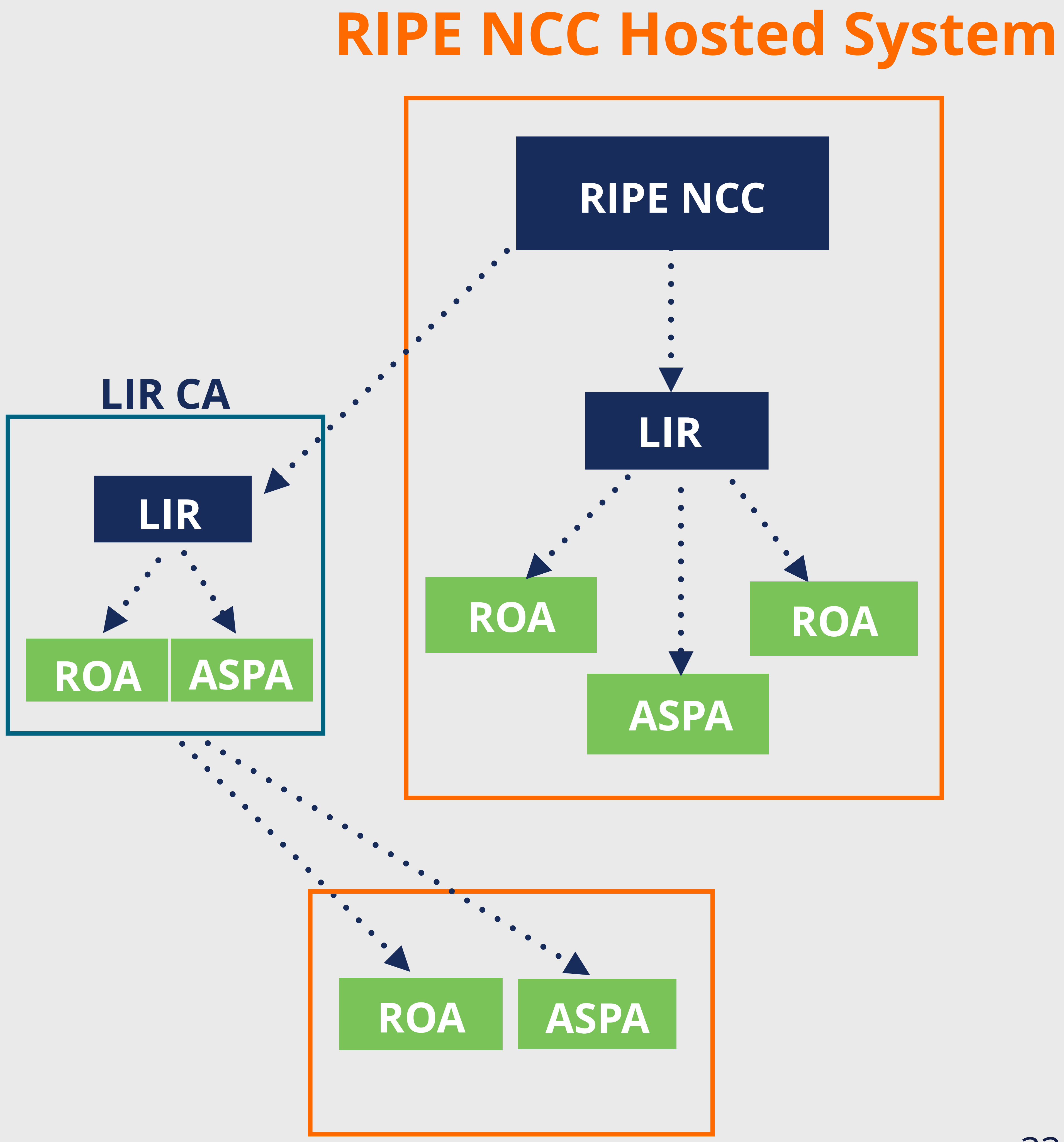
Delegated RPKI

- Each resource holder 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, ASPAs, BGPsec certificates
- Certificate Authority (CA) Software
  - **Krill** (NLnet Labs)
  - **rpkid** (Dragon Research Labs)



Hybrid RPKI

- In-between hosted and delegated RPKI
- The LIR:
  - Runs its own CA as a child of the RIR
  - Manages keys/key rollovers and object creation
  - RIR **publishes** LIR's objects in its repository
- Supported by APNIC, ARIN, RIPE NCC and NIRs
- A. k. a. "Publication in parent" or "**Publication as a service**"



RIPE NCC Hosted Solution

1
2
3
RPKI
Overview
Overview of your dashboard
ROAs
Manage your ROA objects
Alerts
Setup your alerts
History
View your CA history
Go to overview
Reseaux IP Europeens Network
nl.ripencc-ts
Search for ASN/prefix
Create ROA
Create ROA
Create 2 ROAs

BGP Announcements and ROAs

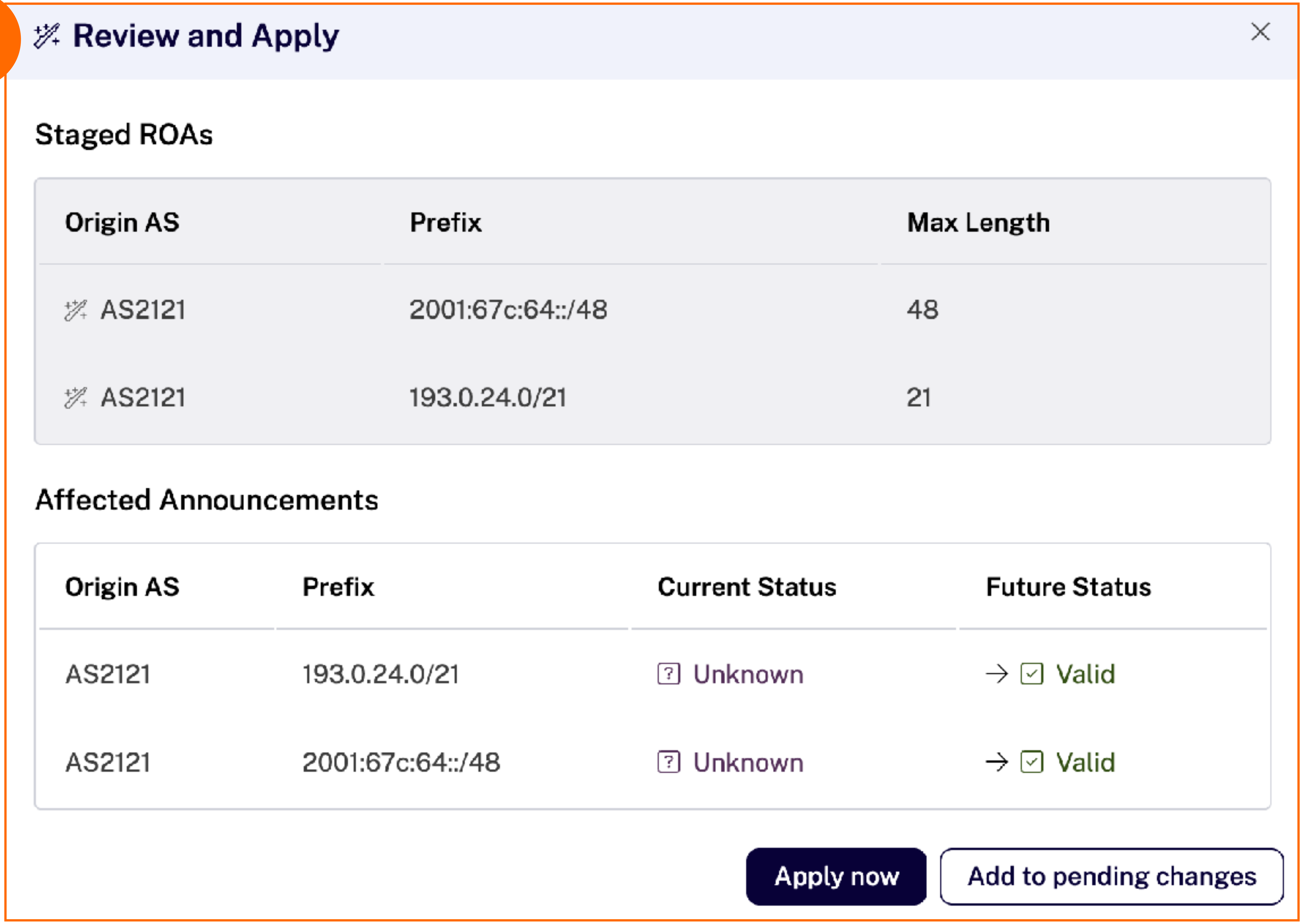
BGP Announcements: 2 | ROAs: 0 | Pending Changes: 0

Show status: ✕ Invalid ✕ Unknown ✕ Valid

	Origin AS	Prefix	Status
☑	AS2121	193.0.24.0/21	Unknown
☑	AS2121	2001:67c:64::/48	Unknown

RIPE NCC Hosted Solution

4



Review and Apply

Staged ROAs

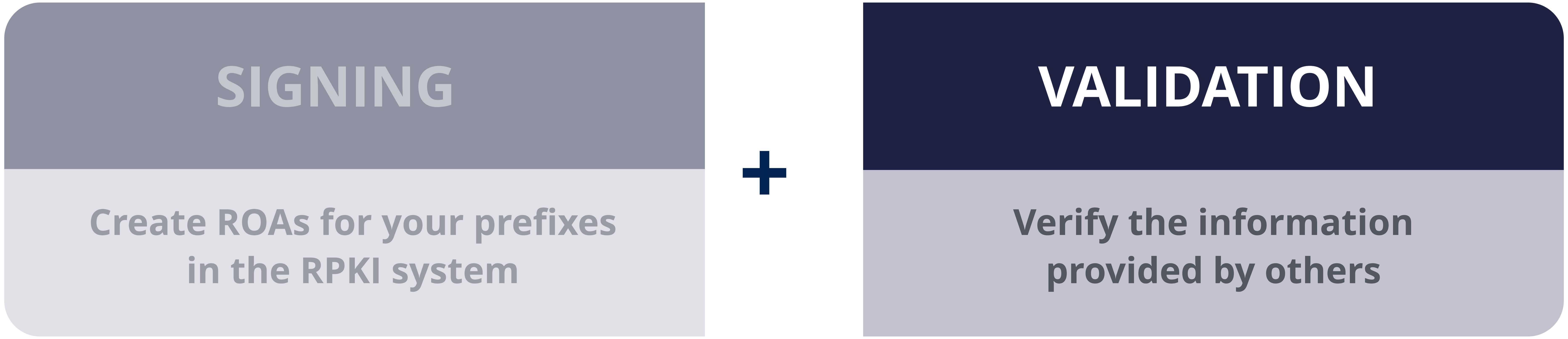
Origin AS	Prefix	Max Length
AS2121	2001:67c:64::/48	48
AS2121	193.0.24.0/21	21

Affected Announcements

Origin AS	Prefix	Current Status	Future Status
AS2121	193.0.24.0/21	? Unknown	→ ☑ Valid
AS2121	2001:67c:64::/48	? Unknown	→ ☑ Valid

Elements of RPKI

- The RPKI system consists of two parts:



SIGNING

Create ROAs for your prefixes in the RPKI system

+

VALIDATION

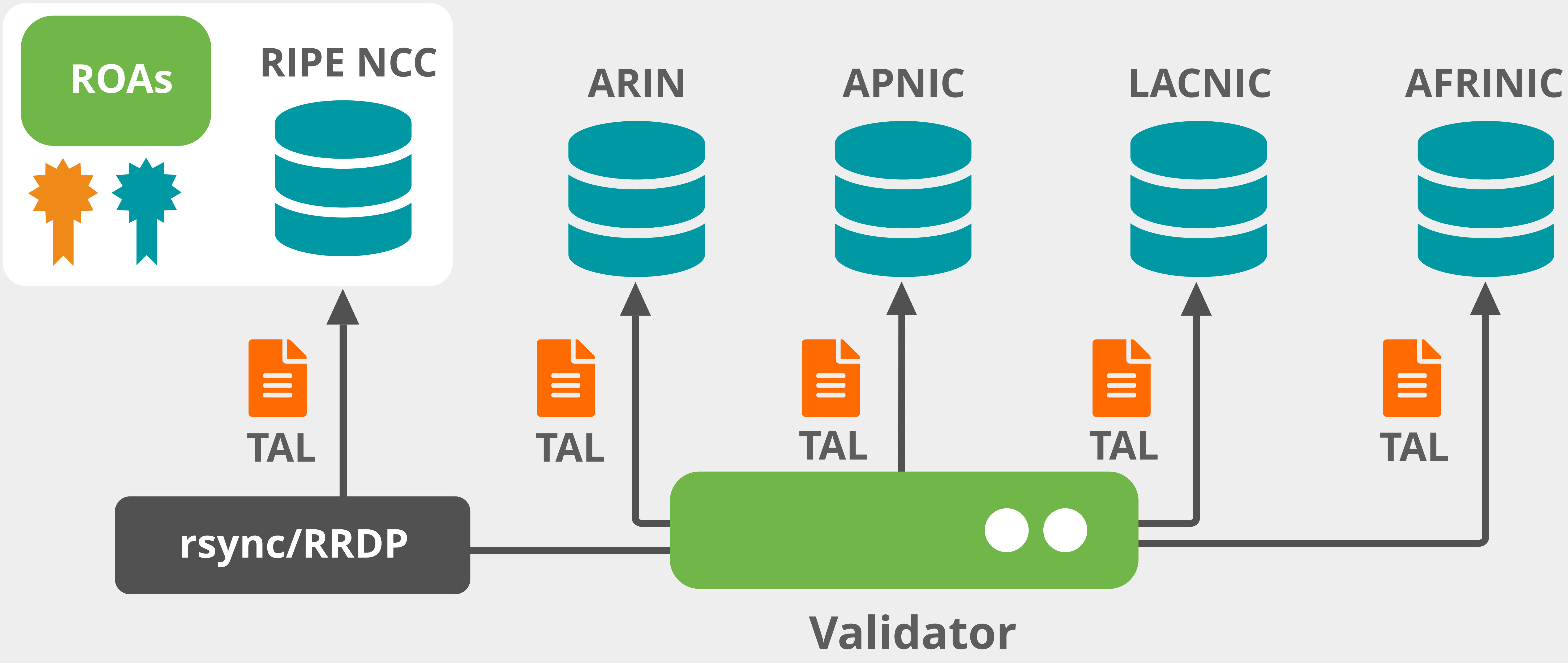
Verify the information provided by others

RPKI Validation

- Verifying the information provided by others
- First, **validate the RPKI data**
  - Install a validator software (relying party) locally in your network
  - Verify holdership through a public key and certificate infrastructure
- Then, **validate the** BGP announcements
  - This is done in a **BGP router** in your network
  - BGP Origin Validation (**BGP OV**) or Route Origin Validation (**ROV**) validates **origin AS**
  - Autonomous System Provider Authorization (**ASPA**) partially validates **AS path**

RPKI Validator

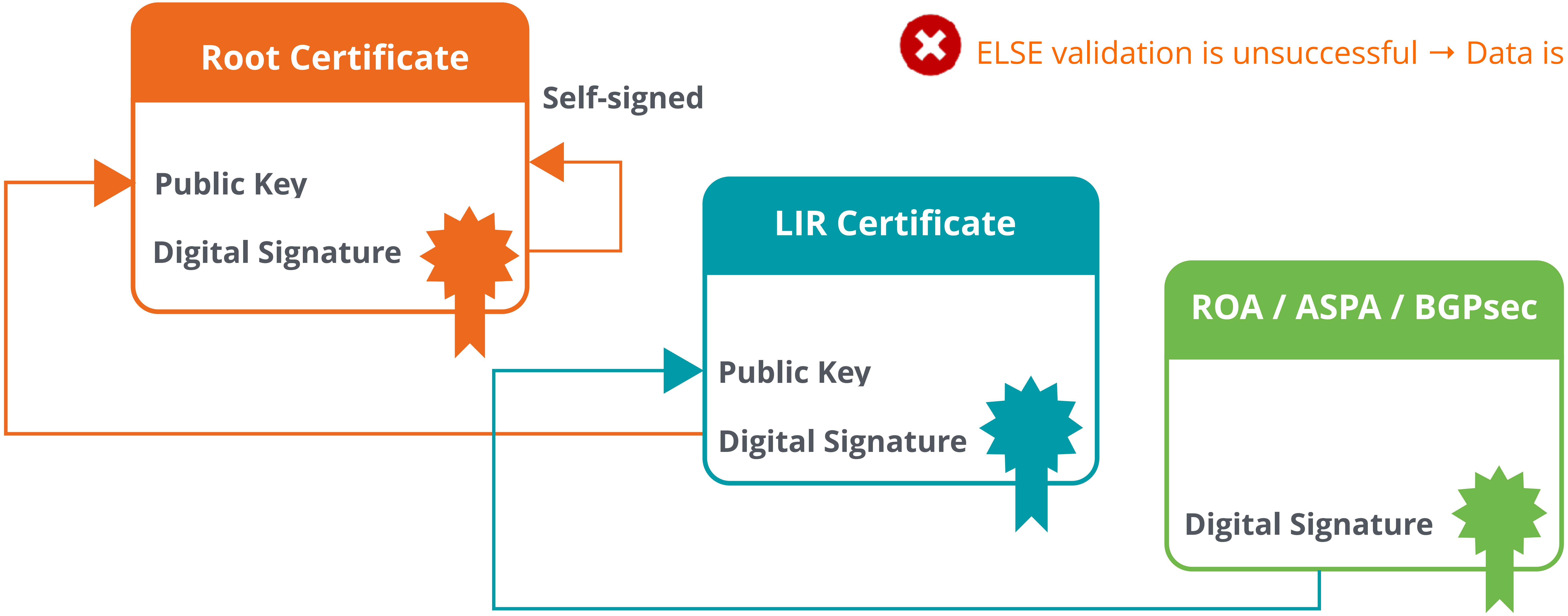
- Also known as **Relying Party (RP)** software
- Connects to RPKI repositories via **rsync** or **RRDP** protocol
- Uses information in **Trust Anchor Locators** (TAL) to connect to the repositories



ROA Validation Process

✓ IF chain is complete ➝ Data is **VALID**

✗ ELSE validation is unsuccessful ➝ Data is **INVALID**



RPKI Validator Options

- **Routinator**
  - Built by NLNet Labs
- **FORT**
  - Open source RPKI validator
- **rpki-client**
  - Integrated in OpenBSD

Links for RPKI Validators:

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

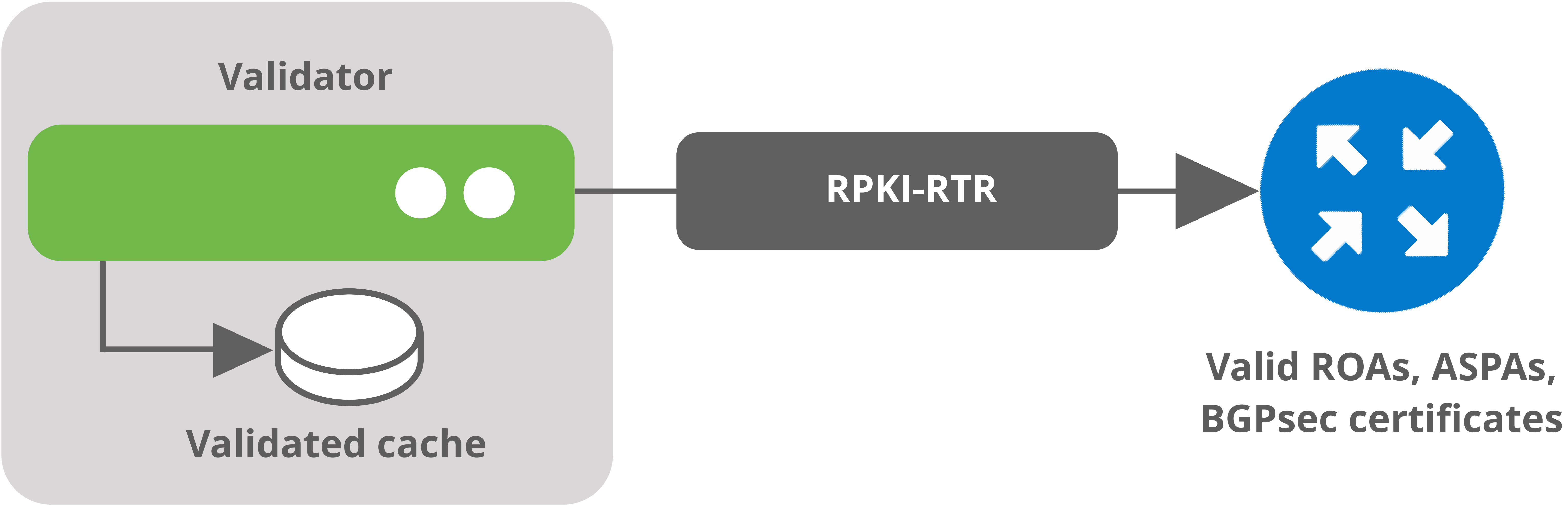
https://github.com/NICMx/FORT-validator/

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

More Information:

https://rpki.readthedocs.io

Only valid objects are sent to the router

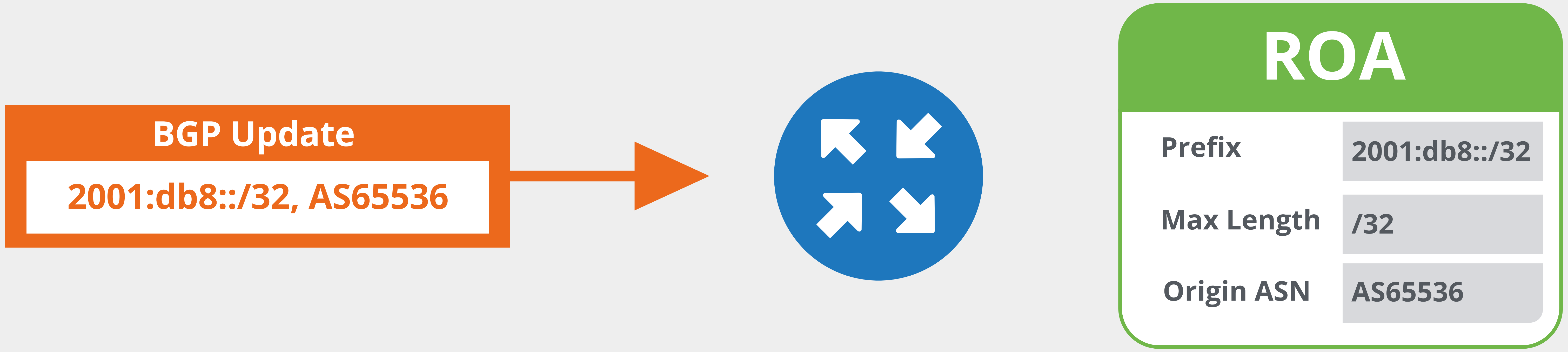


Router uses this information to make better routing decisions

✓ OR ✗

BGP Origin Validation (BGP OV)

- RPKI based route filtering
- BGP announcements are compared against the **valid** ROAs
  - **Origin ASN** and **max-length** must match
- Router decides the validation states of **routes**:
  - **Valid**, **Invalid** or **Not-Found**



BGP Update

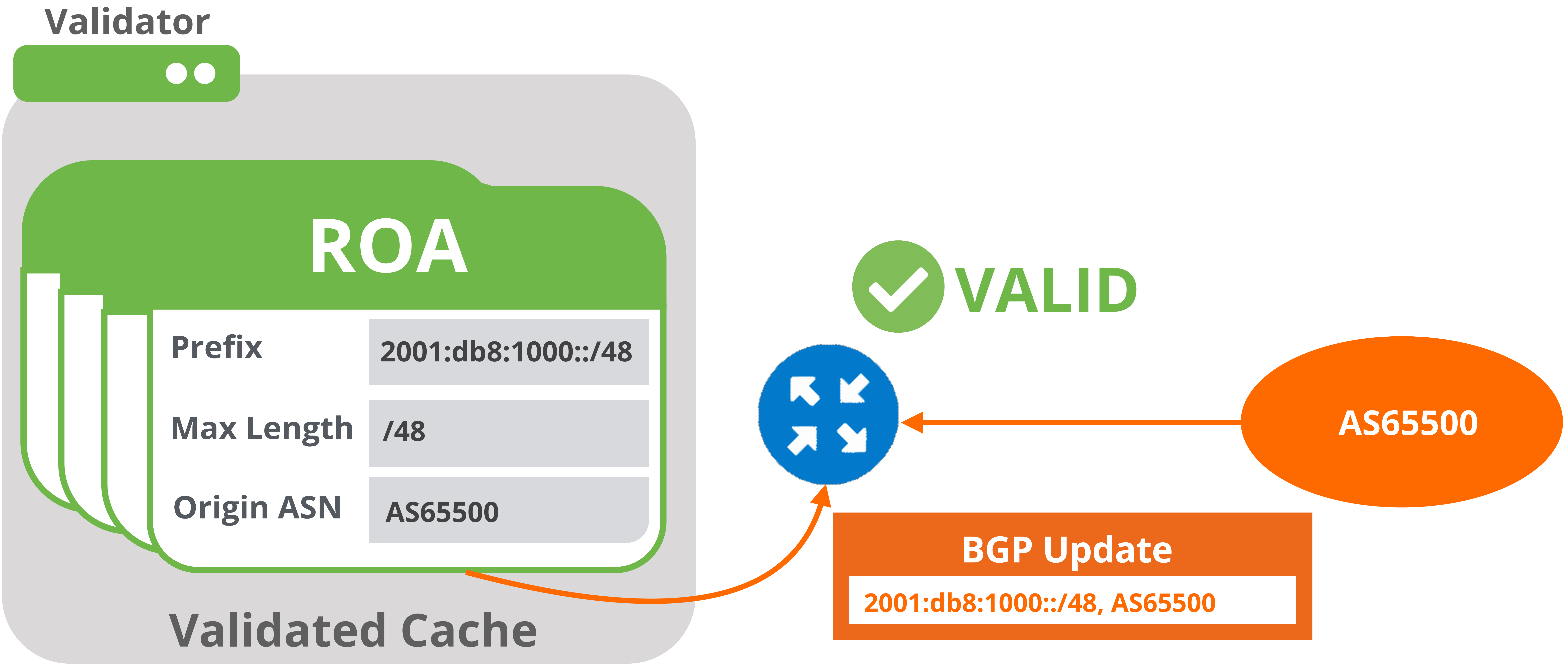
2001:db8::/32, AS65536

ROA

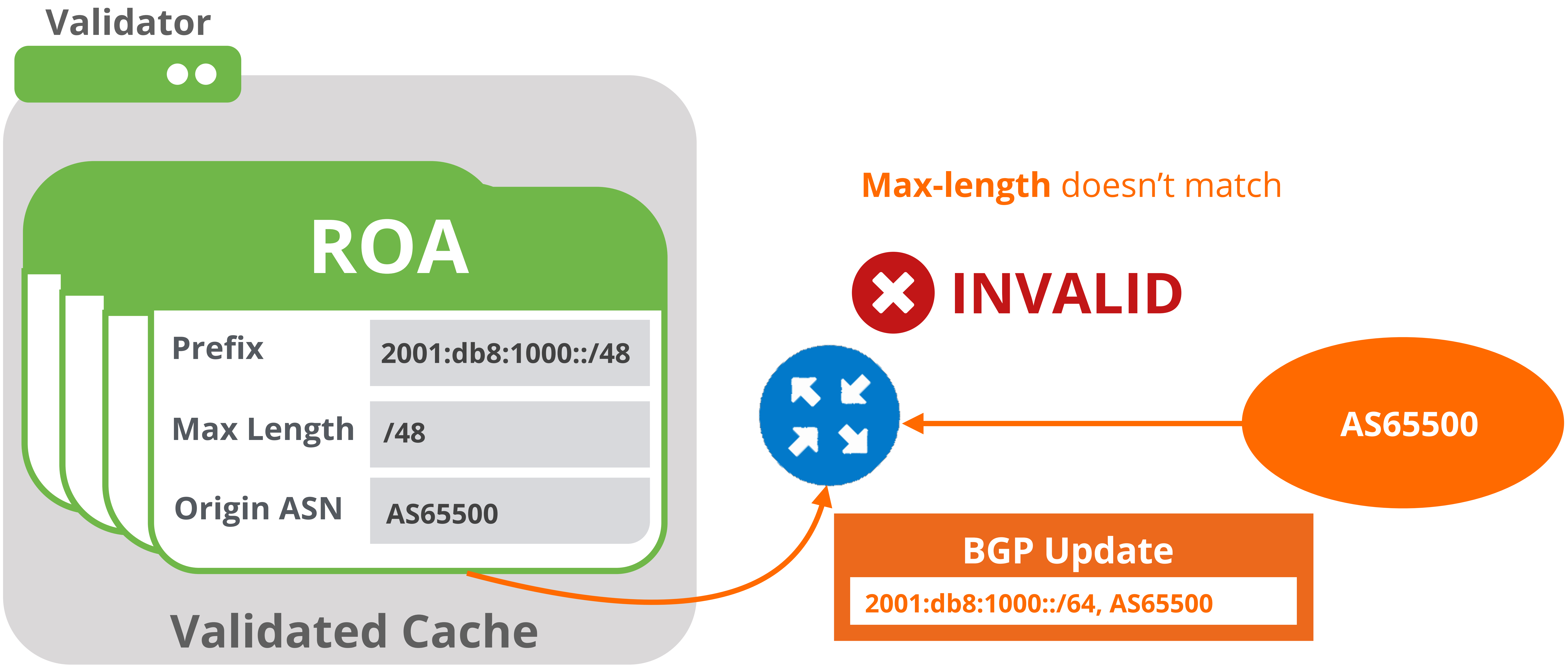
Prefix	2001:db8::/32
Max Length	/32
Origin ASN	AS65536

RFC 6811 - BGP Prefix Origin Validation https://datatracker.ietf.org/doc/html/rfc6811

How Does RPKI Validate the Origin?



How Does RPKI Validate the Origin?



Validator

ROA

Prefix	2001:db8:1000::/48
Max Length	/48
Origin ASN	AS65500

Validated Cache

Max-length doesn’t match

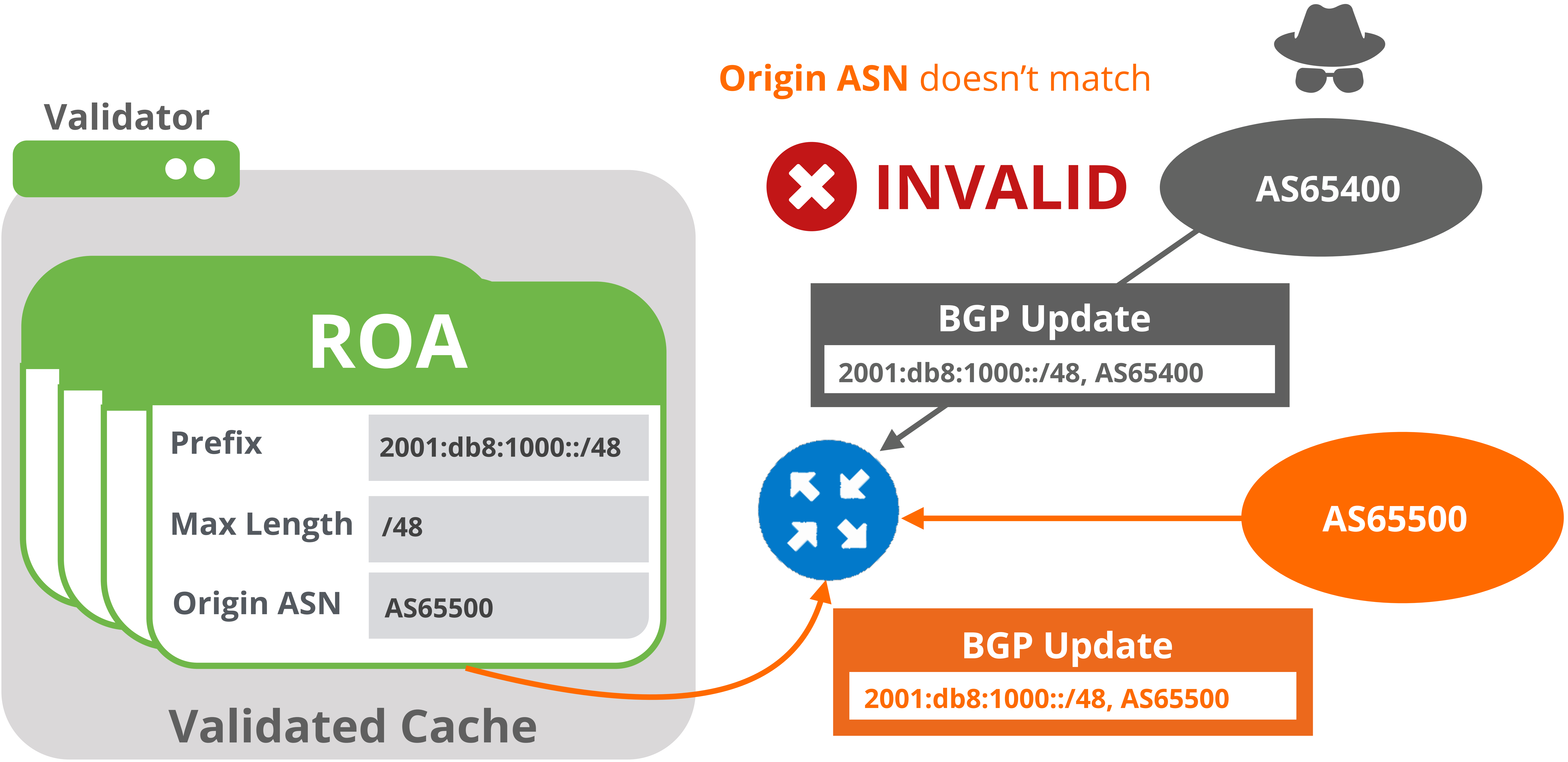
✖ INVALID

AS65500

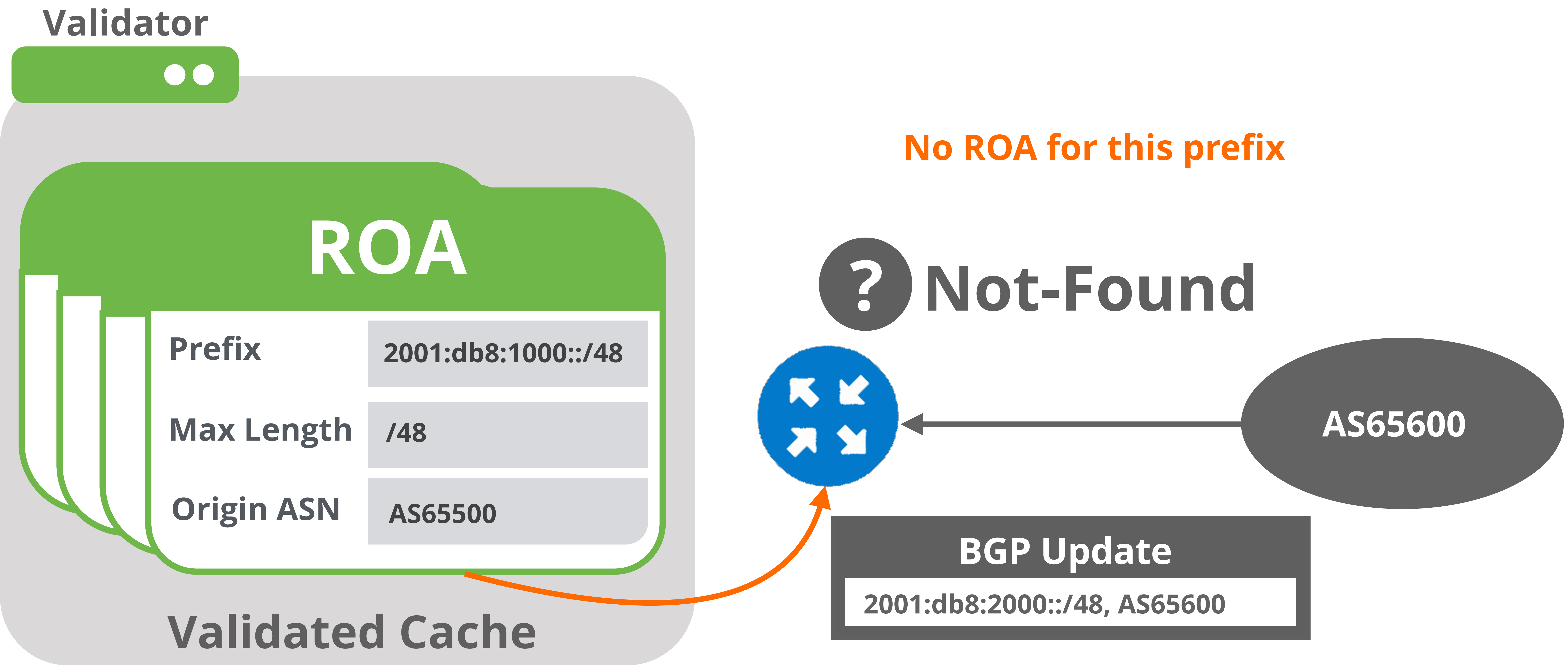
BGP Update

2001:db8:1000::/64, AS65500

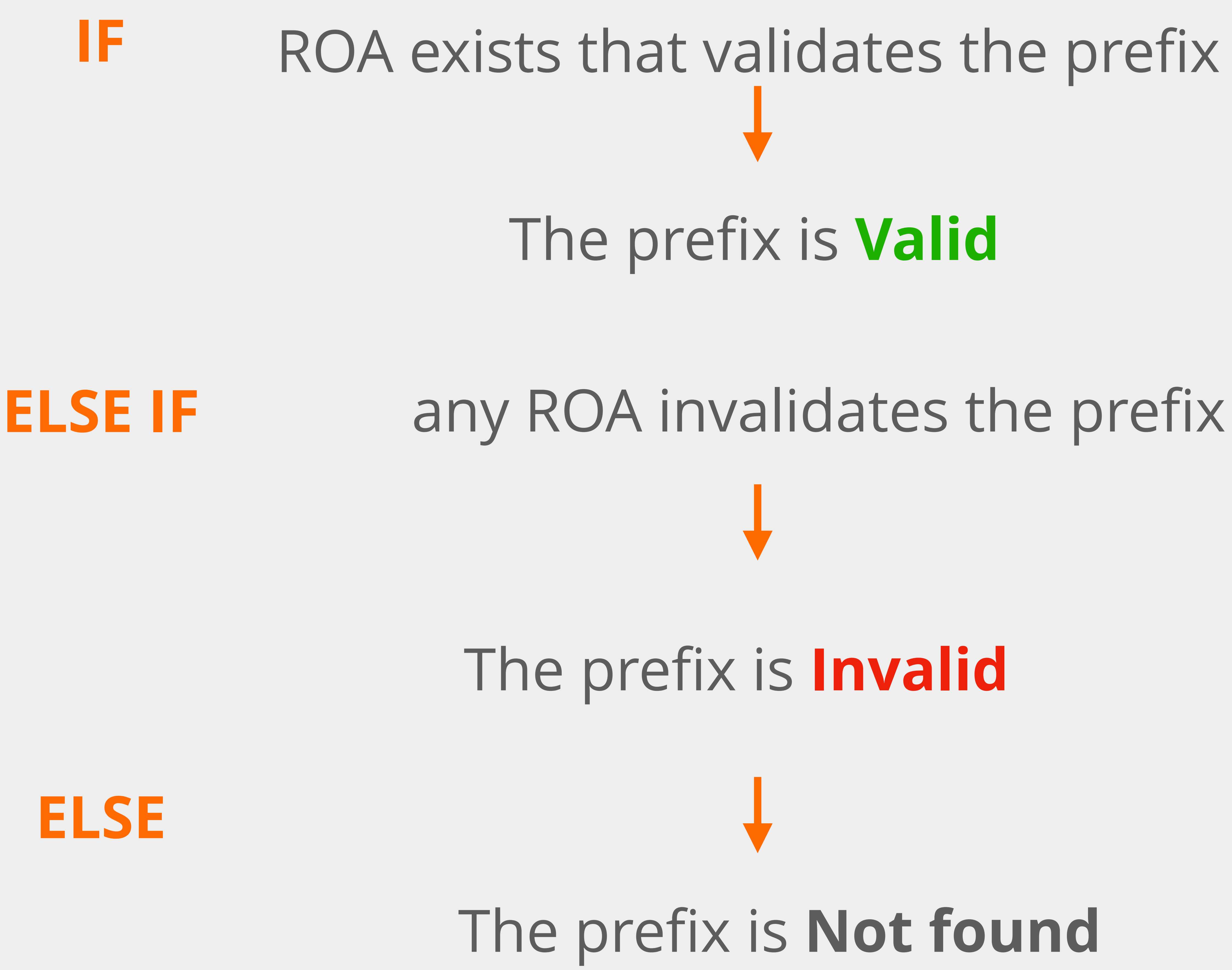
How Does RPKI Validate the Origin?



How Does RPKI Validate the Origin?



The General Rule



IF ROA exists that validates the prefix

↓

The prefix is **Valid**

ELSE IF any ROA invalidates the prefix

↓

The prefix is **Invalid**

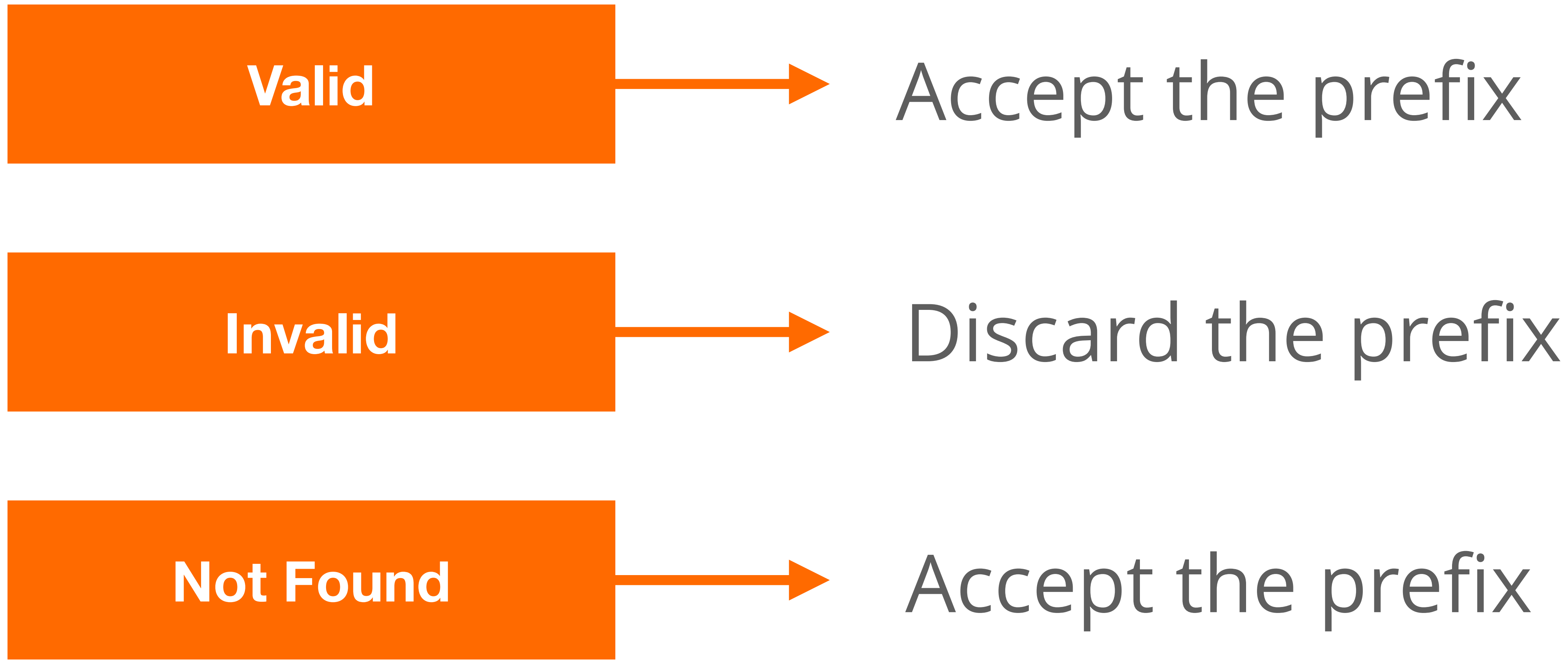
ELSE

↓

The prefix is **Not found**

After Validating

- You have to make a decision: Accept or Discard



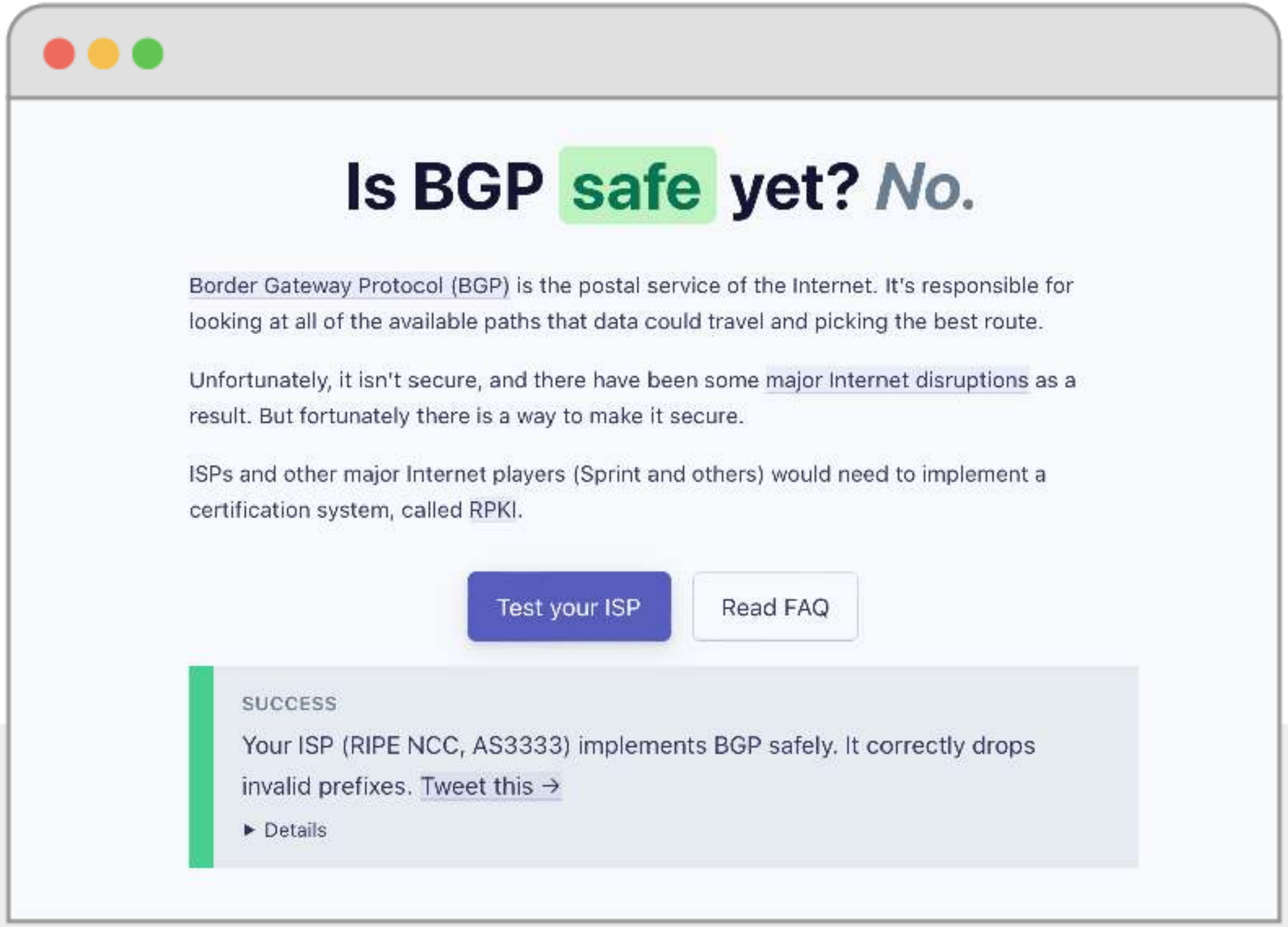
Valid → Accept the prefix

Invalid → Discard the prefix

Not Found → Accept the prefix

Major Networks and RPKI Invalids

- Major networks are dropping invalids
  - Arelion, AT&T, Cloudflare, Netflix, Swisscom, Cogent and etc.
- They follow a phased approach: First peers, then customers



Is BGP safe yet? No.

Border Gateway Protocol (BGP) is the postal service of the Internet. It's responsible for looking at all of the available paths that data could travel and picking the best route.

Unfortunately, it isn't secure, and there have been some major Internet disruptions as a result. But fortunately there is a way to make it secure.

ISPs and other major Internet players (Sprint and others) would need to implement a certification system, called RPKI.

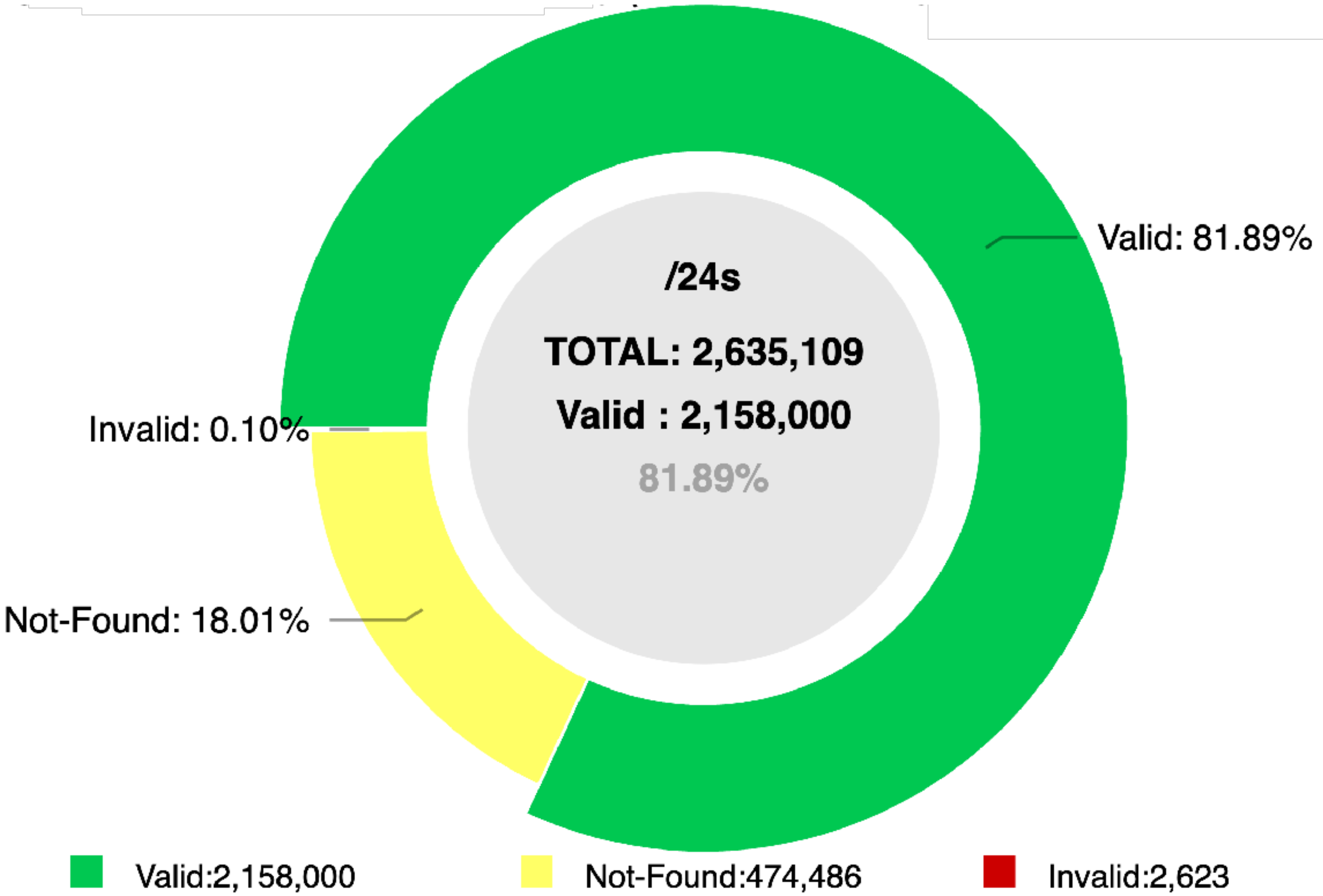
SUCCESS

Your ISP (RIPE NCC, AS3333) implements BGP safely. It correctly drops invalid prefixes. Tweet this →

▸ Details

More information: https://isbgpsafeyet.com/

ROV in the RIPE NCC Service Region (IPv4)



2025-02-23

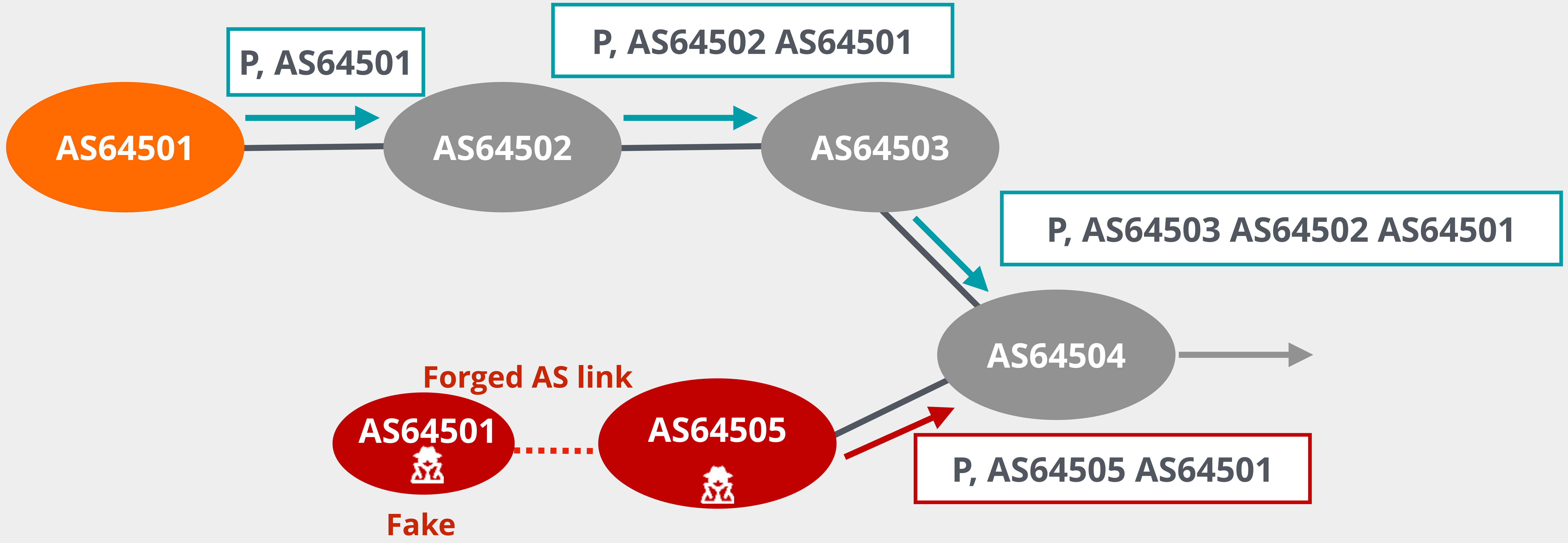
https://rpki-monitor.antd.nist.gov

What’s Next for Routing Security?

Dealing with Path Hijacks…

Fake Path with Correct Origin

- This is not covered by origin validation
- The attacker:
  - Creates a forged AS link between two ASes
  - Reroutes the traffic to itself

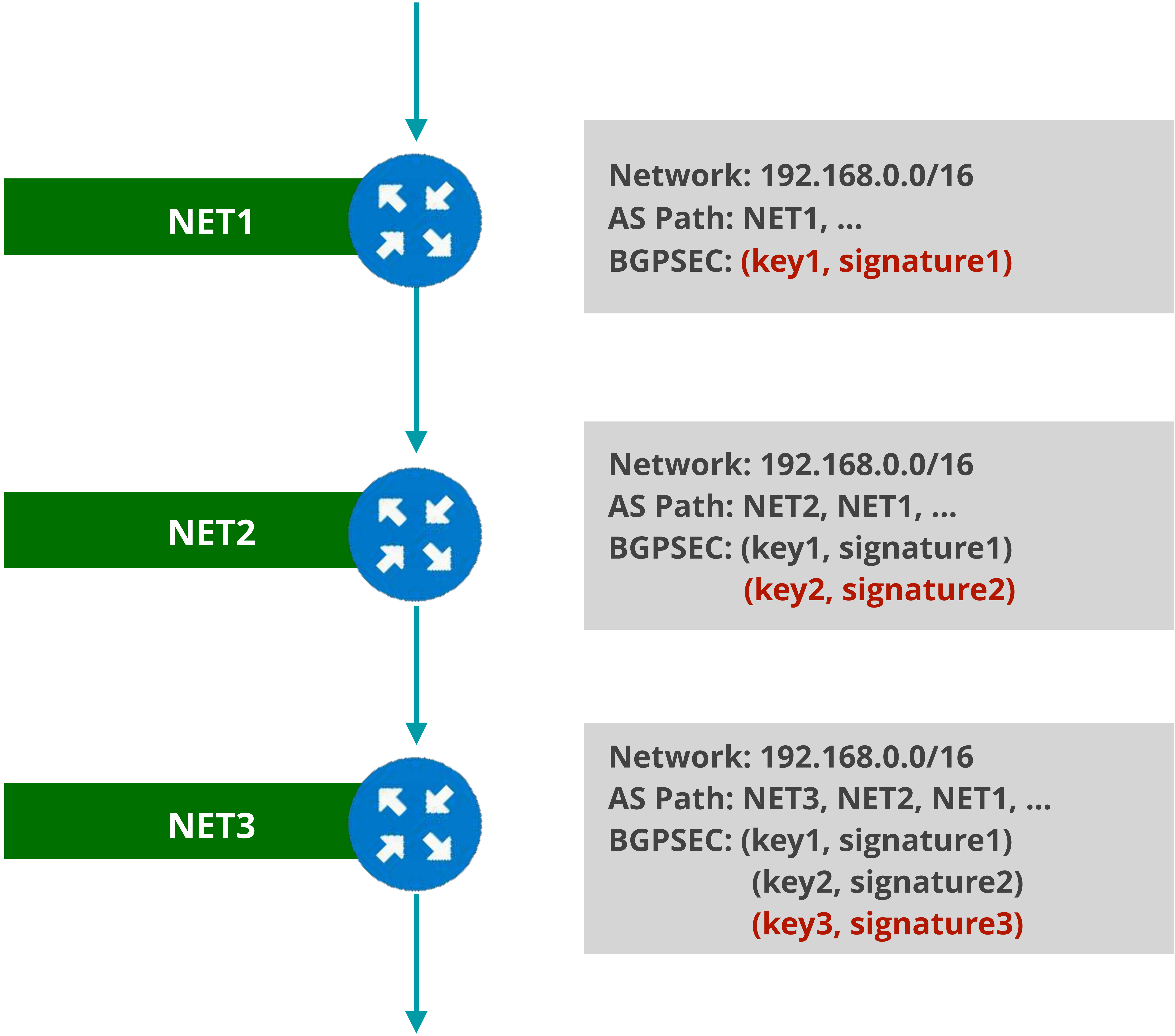


What’s Next for Routing Security?

- RPKI today focuses mostly on **Origin Validation**
- Path manipulations are still possible
  - Origin AS remains intact in the altered AS Path
- **Path validation solutions: BGPsec and ASPA**

BGPsec

- Designed to supplement BGP Origin Validation
- Relies on the RPKI certificates
    - **Router certificates** are issued to routers within an autonomous system
- Introduces a new BGP path attribute, **BGPsec_PATH**
    - Optional, non-transitive attribute
    - Carries digitally signed AS path information
    - Support is negotiated between BGP speakers



Network: 192.168.0.0/16
AS Path: NET1, ...
BGPSEC: (key1, signature1)

Network: 192.168.0.0/16
AS Path: NET2, NET1, ...
BGPSEC: (key1, signature1)
(key2, signature2)

Network: 192.168.0.0/16
AS Path: NET3, NET2, NET1, ...
BGPSEC: (key1, signature1)
(key2, signature2)
(key3, signature3)

BGPsec Limitations

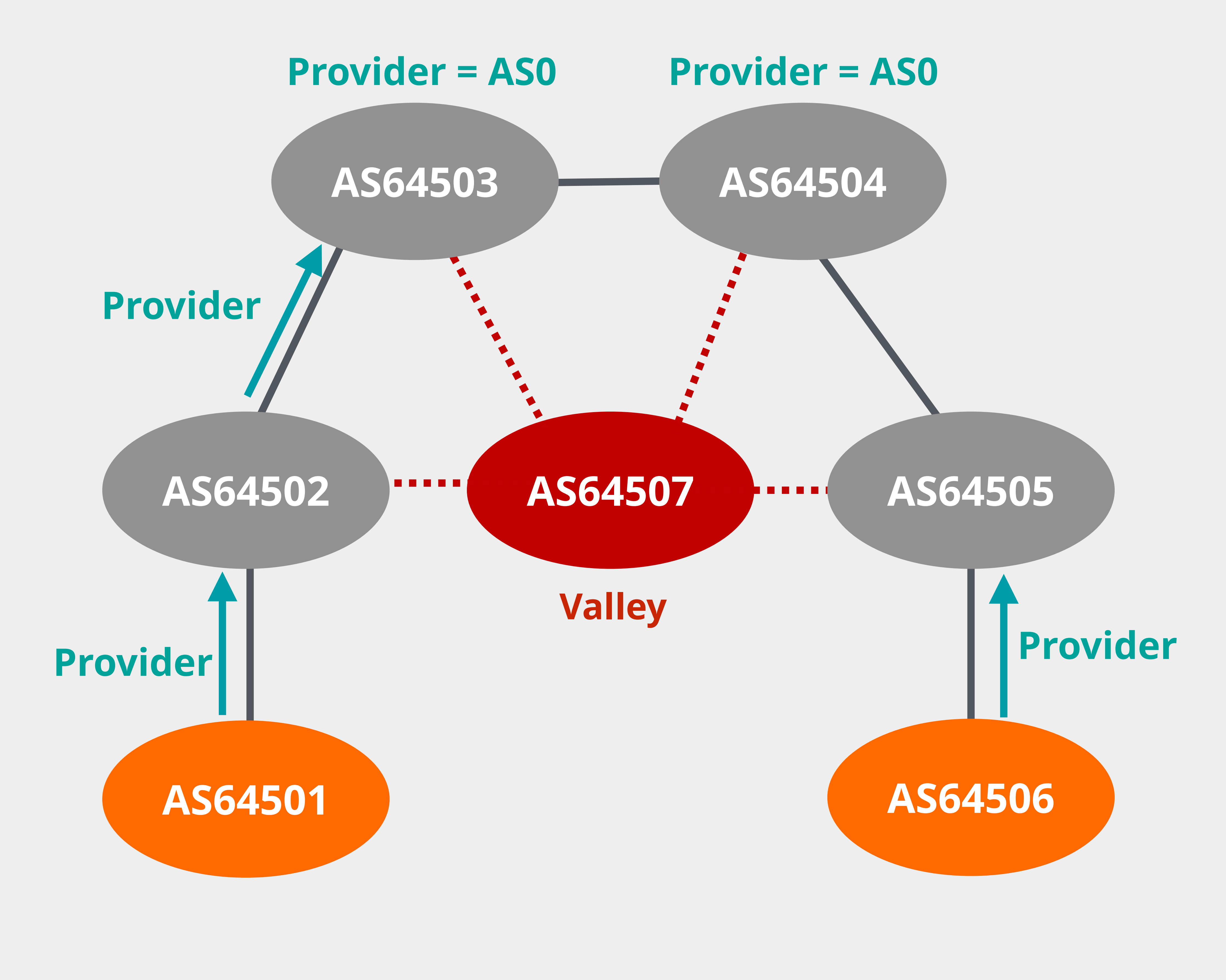
- Does not offer origin validation
- Does not **prevent route leaks** (misconfigured routers will sign even wrong information)
- **Expensive to run**, requires more powerful routers
  - UPDATE messages are larger because of digital signatures
  - One UPDATE message is required for each prefix
  - BGP speakers need to perform cryptographic functions
- **Incremental deployment is tricky**

Autonomous System Provider Authorisation

- Introduces a new digitally signed object, an **ASPA**
  - ASPA object defines **upstreams (providers) for a defined Autonomous system**
- ASPA is a **lightweight solution for path validation**
  - Works very similar to ROV
  - Does not require a new BGP attribute
  - Verifies the sequence of ASes along the path
- **Supported in RIPE NCC Hosted RPKI since 26 November 2025**

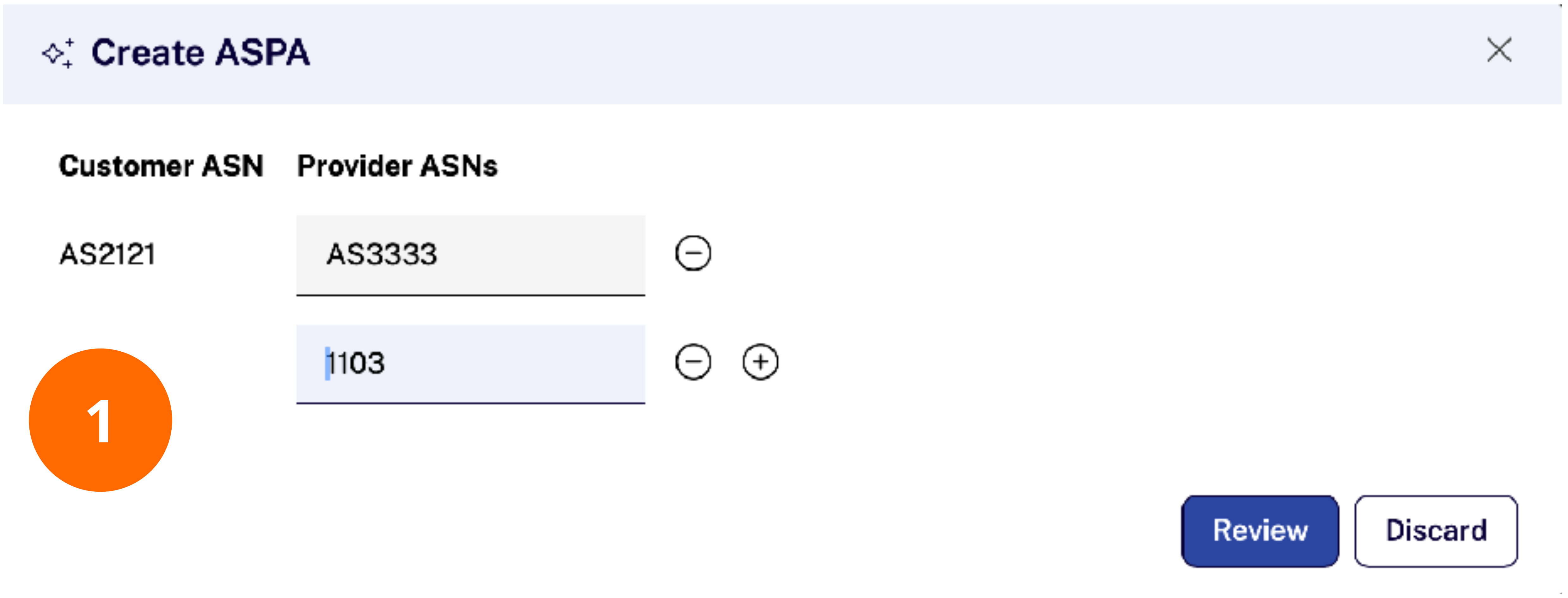
How Does ASPA Work?

- AS holder creates an **ASPA object** and signs it
  - Authorises a set of **Provider ASes** to propagate its route announcements
- In the Validation process, checks the AS path
  - Each AS-to-AS hop gets verified as:
    - **Provider**
    - **NOT Provider**
    - **No Attestation** (no ASPA exists)
  - Paths with **valleys** are rejected



ASPA in the RIPE NCC RPKI Portal

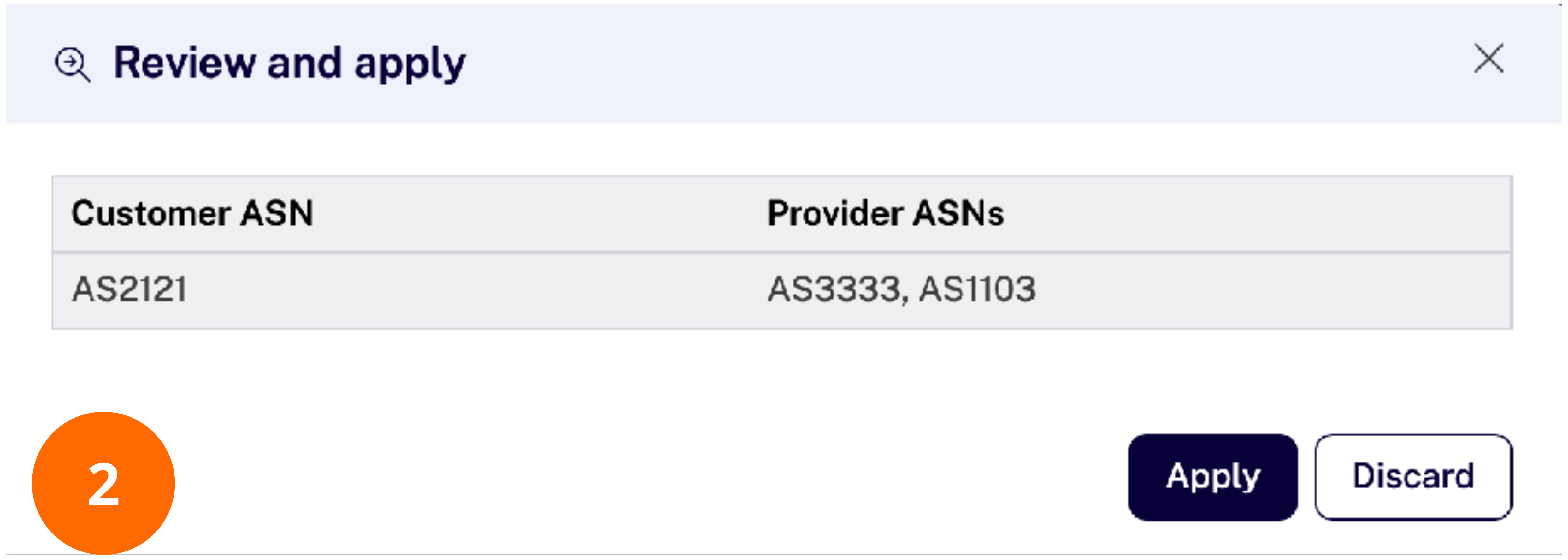
- You define a **set of providers** for each ASN you hold
- Put in:
  - Your direct upstream ASNs
  - Your **backup** upstream ASNs
- **Do not** put in:
  - Your customers or peers
- **We don't know** who **ALL** your upstreams are
  - You have to provide the list yourself



1

Create ASPA

Customer ASN	Provider ASNs
AS2121	AS3333
	1103



2

Review and apply

Customer ASN	Provider ASNs
AS2121	AS3333, AS1103

Summary

- Incidents in BGP happen all the time
- Most of them are just mistakes
- **Internet Routing Registries** help, but they have limitations
- RPKI provides reliable cryptography-backed distributed database, supported consistently by all 5 Regional Internet Registries
- **Route Origin Validation** is first and well deployed feature of RPKI
- **Autonomous System Provider Authorisation** is rolling out right now

Questions ?

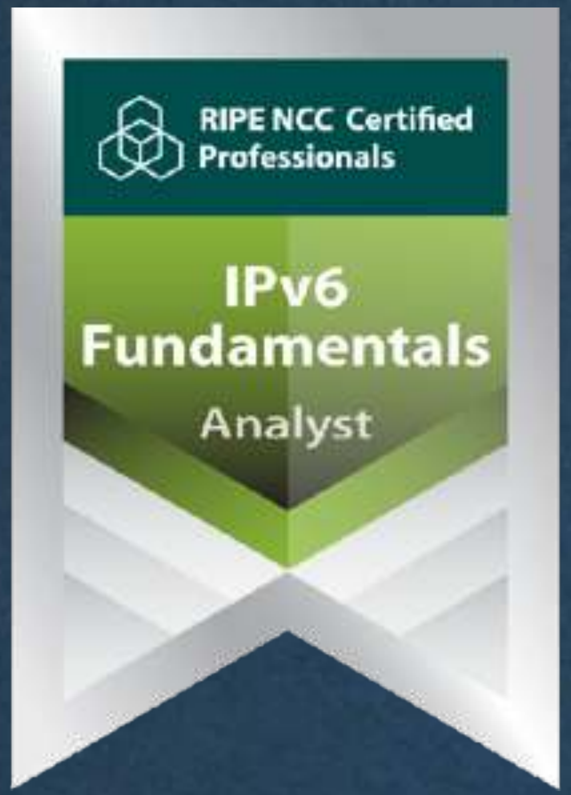
Ondrej.Caletka@ripe.net
https://Ondřej.Caletka.cz
@oskar456@mastodon.social

RIPE NCC
Academy

Learn something new today!

academy.ripe.net

RIPE NCC Certified Professionals



RIPE NCC Certified Professionals
RIPE Database
Associate

RIPE NCC Certified Professionals
BGP Security
Associate

RIPE NCC Certified Professionals
IPv6 Security
Expert

https://getcertified.ripe.net/

What's Next in BGP

Webinars

Attend another webinar live wherever you are.

- BGP Filtering (1 hr)
- Deploying RPKI (2 hrs)
- Introduction to RPKI (1 hr)
- Internet Routing Registry (1 hr)

Face-to-face

Meet us at a location near you for a training session delivered in person.

- BGP Routing Security (8.5 hrs)

For more info click the link below

learning.ripe.net

E-learning

Learn at your own pace at our online Academy.

- BGP Security (10 hrs)

For more info click the link below

academy.ripe.net

Examinations

Learnt everything you needed? Get certified!

- BGP Security Associate

For more info click the link below

getcertified.ripe.net

Ënn

Vége

Son

Lõpp

Kraj

Fine

Fim

Соңы

Endir

დასასრული

Amaia

Sfârşit

Fin

Slut

An Críoch

Finvezh

הסוף

Loppu

النهاية

Einde

Конец

Fí

پایان

վերջ

Tmiem

Slutt

Край

Ende

Кінець

Liðugt

Konec

Beigas

Y Diwedd

Koniec

Finis

Крај

Fund

Τέλος

Pabaiga

Copyright Statement

[...]

The RIPE NCC Materials may be used for **private purposes, for public non-commercial purpose, for research, for educational or demonstration purposes**, or if the materials in question specifically state that use of the material is permissible, and provided the RIPE NCC Materials are not modified and are properly identified as RIPE NCC documents. Unless authorised by the RIPE NCC in writing, any use of the RIPE NCC Materials for advertising or marketing purposes is strictly forbidden and may be prosecuted. The RIPE NCC should be notified of any such activities or suspicions thereof.

[...]

Find the full copyright statement here:
https://www.ripe.net/about-us/legal/copyright-statement