RIPE NCC
RIPE NETWORK COORDINATION CENTRE

BGP Security Webinars

Deploying RPKI

Webinar

RIPE NCC Learning & Development

This session is being recorded

Take the poll!

Have you implemented **RPKI** yet?

⏱ 1 min.

Agenda

- BGP & Routing Security
- RPKI: Resource Certification
- Registering in RPKI System: Route Origin Authorisation (ROA)
- RPKI Validation: Deploying RPKI Validators
- Secure routing with RPKI
    - Validating BGP Announcements
    - Discarding BGP Invalids

BGP & Routing Security

BGP has some challenges …

- BGP has some challenges from the perspective of routing security
  - It is only based on trust, no built-in security
  - No verification of the correctness of prefixes or AS paths
- These challenges are discussed in RFC#4272: “BGP Security Vulnerabilities Analysis”.

RFC#4272,“BGP Security Vulnerabilities Analysis”

Vulnerabilities of BGP

- Based on RFC, BGP has three fundamental vulnerabilities:

1. No internal mechanism to protect the integrity and source authenticity of BGP messages
2. No mechanism specified to validate the authority of an AS to announce NLRI
3. No mechanism to verify the authenticity of the attributes of a BGP update message

- These vulnerabilities can be exploited either **maliciously** or **accidentally**

Due to these vulnerabilities …

- Any AS can announce any prefix
  - BGP prefix hijacks due to malicious activity / mis-origination
- Any AS can prepend any ASN to the AS path
  - Path hijacks, MITM
- Fake routing information could be propagated over the Internet and disrupt overall Internet behaviour

For Secure Internet Routing …

- Do not be the cause!
  - Announce the right prefixes to the right peers
  - Have proper filters in place to eliminate route leaks
- Do not spread others’ mistakes or attacks!
  - Validate the routing information you receive
- Do not be the victim!
  - Implement recommended security measures to protect your network

How to validate incoming routes?

1 Is an Autonomous System (AS) authorised to originate a certain IP prefix?

- The IRR system was introduced to address this
  - Used to register prefixes and routing policies by using the RPSL language
  - But unfortunately, IRR data is not sufficiently accurate, up-to-date or complete for filtering purposes
- **RPKI** aims to complement and expand this effort
  - Validates the routes based on trusted, accurate and up-to-date RPKI data

How to validate incoming routes?

2 Are BGP path attributes legitimate and correct?

- Requires validation of whole BGP path
  - No path validation is available for now!
  - There is no implementation for BGPsec yet.
- RPKI is stepping stone to path validation!

RPKI

Resource Certification

What is RPKI?

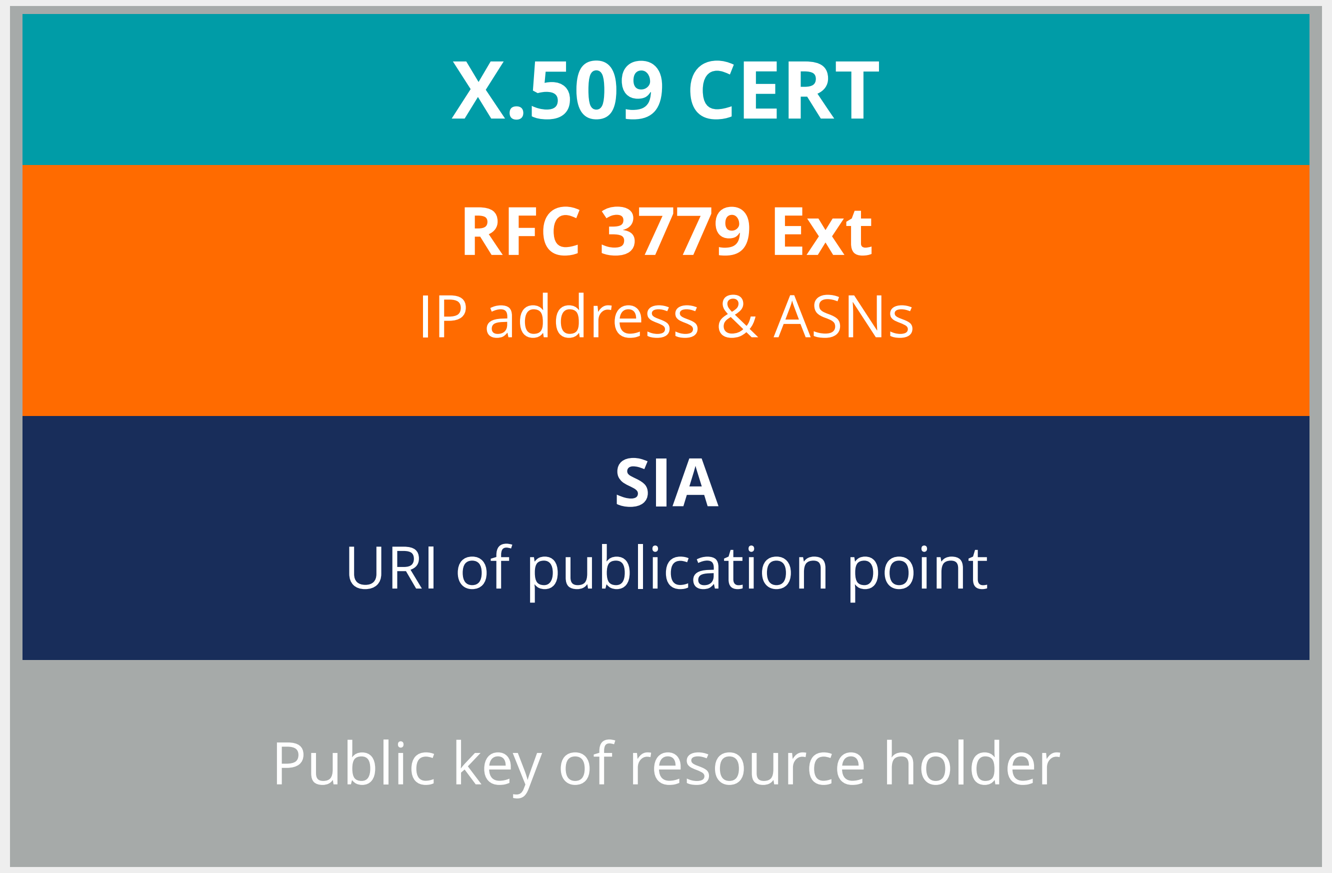
- RPKI aka **resource certification** is …
  - a security framework developed by the IETF
  - designed to make Internet routing more secure and reliable

Resource
Public
Key
Infrastructure

How does RPKI secure Internet routing?

- Verifies the association between resource holders and their Internet number resources

- Attaches digital certificate to IP addresses and AS numbers
  - uses X.509 PKI certificates with RFC#3779 extensions



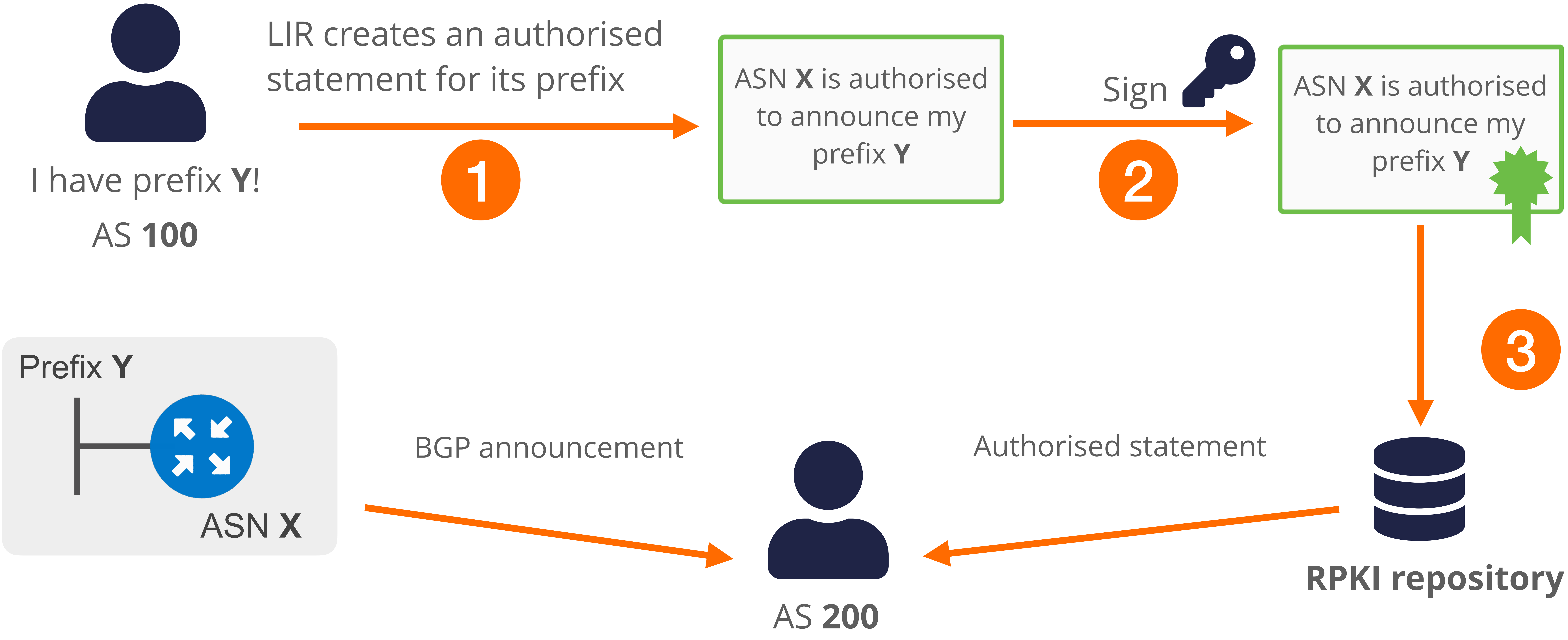
X.509 CERT

RFC 3779 Ext
IP address & ASNs

SIA
URI of publication point

Public key of resource holder

How does RPKI secure Internet routing?



I have prefix **Y**!

AS **100**

LIR creates an authorised statement for its prefix

1

ASN **X** is authorised to announce my prefix **Y**

Sign

2

ASN **X** is authorised to announce my prefix **Y**

3

RPKI repository

Authorised statement

AS **200**

BGP announcement

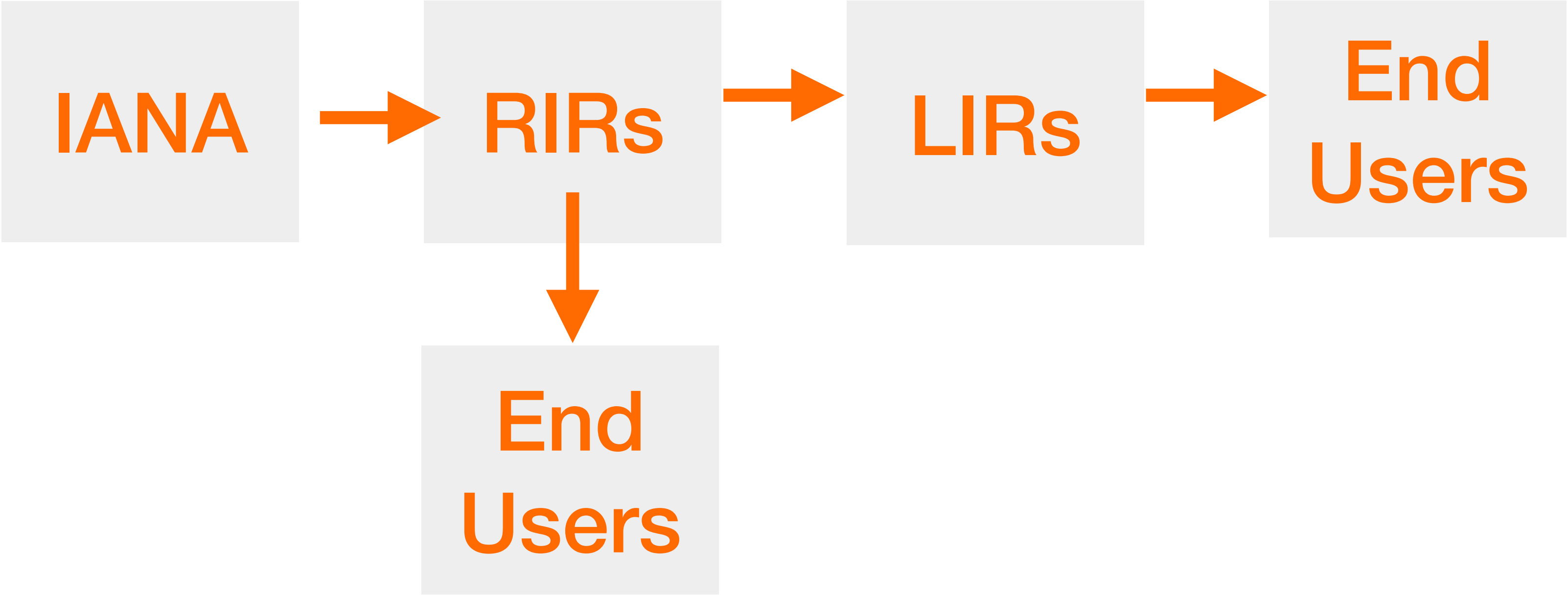
Prefix **Y**

ASN **X**

4 Others use those statements to make better routing decisions!

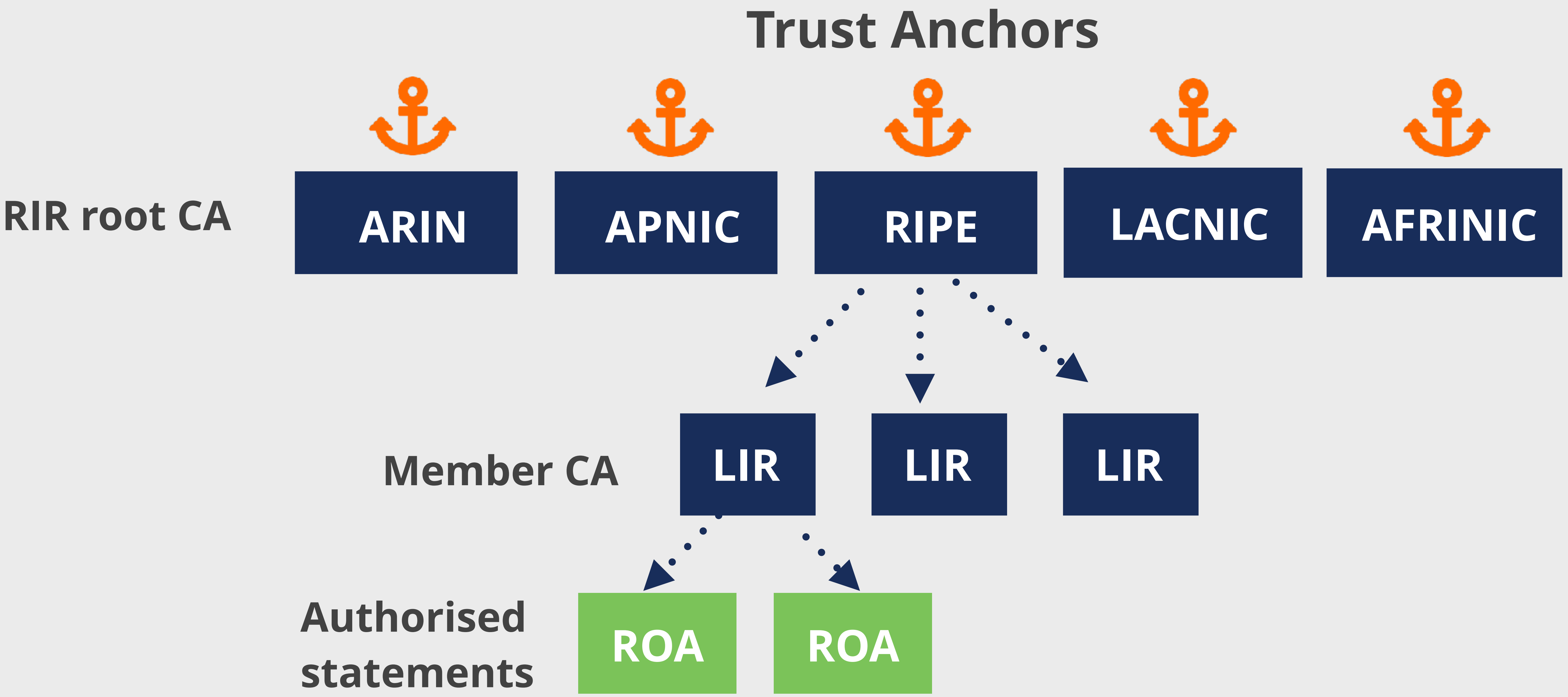
Trust in RPKI

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



IANA → RIRs → LIRs → End Users

RIRs → End Users



Trust Anchors

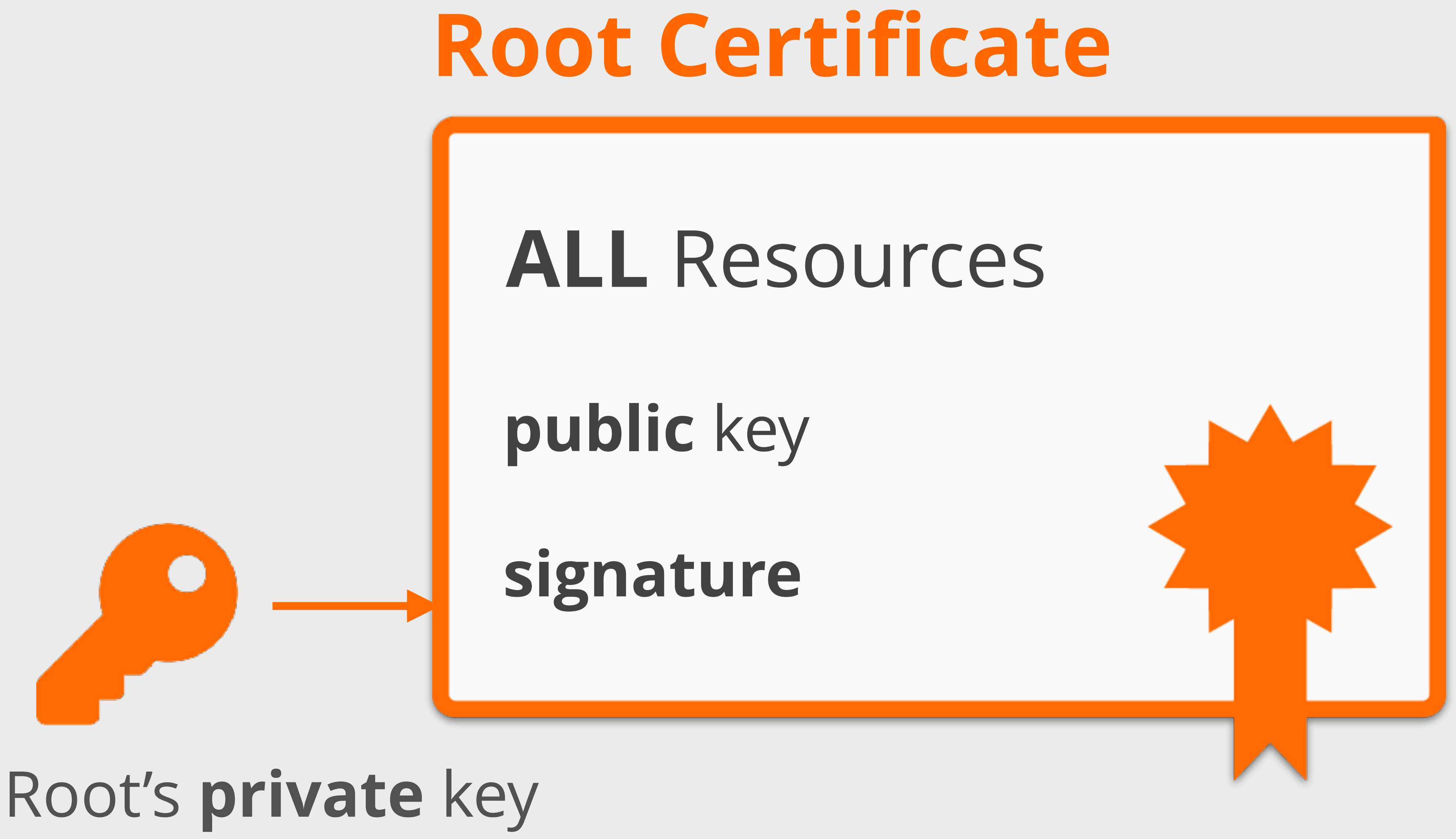
RIR root CA: ARIN, APNIC, RIPE, LACNIC, AFRINIC

Member CA: LIR, LIR, LIR

Authorised statements: ROA, ROA

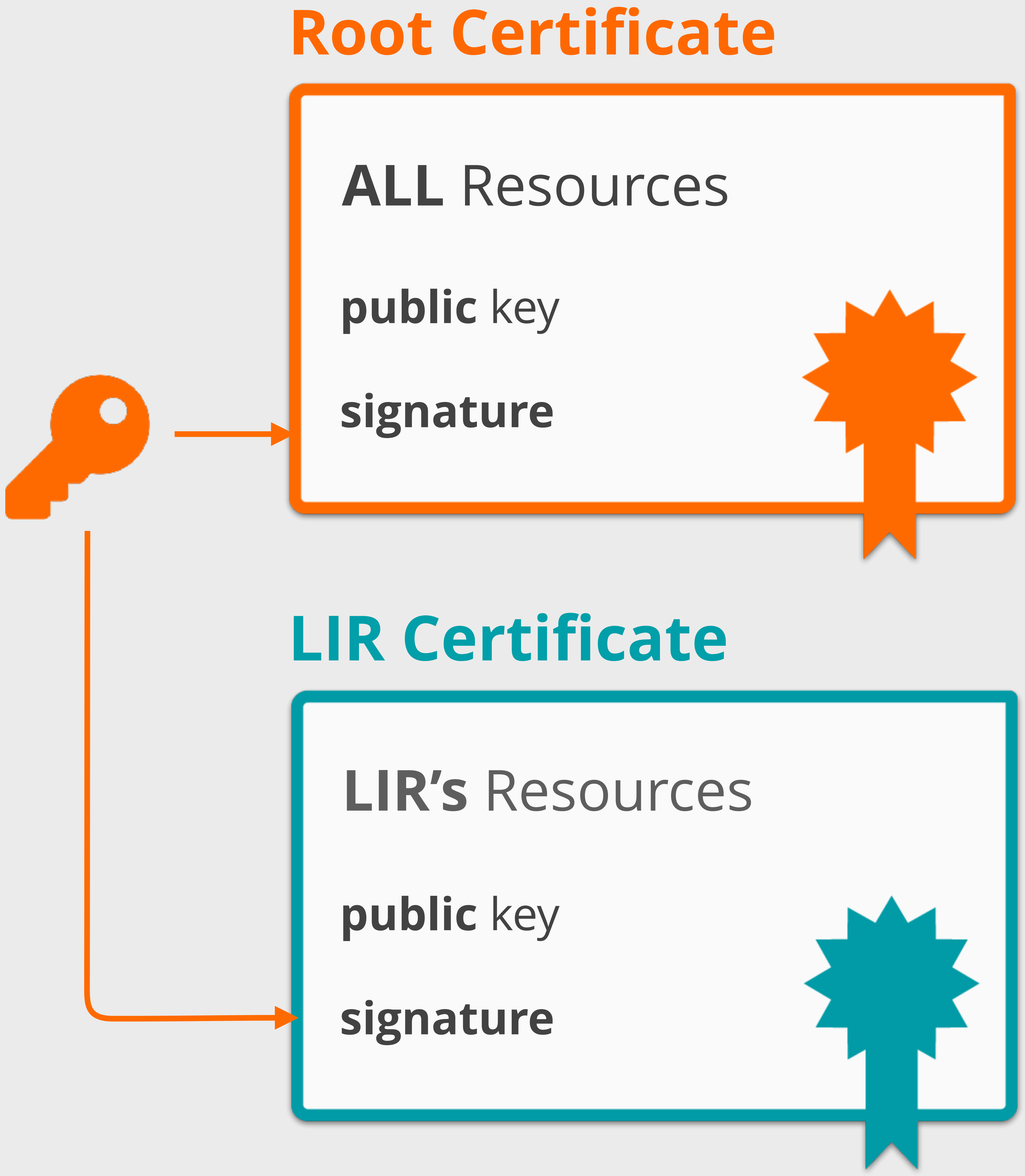
Trust in RPKI

- Root certificate
  - **Self-signed**
  - RIRs use root certificate to sign LIRs' certificates



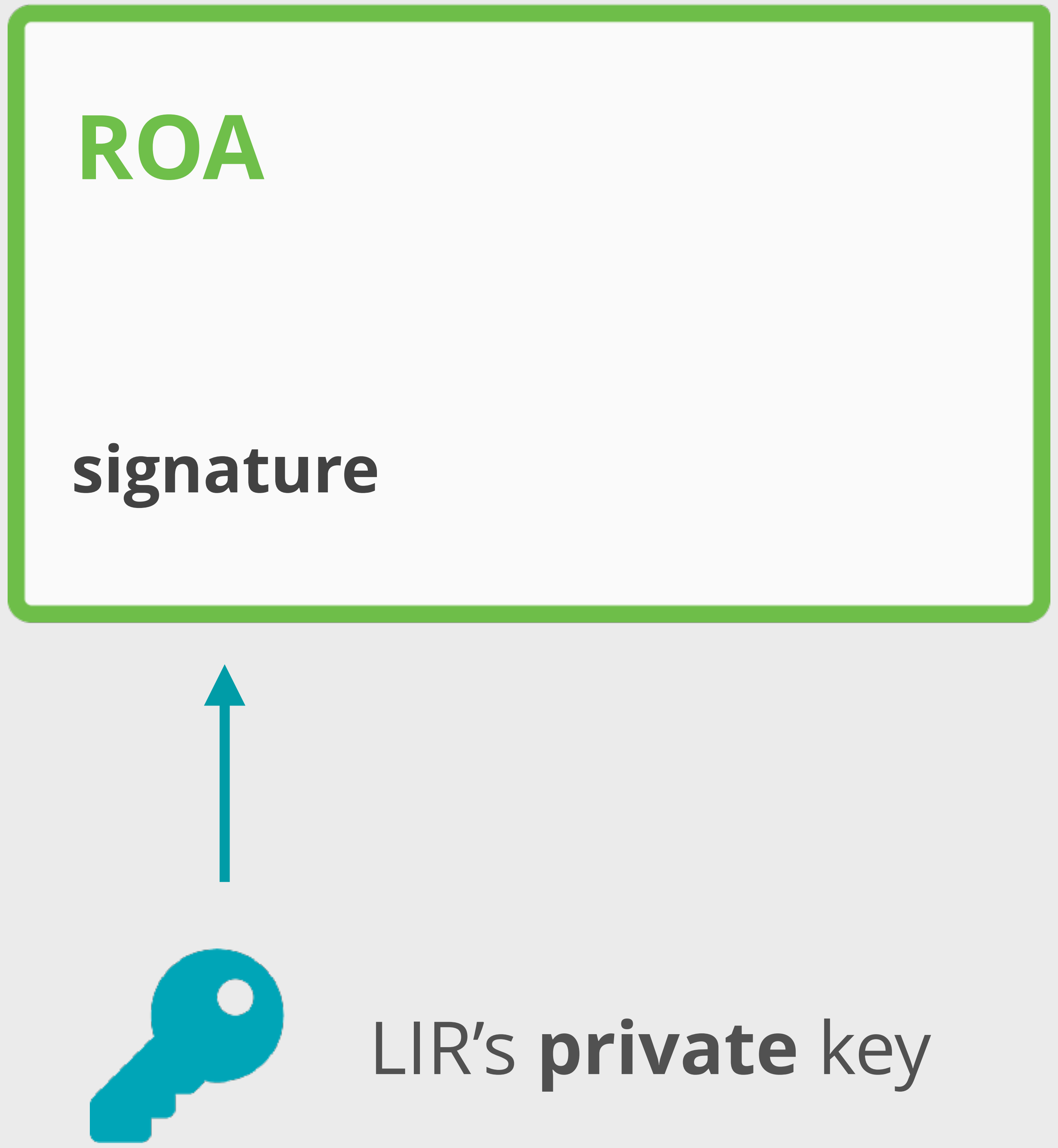
Trust in RPKI

- Root certificate
  - **Self-signed**
  - RIRs use root certificate to sign LIRs' certificates
- LIR certificate
  - Resource certificate for member allocations
  - Binds LIR's resources to LIR's public key
  - Proves legitimate holdership for the LIR's resources

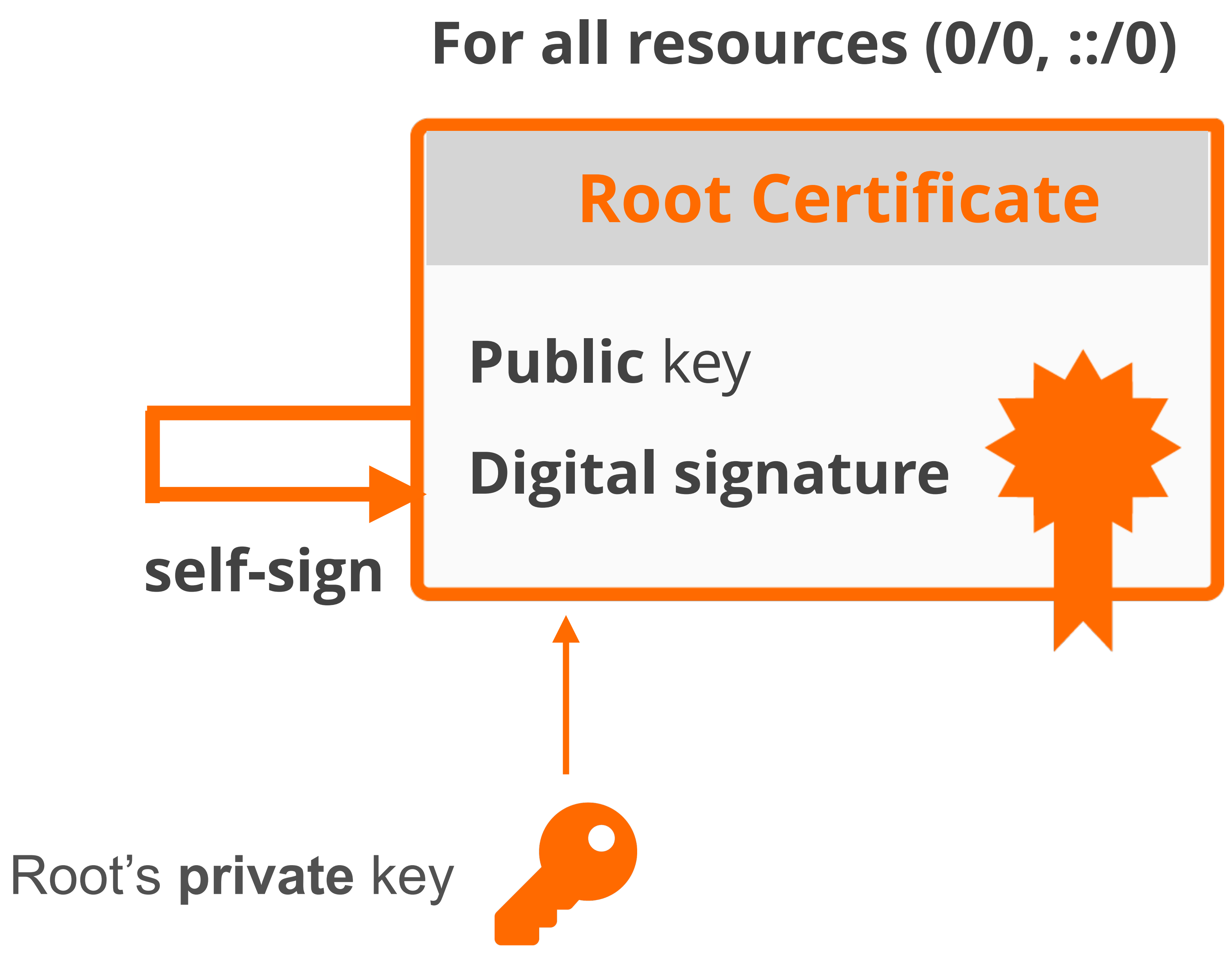


Trust in RPKI

- Authorised statements
  - Known as a ROA (Route Origin Authorisation)
  - Cryptographically signed object
  - Signed by LIR’s private key



RPKI Chain of Trust



For all resources (0/0, ::/0)

Root Certificate

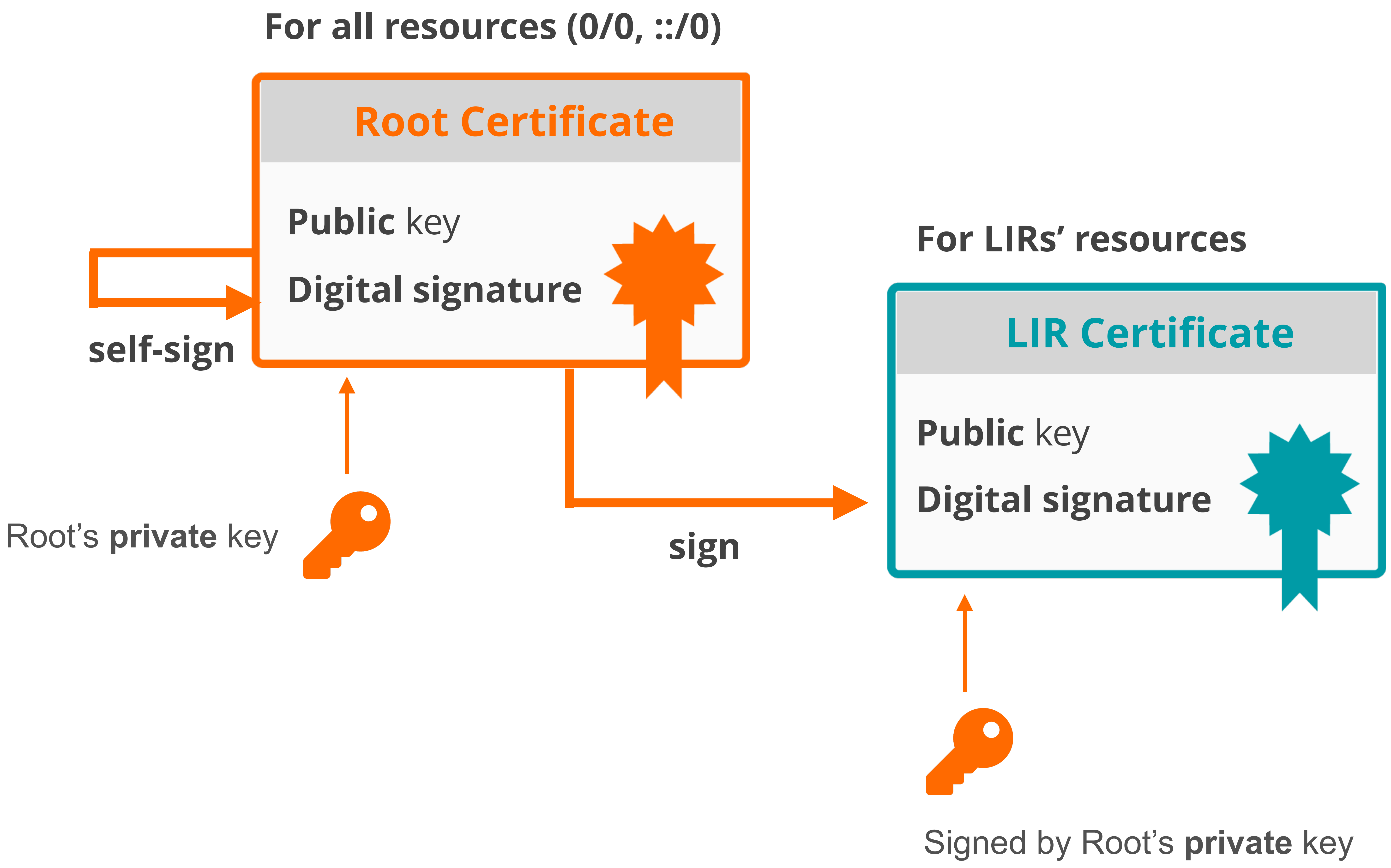
Public key

Digital signature

self-sign

Root’s **private** key

RPKI Chain of Trust



For all resources (0/0, ::/0)

Root Certificate

Public key

Digital signature

self-sign

Root's **private** key

sign

For LIRs' resources

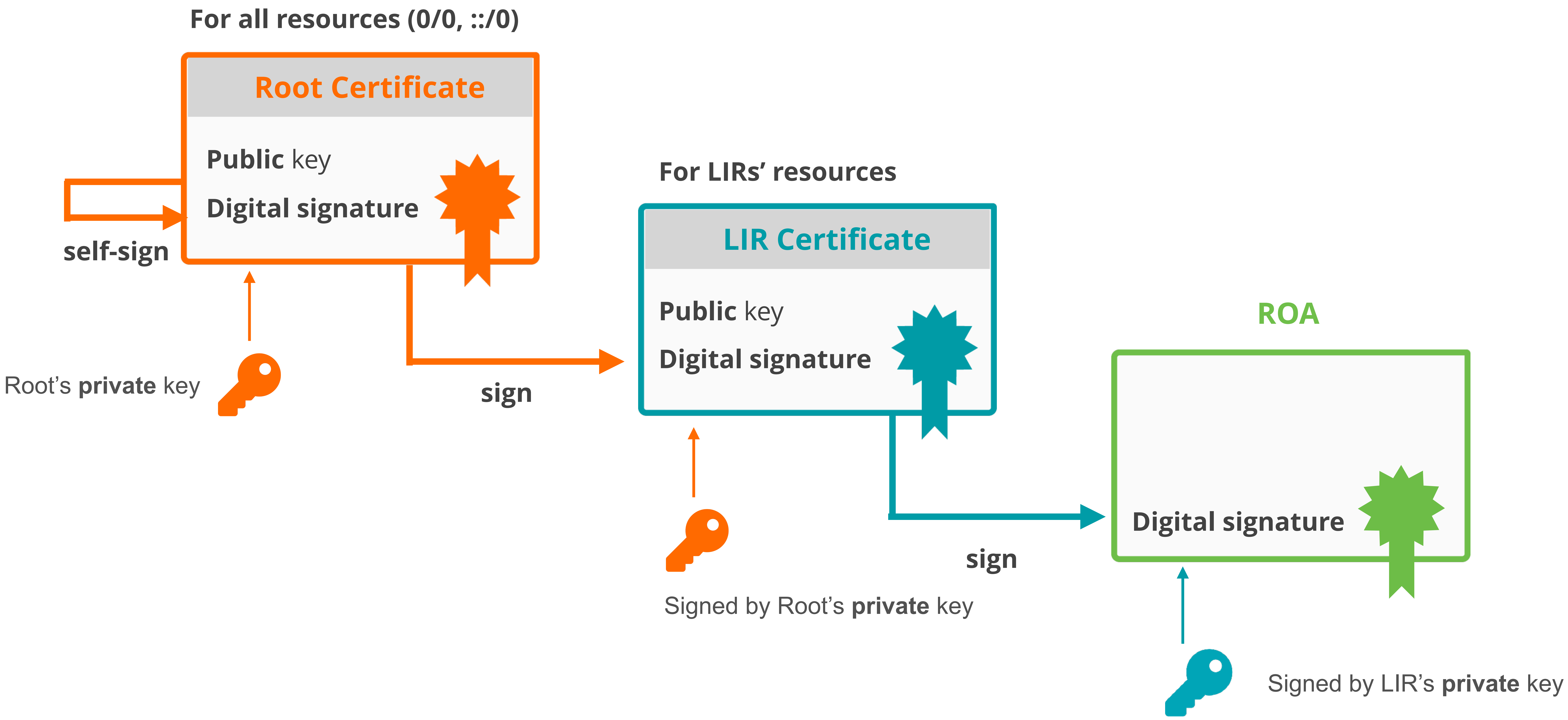
LIR Certificate

Public key

Digital signature

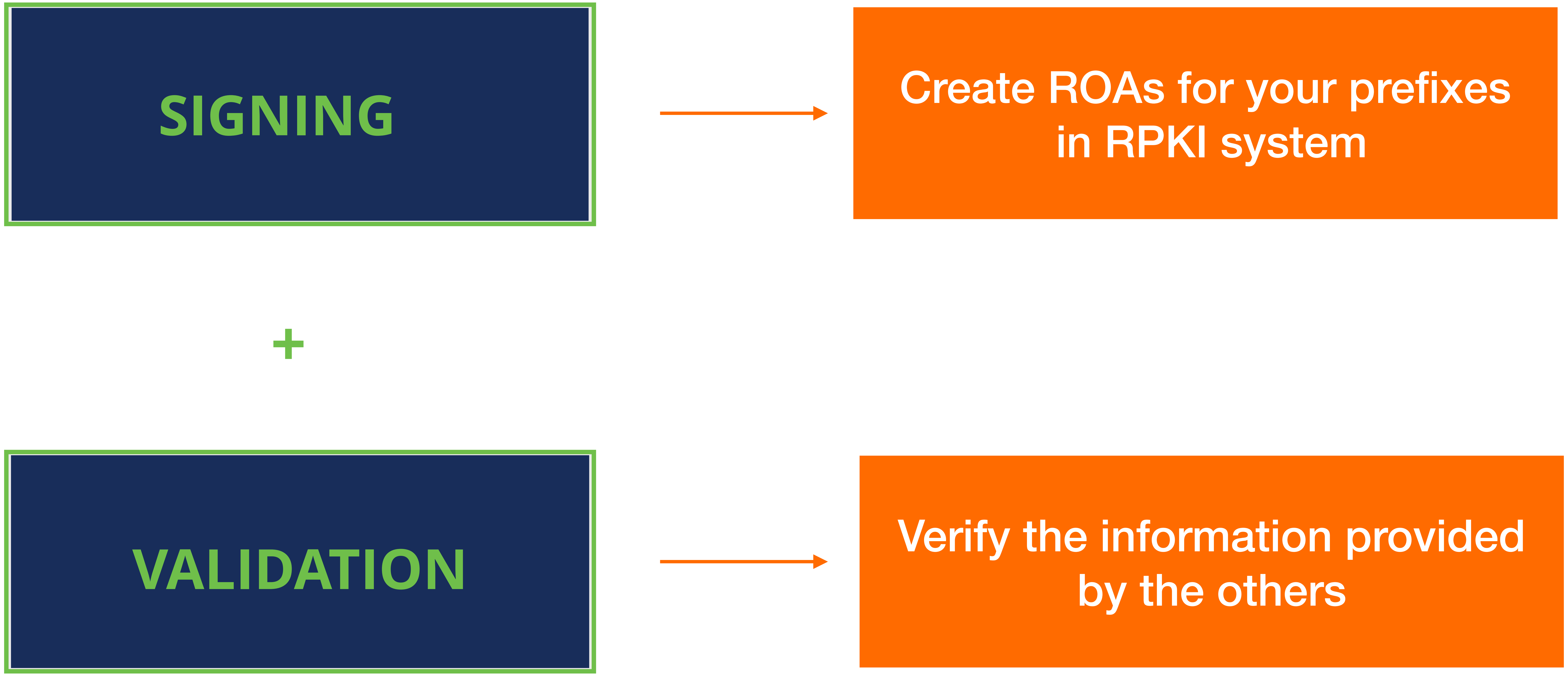
Signed by Root's **private** key

RPKI Chain of Trust



Elements of RPKI

- RPKI system consists of two parts …



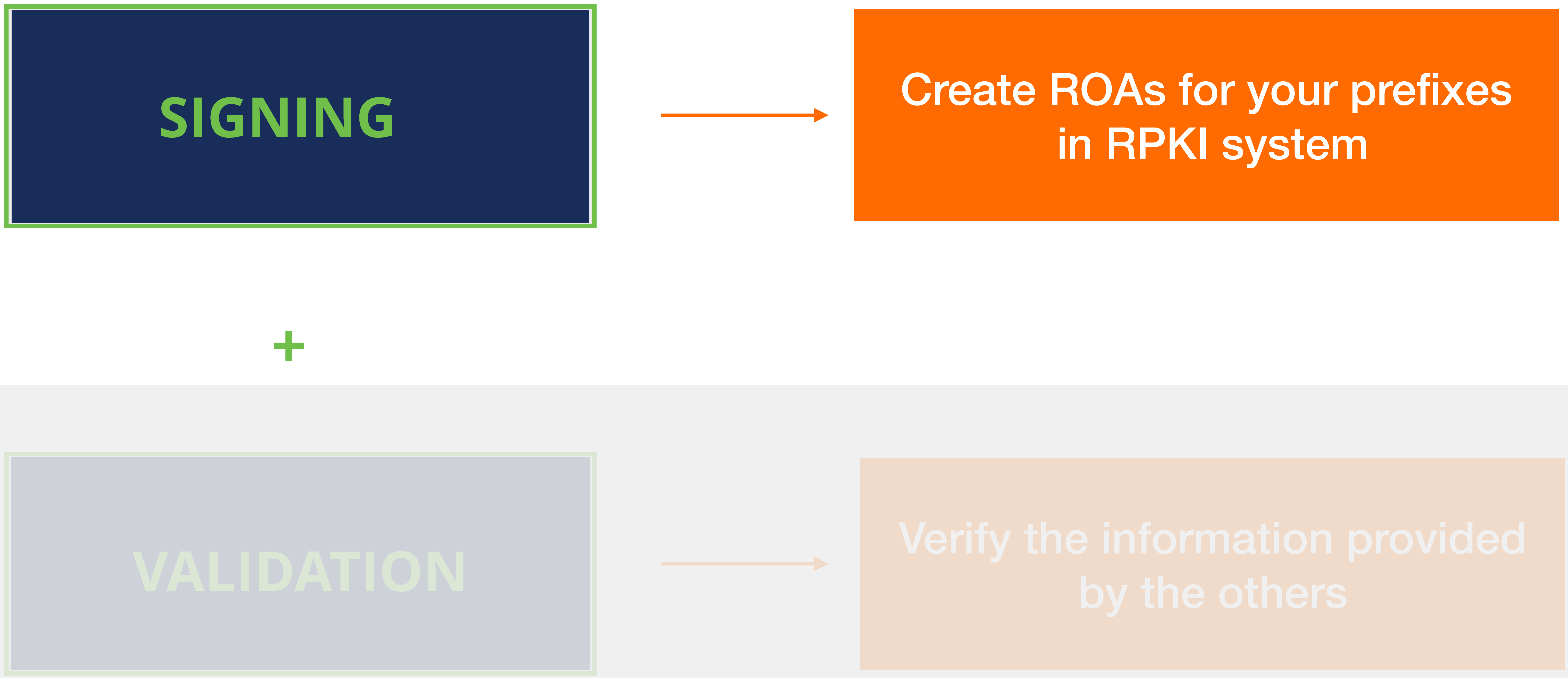
SIGNING → Create ROAs for your prefixes in RPKI system

+

VALIDATION → Verify the information provided by the others

Elements of RPKI

- RPKI system consists of two parts …



SIGNING → Create ROAs for your prefixes in RPKI system

+

VALIDATION → Verify the information provided by the others

Registering in the RPKI system

Route Origin Authorisation

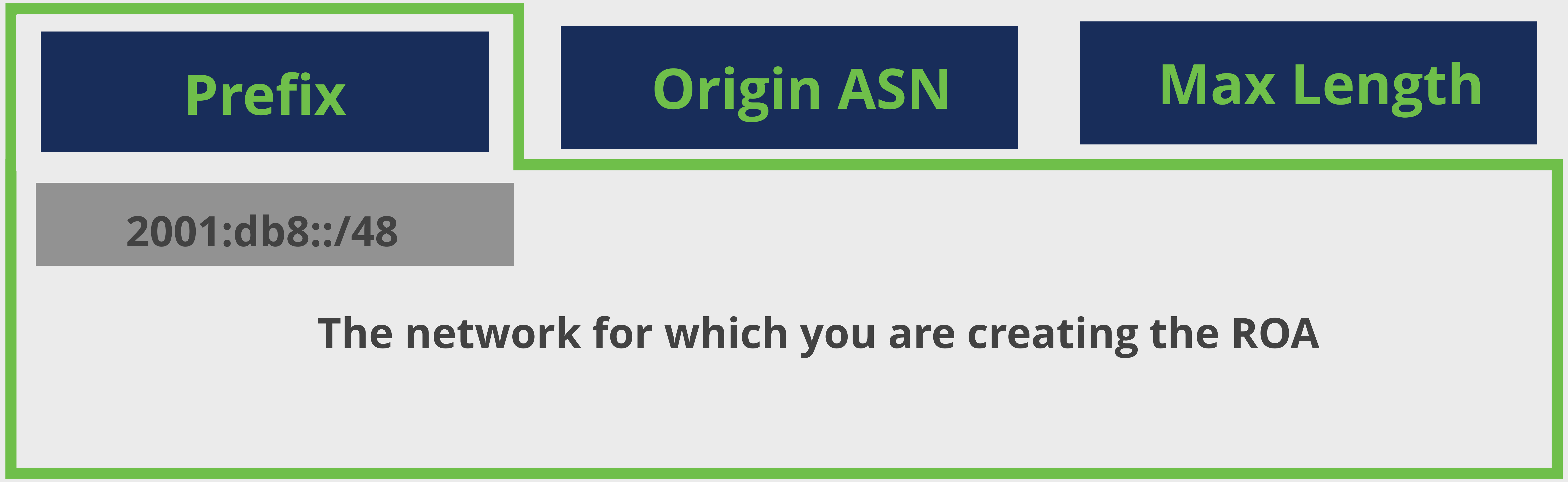
ROA (Route Origin Authorisation)

- An authorised statement created by the resource holder
- It 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 AS	**AS65536**

What is in a ROA?



Prefix

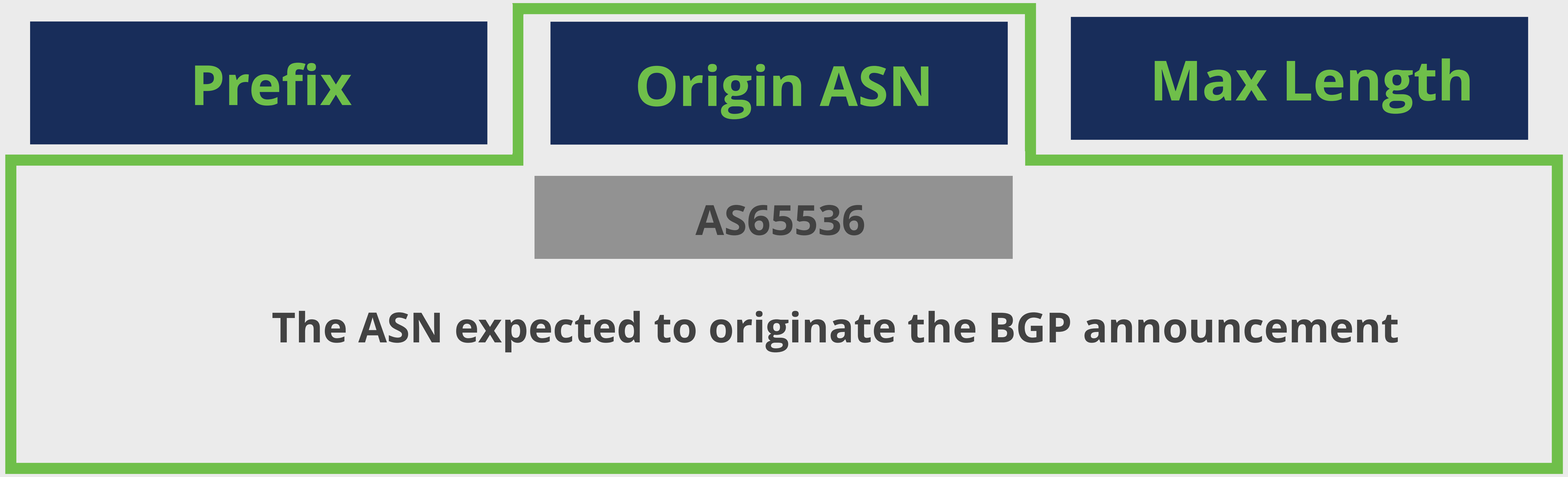
Origin ASN

Max Length

2001:db8::/48

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 authorised to advertise

Max-Length

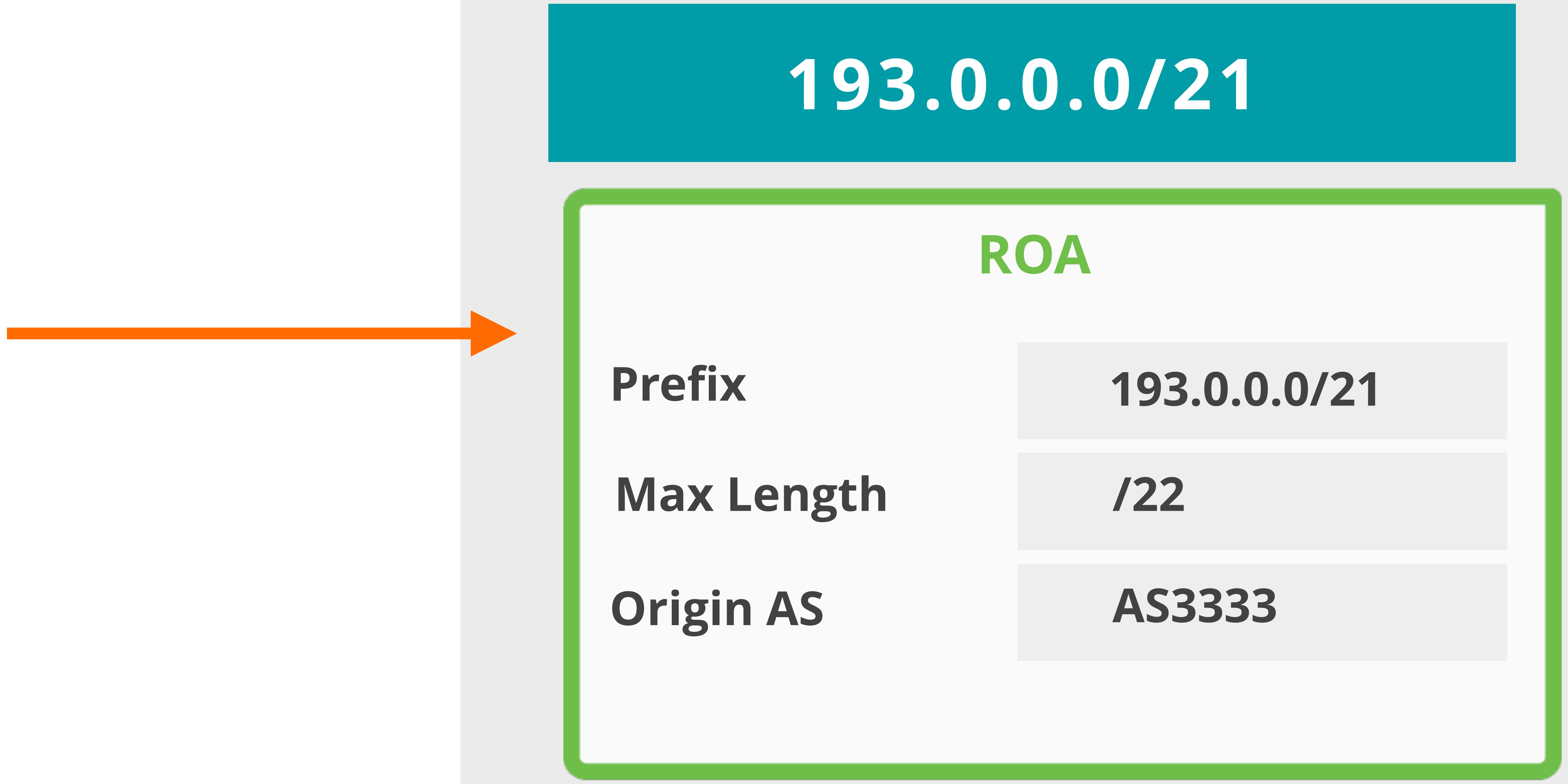
AS3333 has an IP address allocation

193.0.0.0/21

Max-Length

AS3333 has an IP address allocation

AS3333 creates this ROA



193.0.0.0/21

ROA

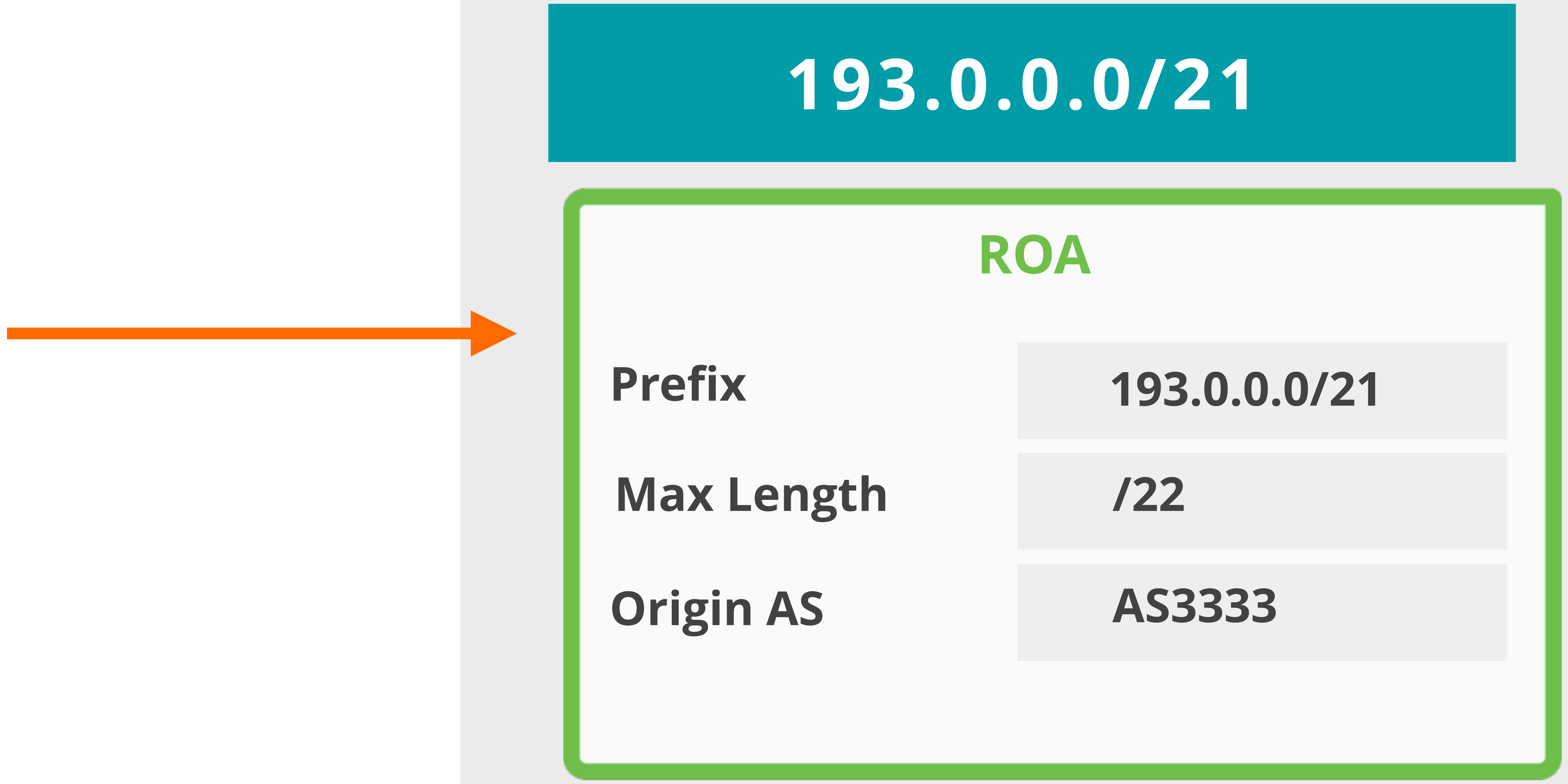
Prefix	193.0.0.0/21
Max Length	/22
Origin AS	AS3333

Max-Length

AS3333 has an IP address allocation

AS3333 creates this ROA

According to ROA;



193.0.0.0/21

ROA

Prefix	193.0.0.0/21
Max Length	/22
Origin AS	AS3333

Max-Length

AS3333 has an IP address allocation

AS3333 creates this ROA

According to ROA;

193.0.0.0/21

ROA

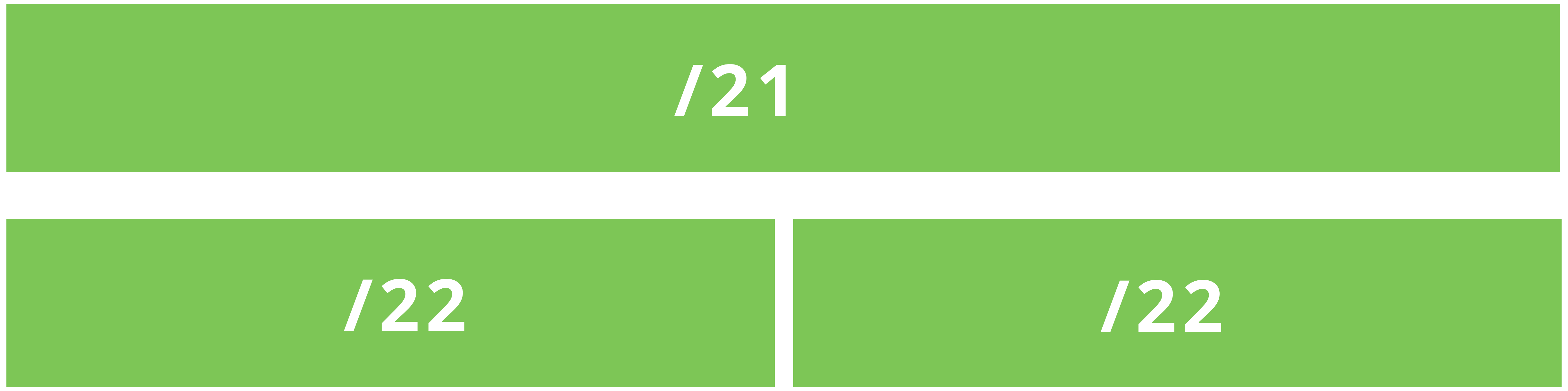
Prefix	193.0.0.0/21
Max Length	/22
Origin AS	AS3333

Max-Length

AS3333 has an IP address allocation

AS3333 creates this ROA

According to ROA;



/21

/22 /22

193.0.0.0/21

ROA

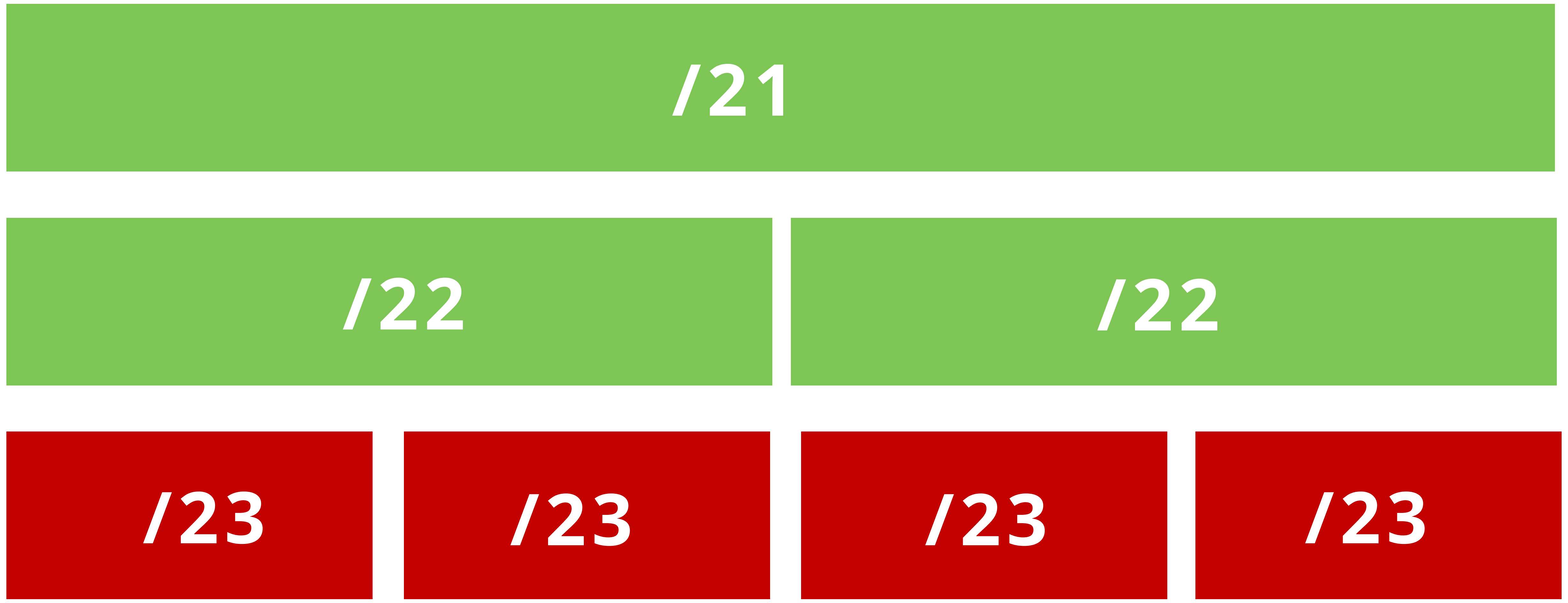
Prefix	193.0.0.0/21
Max Length	/22
Origin AS	AS3333

Max-Length

AS3333 has an IP address allocation

AS3333 creates this ROA

According to ROA;



/21

/22 /22

/23 /23 /23 /23

193.0.0.0/21

ROA

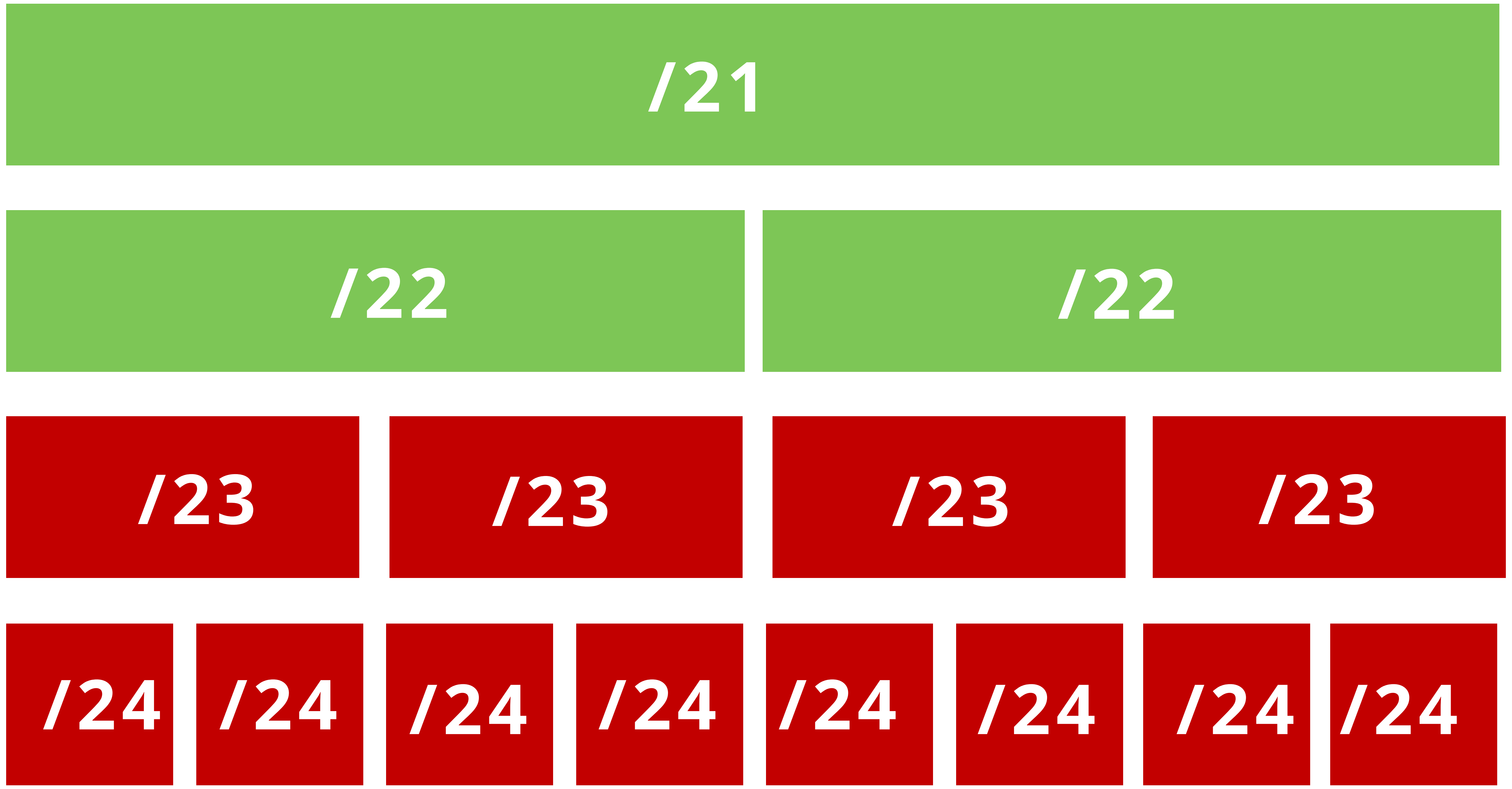
Prefix	**193.0.0.0/21**
Max Length	**/22**
Origin AS	**AS3333**

Max-Length

AS3333 has an IP address allocation

AS3333 creates this ROA

According to ROA;



🟩 /21

🟩 /22 🟩 /22

🟥 /23 🟥 /23 🟥 /23 🟥 /23

🟥 /24 🟥 /24 🟥 /24 🟥 /24 🟥 /24 🟥 /24 🟥 /24 🟥 /24

193.0.0.0/21

ROA

Prefix	193.0.0.0/21
Max Length	/22
Origin AS	AS3333

Max-Length

AS3333 has an IP address allocation

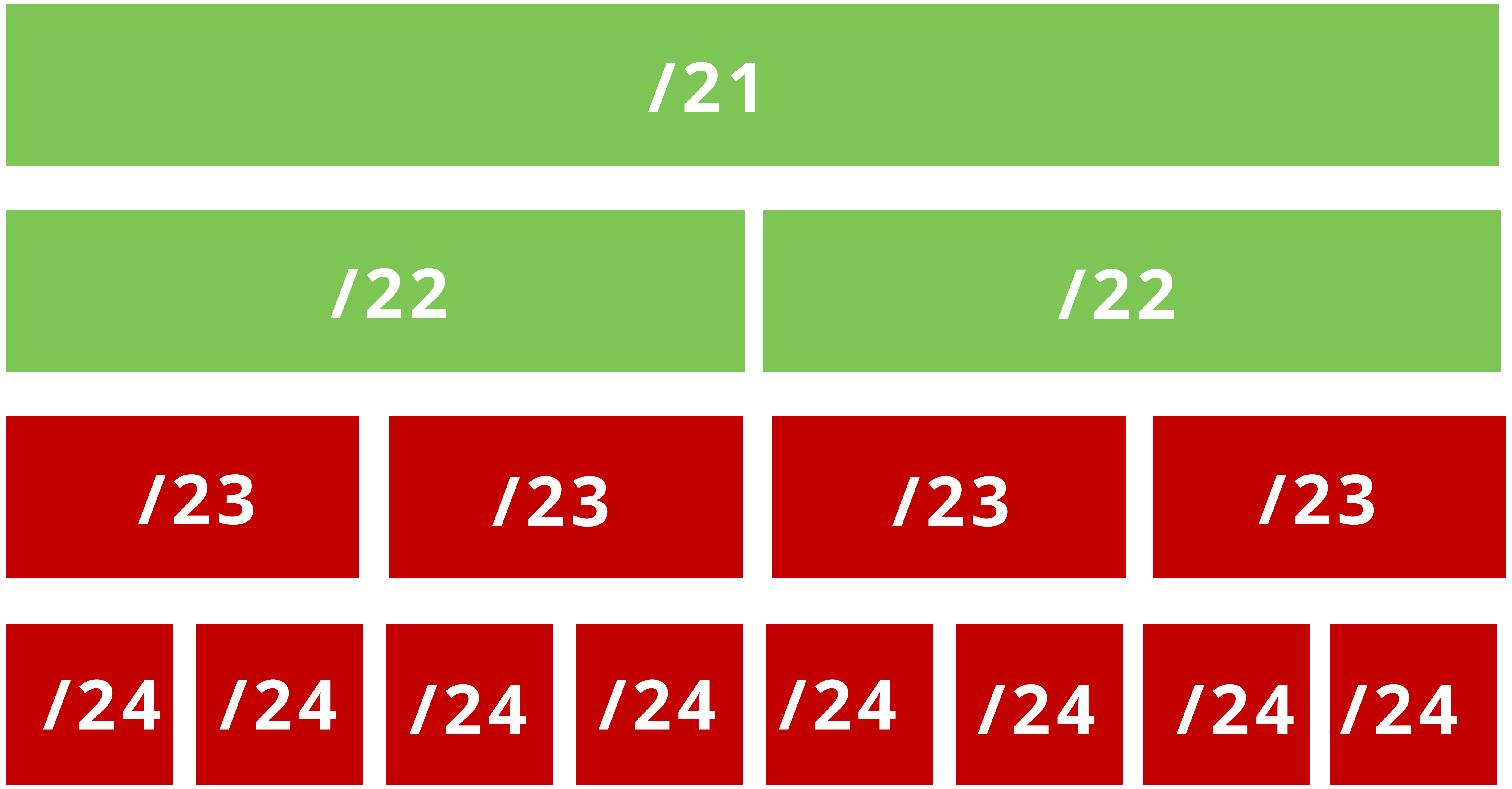
193.0.0.0/21

AS3333 creates this ROA

ROA

Prefix	193.0.0.0/21
Max Length	/22
Origin AS	AS3333

According to ROA;



/21

/22 /22

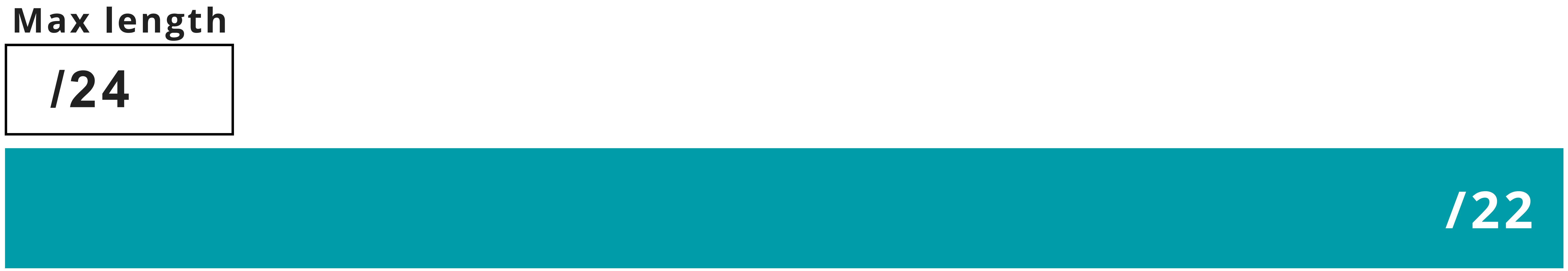
/23 /23 /23 /23

/24 /24 /24 /24 /24 /24 /24 /24

Any more specific announcements are unauthorised by the ROA

How should we use max-length?

Case 1: You create a single ROA authorising the entire /22



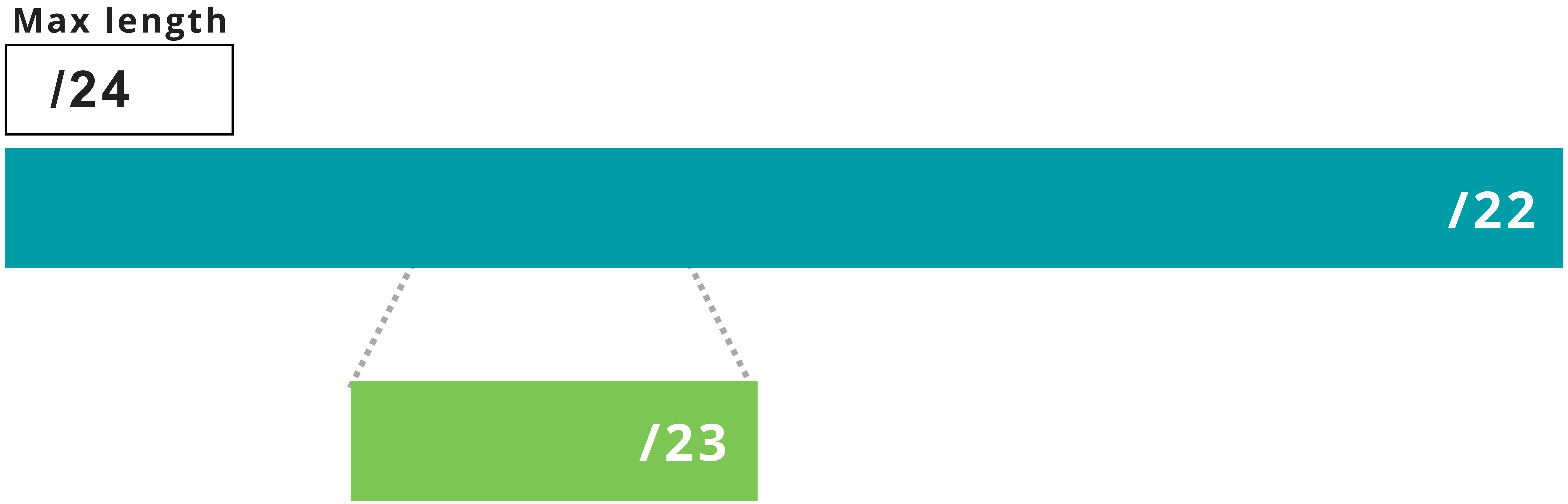
Max length

/24

/22

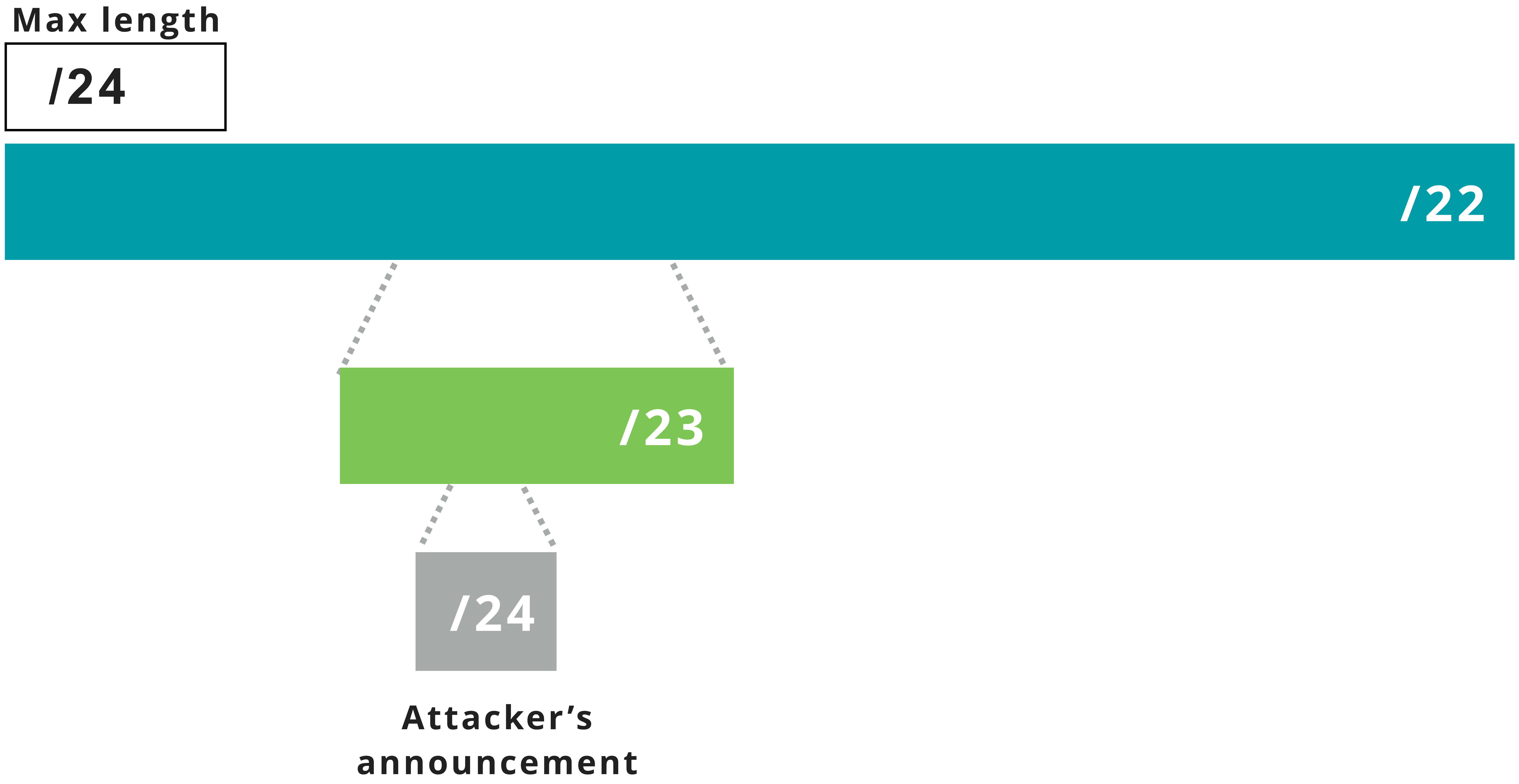
How should we use max-length?

Case 1: You create a single ROA authorising the entire /22



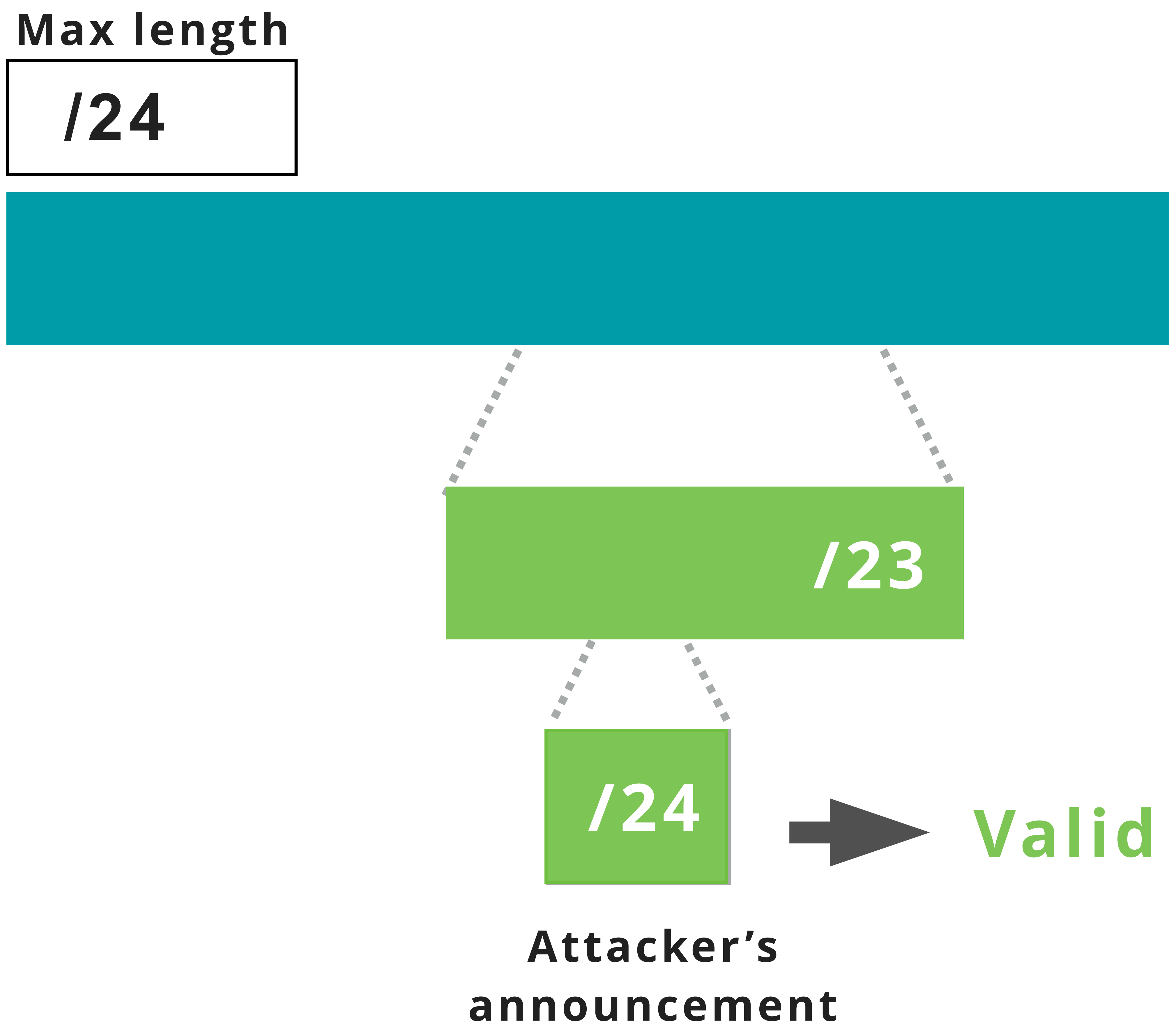
How should we use max-length?

Case 1: You create a single ROA authorising the entire /22



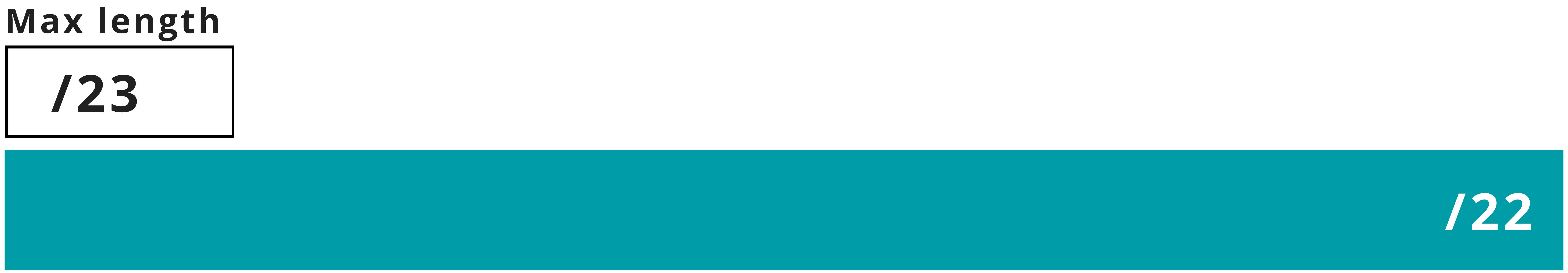
How should we use max-length?

Case 1: You create a single ROA authorising the entire /22



How should we use max-length?

Case 2: You create ROA only for your BGP announcements



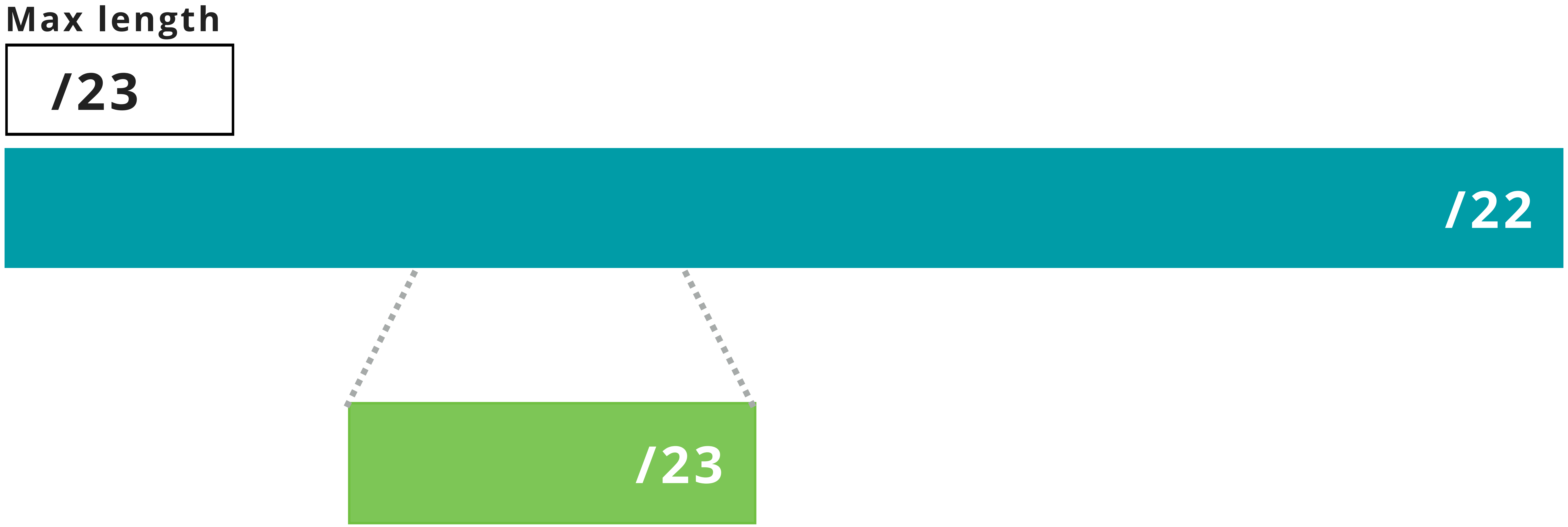
Max length

/23

/22

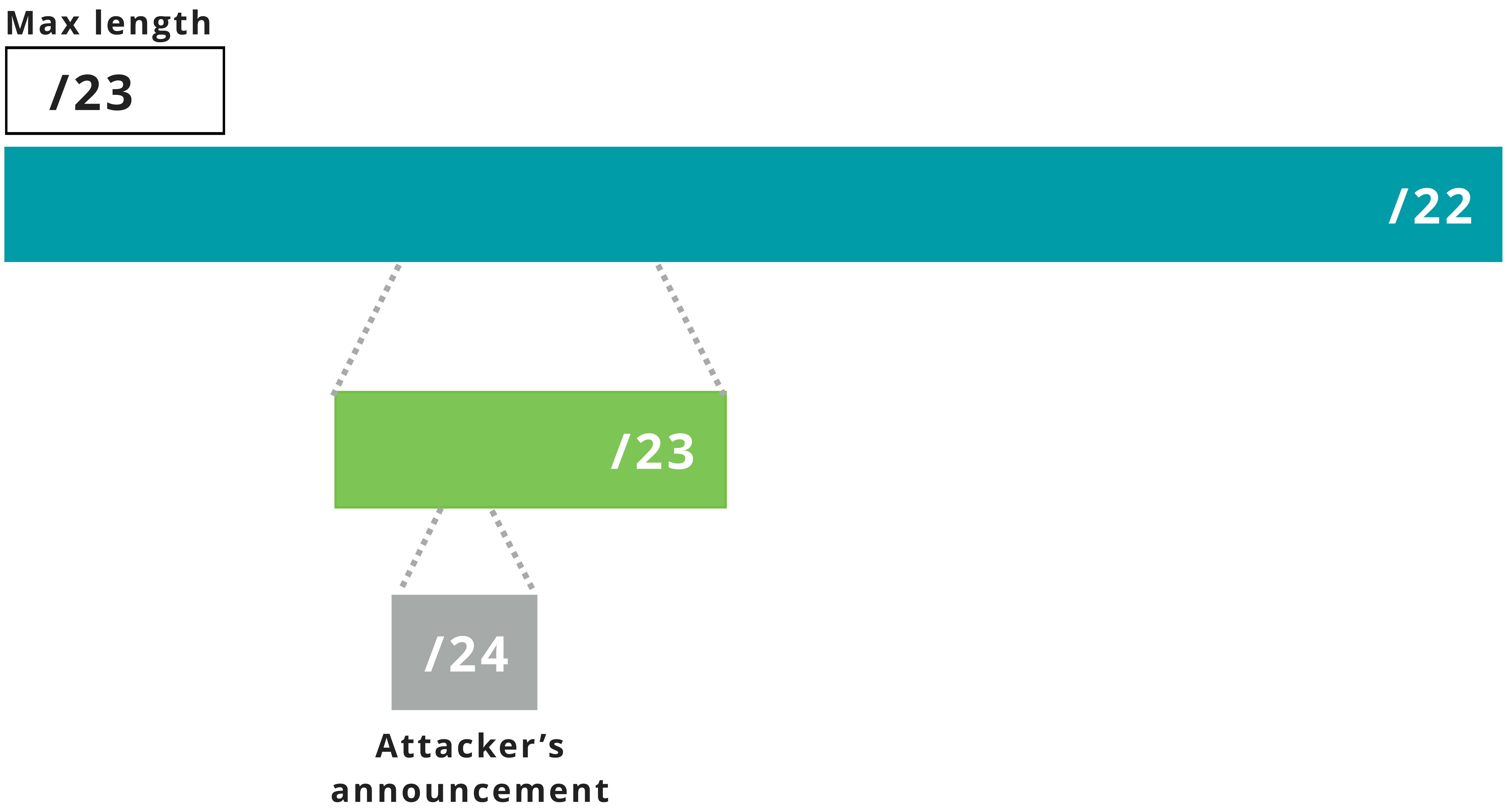
How should we use max-length?

Case 2: You create ROA only for your BGP announcements



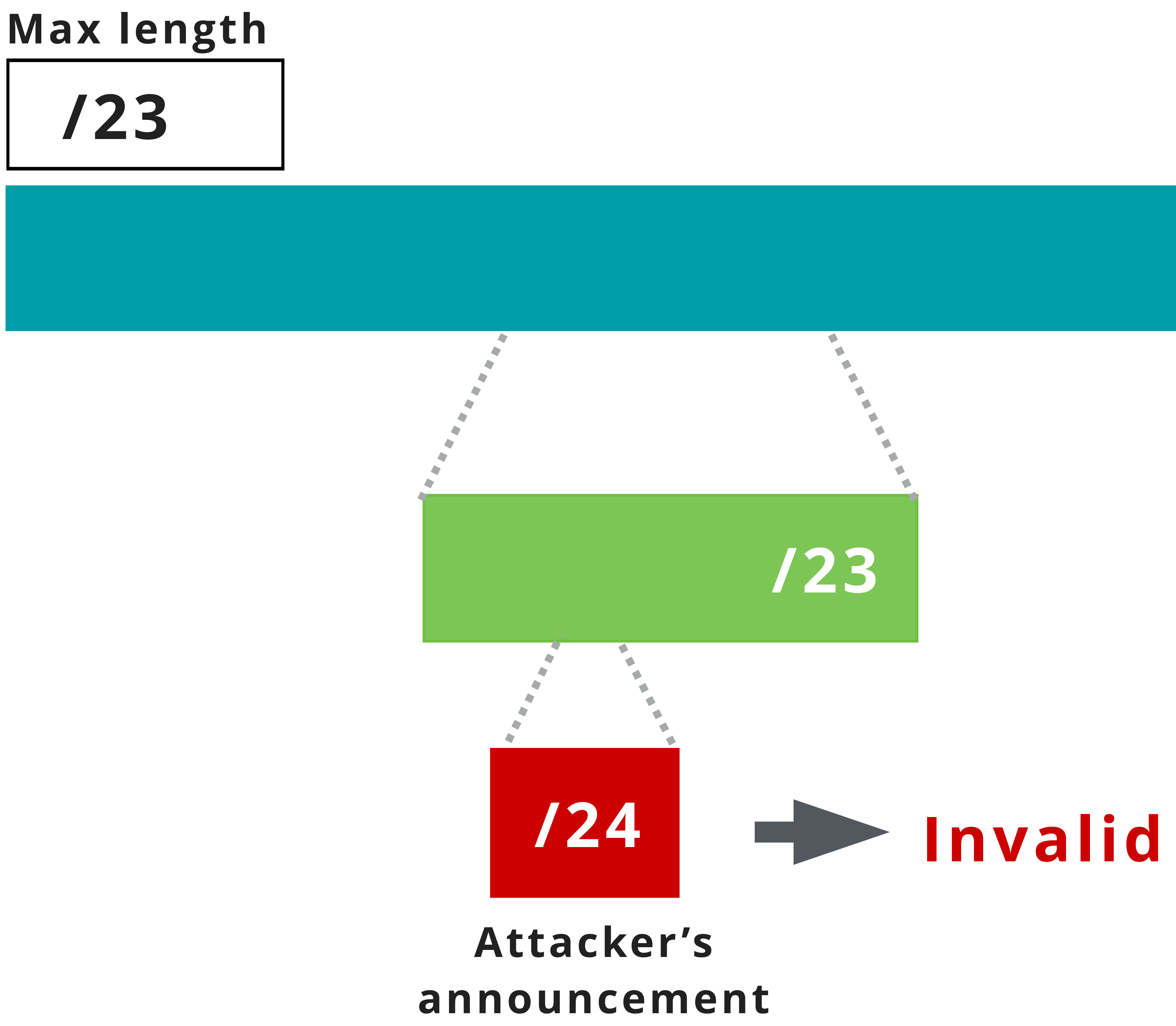
How should we use max-length?

Case 2: You create ROA only for your BGP announcements



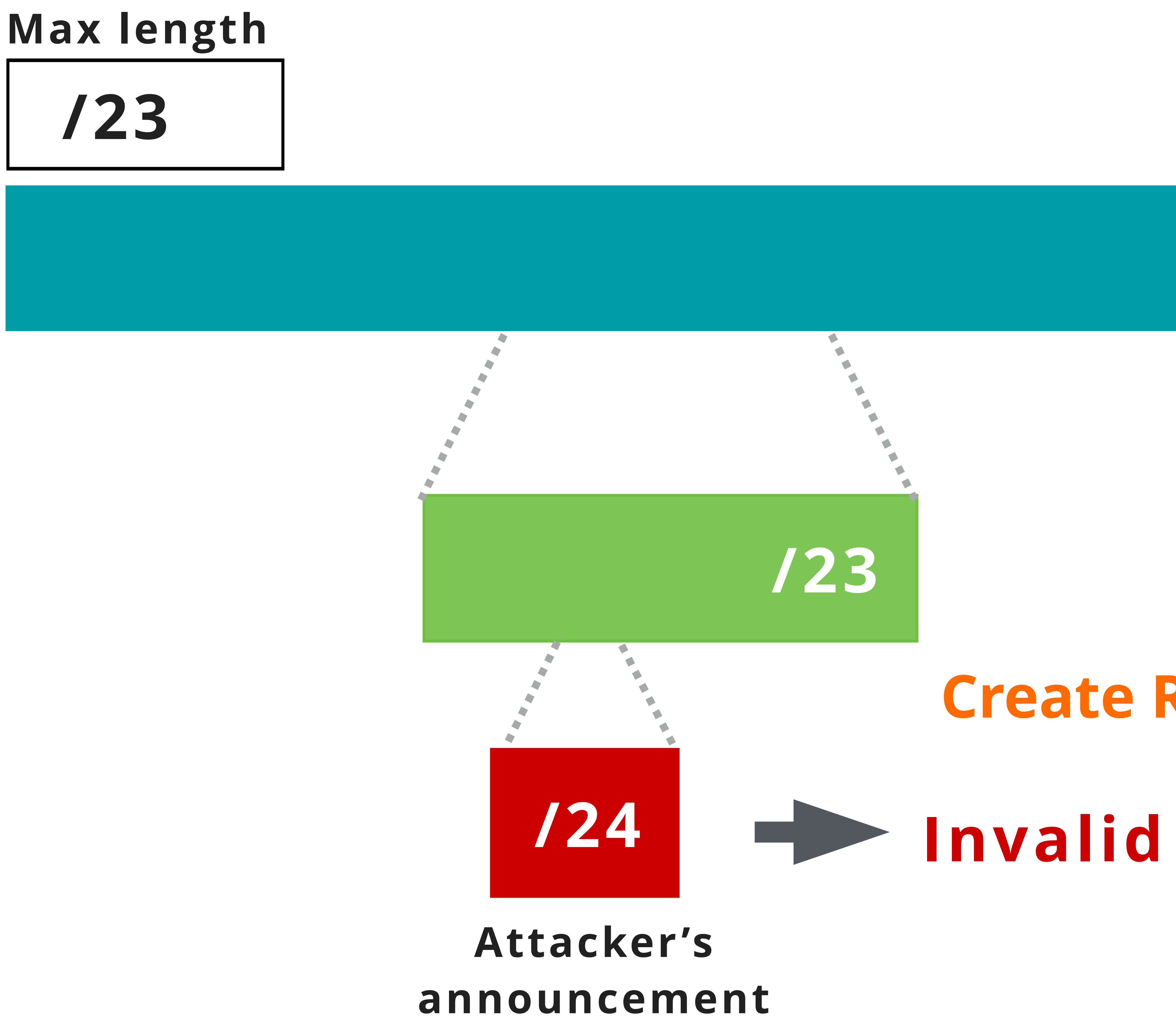
How should we use max-length?

Case 2: You create ROA only for your BGP announcements



How should we use max-length?

Case 2: You create ROA only for your BGP announcements



Create ROAs only for your BGP announcements!

Take the poll!

Which information is correct about **max-length?**

Choose all the correct answers.

1 min.

Take the poll!

According to this ROA, which announcements will be considered **valid** and **accepted** by the router?

ROA

Prefix: 193.0.24.0/23
Origin: AS65530
Max-length: /24

1 min.

How to create a ROA?

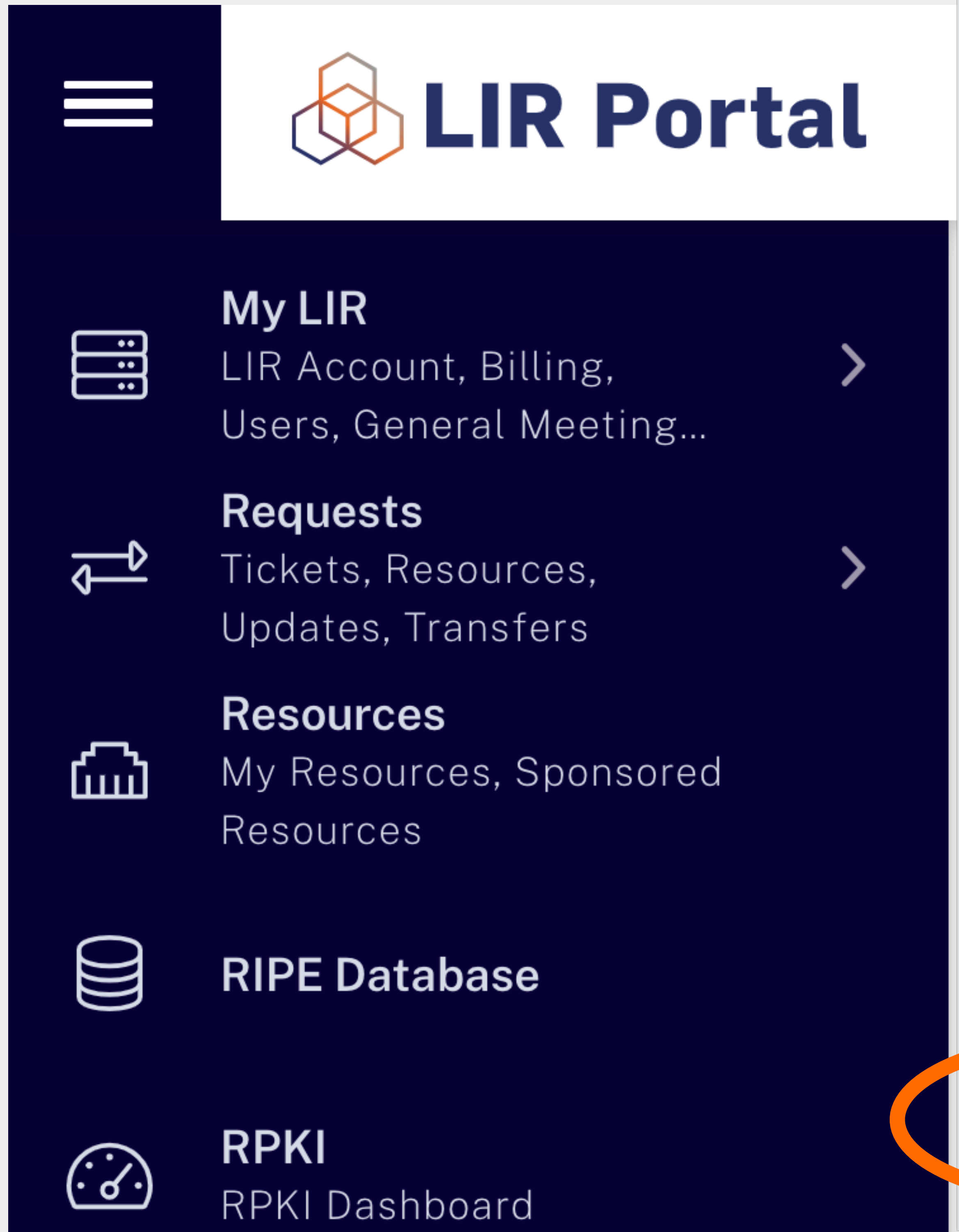
1 Login to LIR Portal (my.ripe.net)

2 Go to the RPKI Dashboard

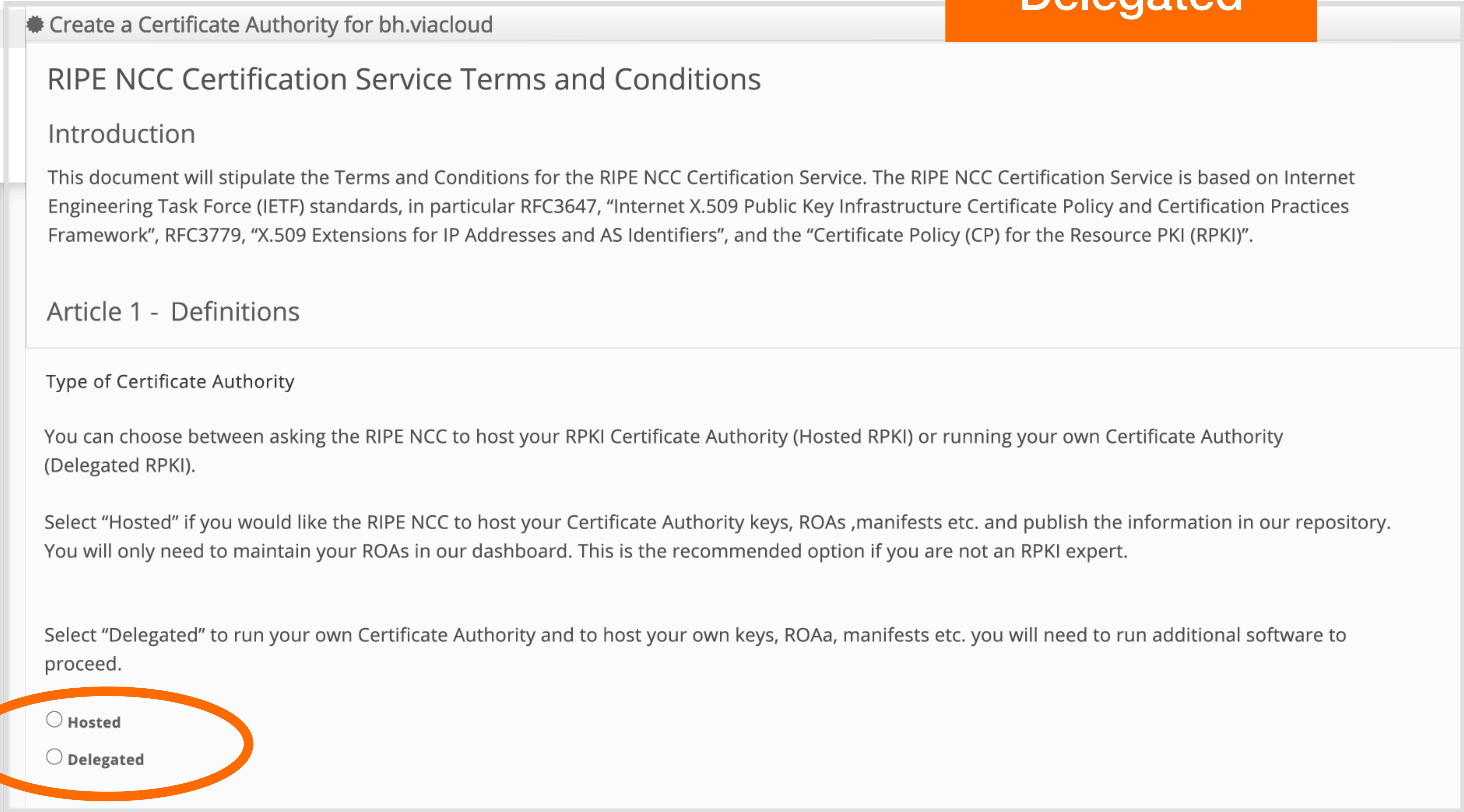
3 Choose which RPKI model to us

Hosted

Delegated



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



Create a Certificate Authority for bh.viacloud

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.

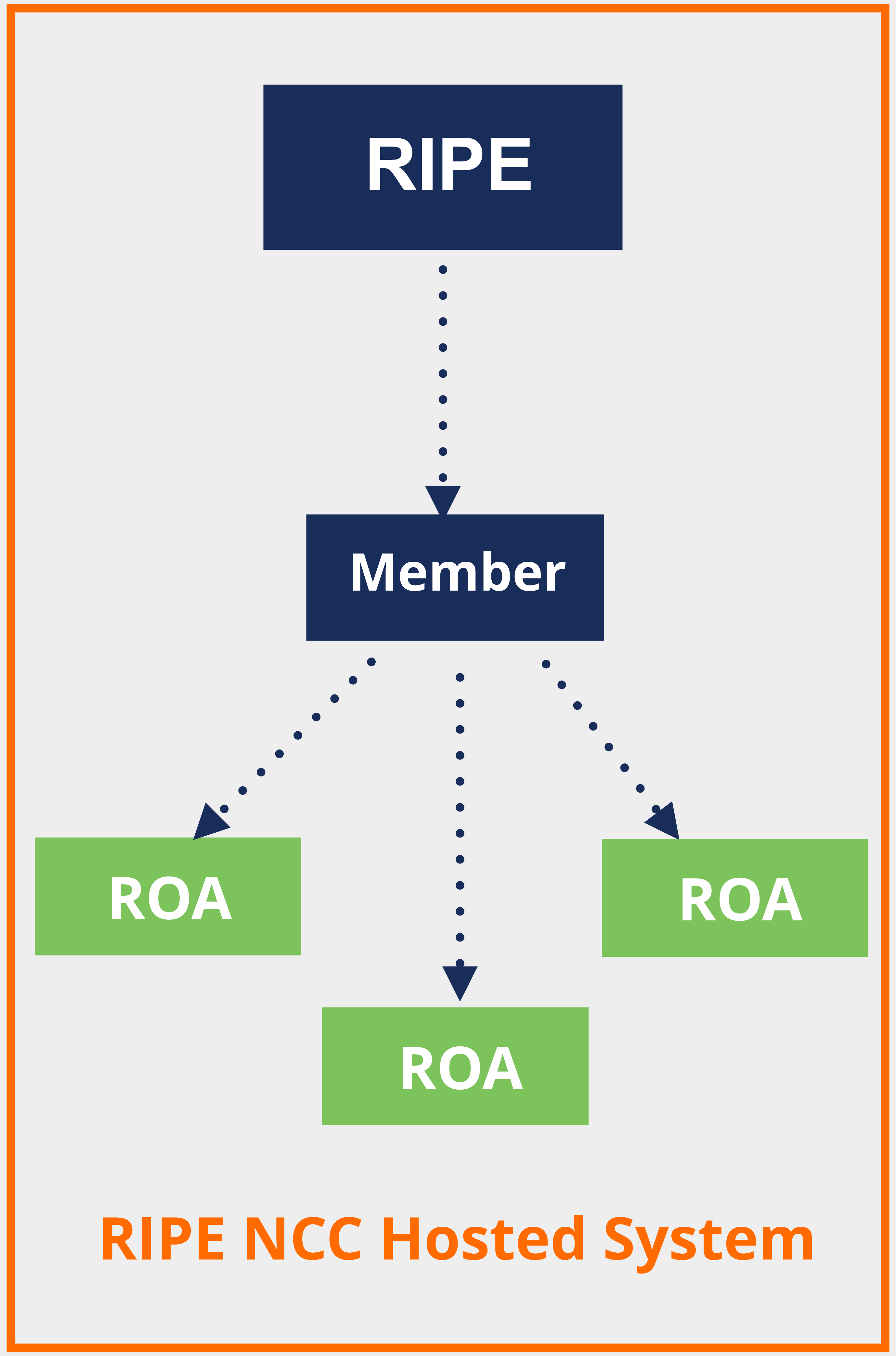
Select "Delegated" to run your own Certificate Authority and to host your own keys, ROAa, manifests etc. you will need to run additional software to proceed.

○ Hosted

○ Delegated

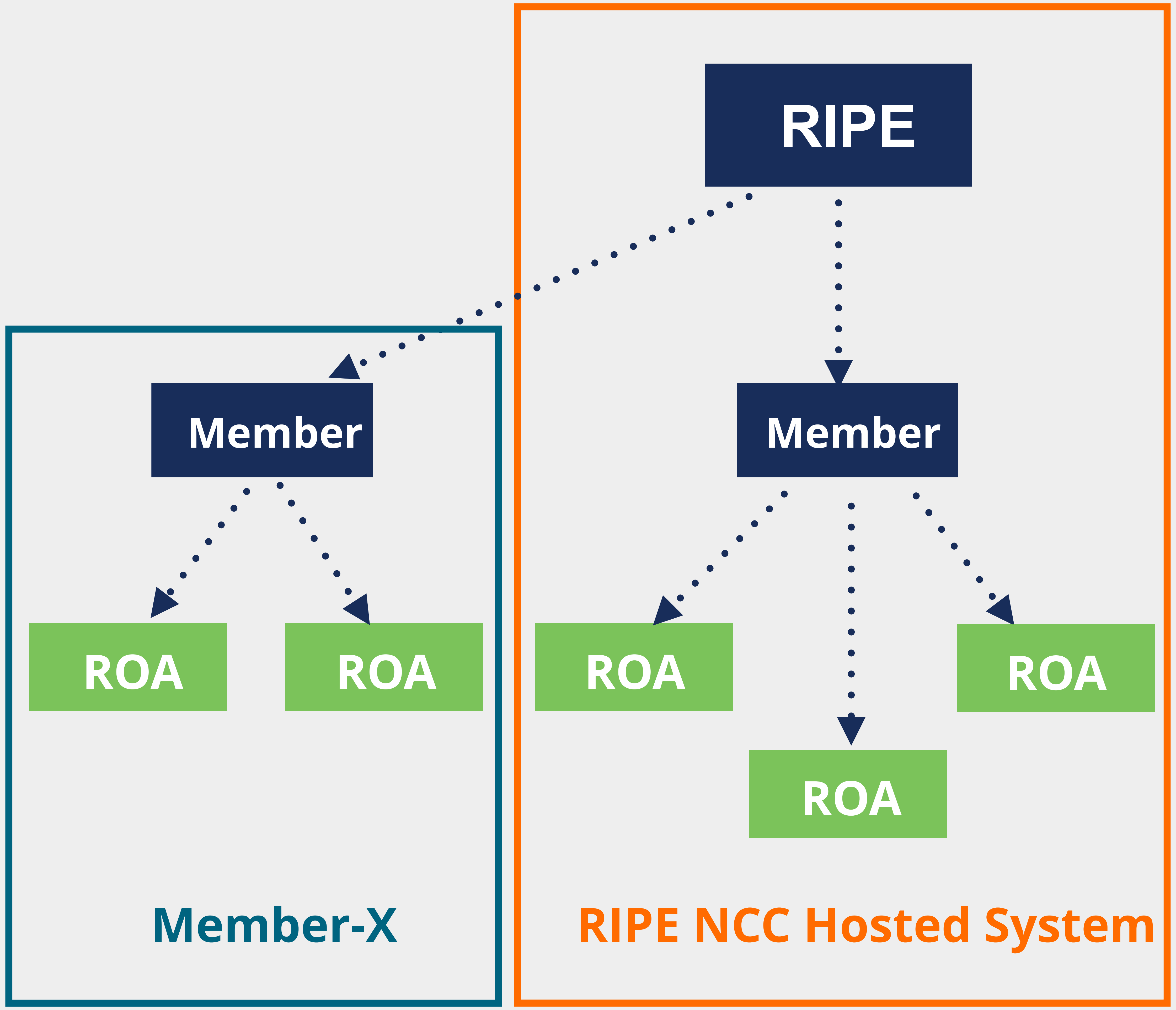
Hosted RPKI

- ROAs are created and published using the RIR member portal
- RIR hosts a CA and signs all ROAs
- Automated signing and key rollovers
- Allows LIRs focus on creating and publishing ROAs

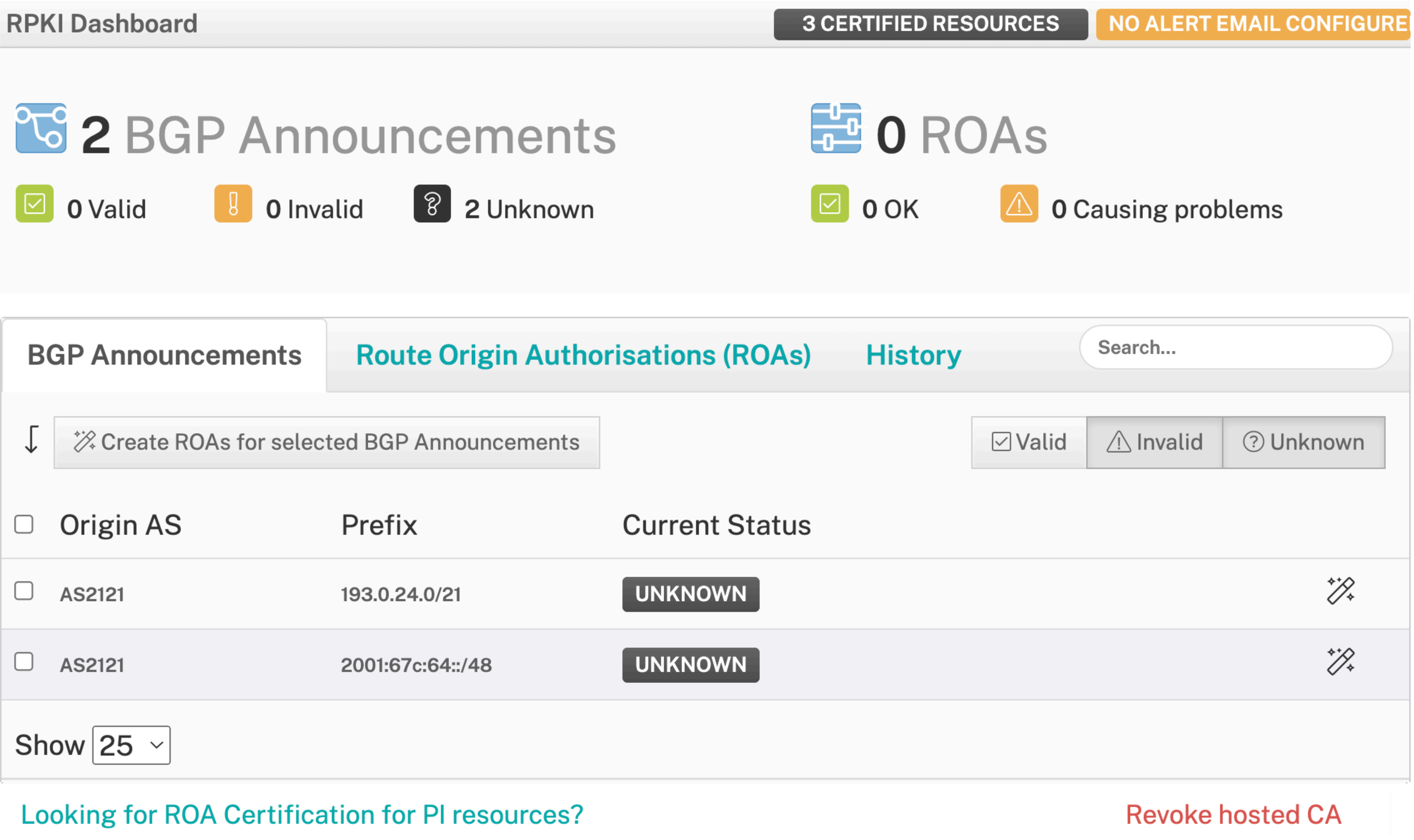


Delegated RPKI

- LIR manages full RPKI system
  - Runs its own CA, manages keys/key rollovers
  - Creates ROAs in its own platform
- LIRs ...
  - Set up connection with RIPE NCC CA
  - Generate an LIR certificate and get it signed by parent CA



RIPE NCC Hosted Solution



RPKI Dashboard

3 CERTIFIED RESOURCES

NO ALERT EMAIL CONFIGURE

2 BGP Announcements

0 Valid

0 Invalid

2 Unknown

0 ROAs

0 OK

0 Causing problems

BGP Announcements | Route Origin Authorisations (ROAs) | History

Search...

Create ROAs for selected BGP Announcements

Valid | Invalid | Unknown

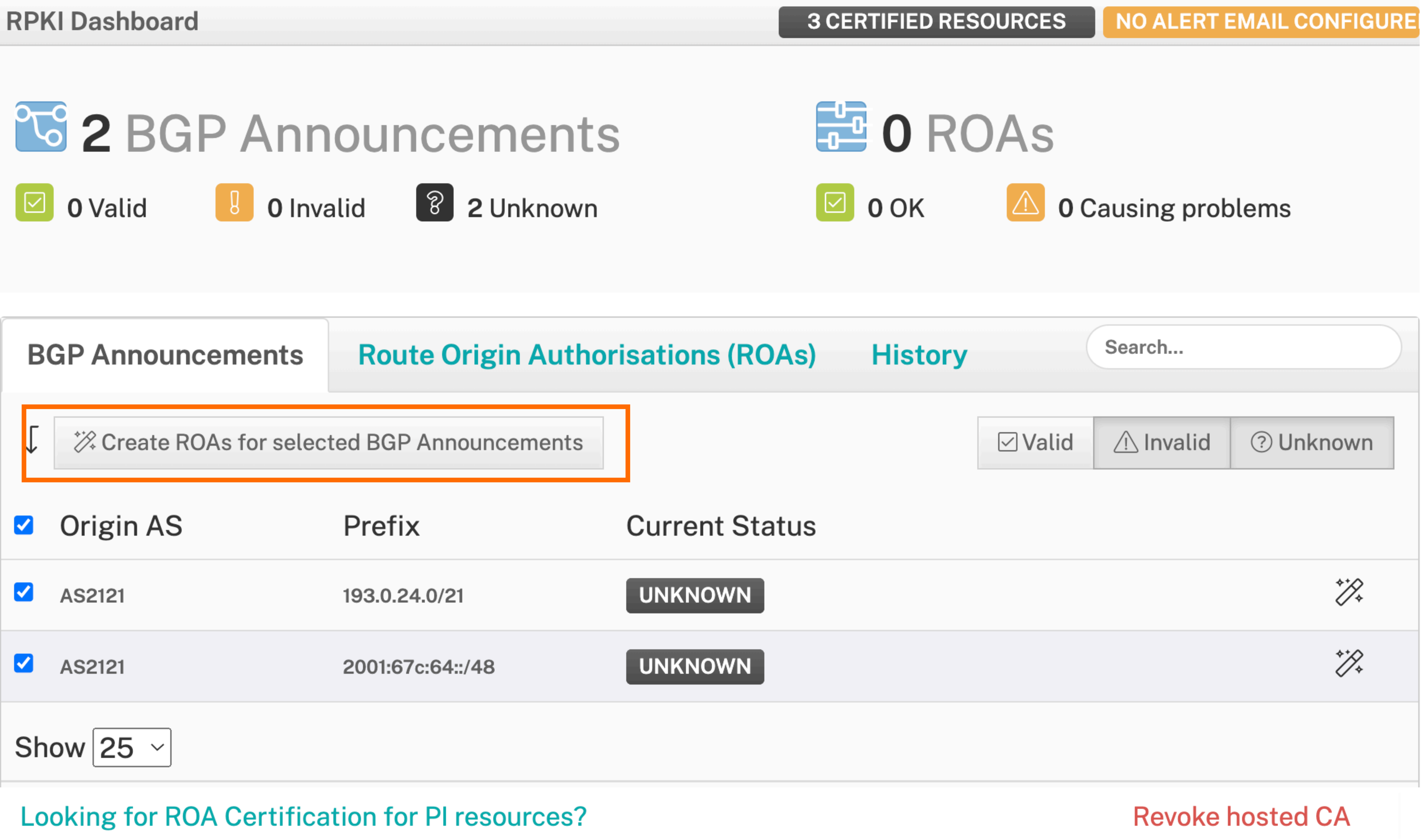
□	Origin AS	Prefix	Current Status
□	AS2121	193.0.24.0/21	UNKNOWN
□	AS2121	2001:67c:64::/48	UNKNOWN

Show 25

Looking for ROA Certification for PI resources?

Revoke hosted CA

RIPE NCC Hosted Solution



RPKI Dashboard

3 CERTIFIED RESOURCES

NO ALERT EMAIL CONFIGURE

2 BGP Announcements

☑ 0 Valid

! 0 Invalid

? 2 Unknown

0 ROAs

☑ 0 OK

⚠ 0 Causing problems

BGP Announcements | Route Origin Authorisations (ROAs) | History | Search...

Create ROAs for selected BGP Announcements

☑ Valid | ⚠ Invalid | ? Unknown

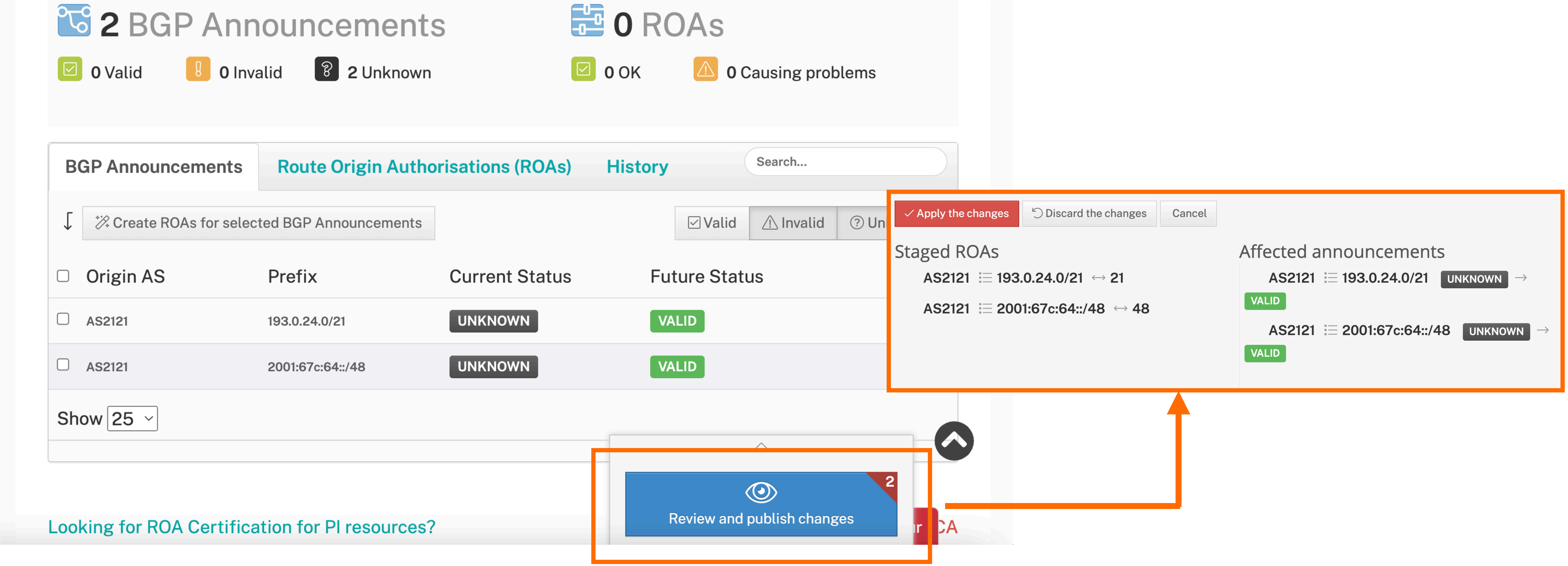
☑	Origin AS	Prefix	Current Status
☑	AS2121	193.0.24.0/21	UNKNOWN
☑	AS2121	2001:67c:64::/48	UNKNOWN

Show 25

Looking for ROA Certification for PI resources?

Revoke hosted CA

RIPE NCC Hosted Solution



2 BGP Announcements

☑ 0 Valid　! 0 Invalid　? 2 Unknown

0 ROAs

☑ 0 OK　⚠ 0 Causing problems

BGP Announcements
Route Origin Authorisations (ROAs)
History
Search...
Create ROAs for selected BGP Announcements
Valid
Invalid
Un

□	Origin AS	Prefix	Current Status	Future Status
□	AS2121	193.0.24.0/21	UNKNOWN	VALID
□	AS2121	2001:67c:64::/48	UNKNOWN	VALID

Show 25

2
Review and publish changes
Looking for ROA Certification for PI resources?
✓ Apply the changes
Discard the changes
Cancel

Staged ROAs

AS2121 193.0.24.0/21 ↔ 21

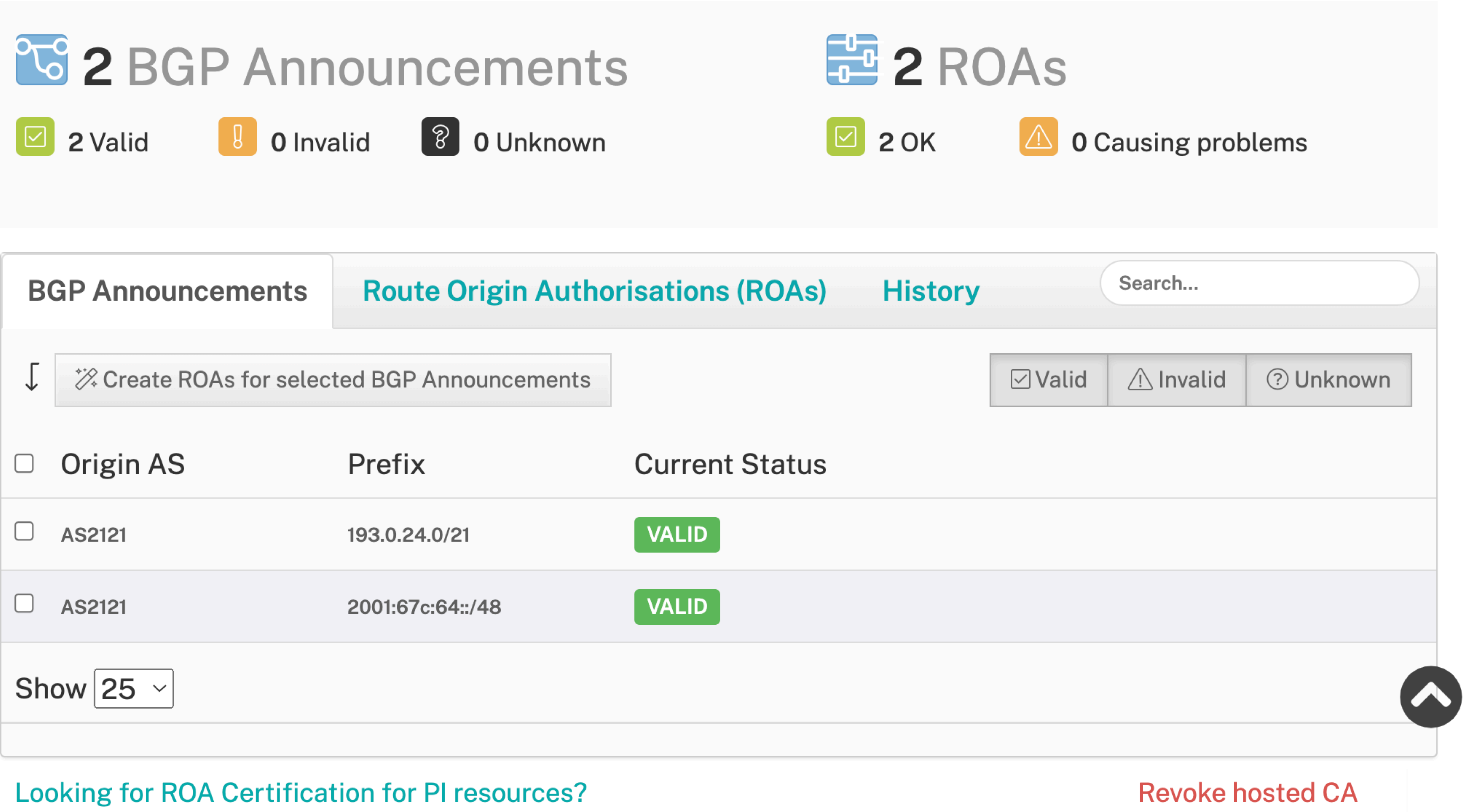
AS2121 2001:67c:64::/48 ↔ 48

Affected announcements

AS2121 193.0.24.0/21 UNKNOWN → VALID

AS2121 2001:67c:64::/48 UNKNOWN → VALID

RIPE NCC Hosted Solution



2 BGP Announcements

2 Valid 0 Invalid 0 Unknown

2 ROAs

2 OK 0 Causing problems

BGP Announcements | Route Origin Authorisations (ROAs) | History | Search...

Create ROAs for selected BGP Announcements

☑ Valid | ⚠ Invalid | ? Unknown

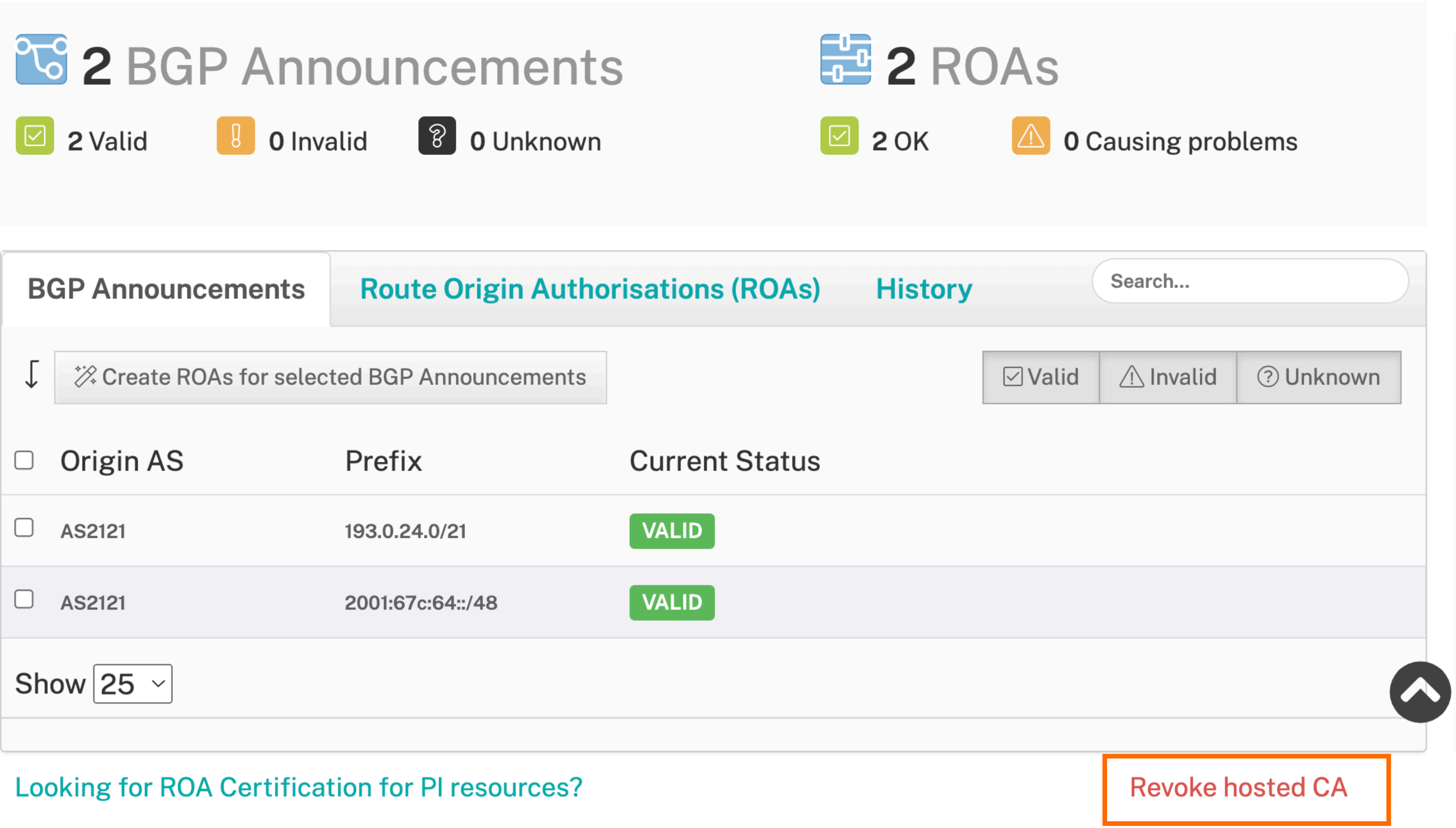
□	Origin AS	Prefix	Current Status
□	AS2121	193.0.24.0/21	VALID
□	AS2121	2001:67c:64::/48	VALID

Show 25

Looking for ROA Certification for PI resources?

Revoke hosted CA

RIPE NCC Hosted Solution



2 BGP Announcements

☑ 2 Valid   ! 0 Invalid   ? 0 Unknown

2 ROAs

☑ 2 OK   ⚠ 0 Causing problems

BGP Announcements
Route Origin Authorisations (ROAs)
History
Search...
Create ROAs for selected BGP Announcements
☑ Valid
⚠ Invalid
? Unknown

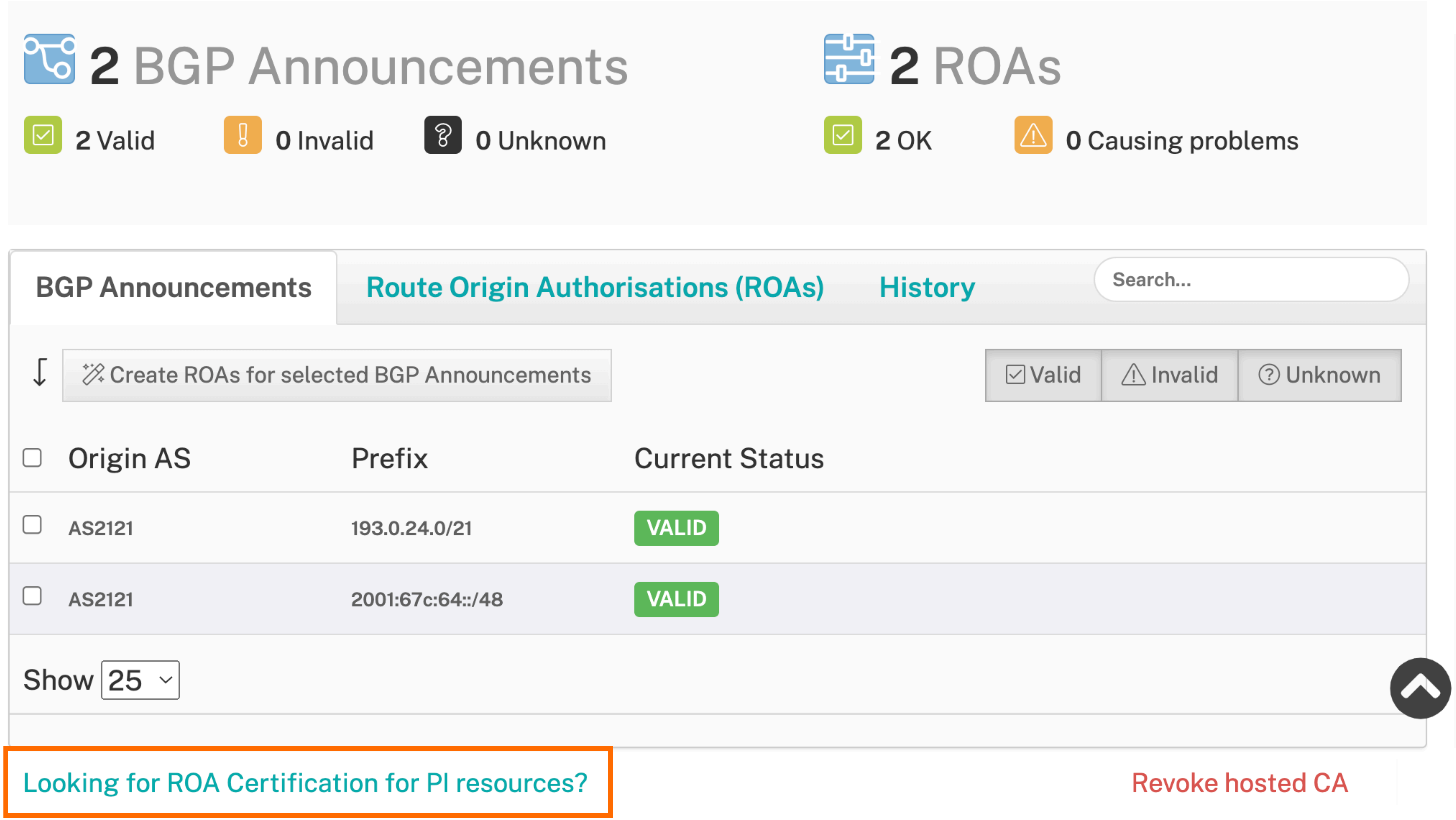
□	Origin AS	Prefix	Current Status
□	AS2121	193.0.24.0/21	VALID
□	AS2121	2001:67c:64::/48	VALID

Show 25

Looking for ROA Certification for PI resources?

Revoke hosted CA

RIPE NCC Hosted Solution



2 BGP Announcements

✓ 2 Valid ! 0 Invalid ? 0 Unknown

2 ROAs

✓ 2 OK ⚠ 0 Causing problems

BGP Announcements
Route Origin Authorisations (ROAs)
History
Search...
Create ROAs for selected BGP Announcements
☑ Valid
⚠ Invalid
? Unknown
Show 25

□	Origin AS	Prefix	Current Status
□	AS2121	193.0.24.0/21	VALID
□	AS2121	2001:67c:64::/48	VALID

Looking for ROA Certification for PI resources?

Revoke hosted CA

Take the poll!

What are the advantages of using **hosted RPKI**?

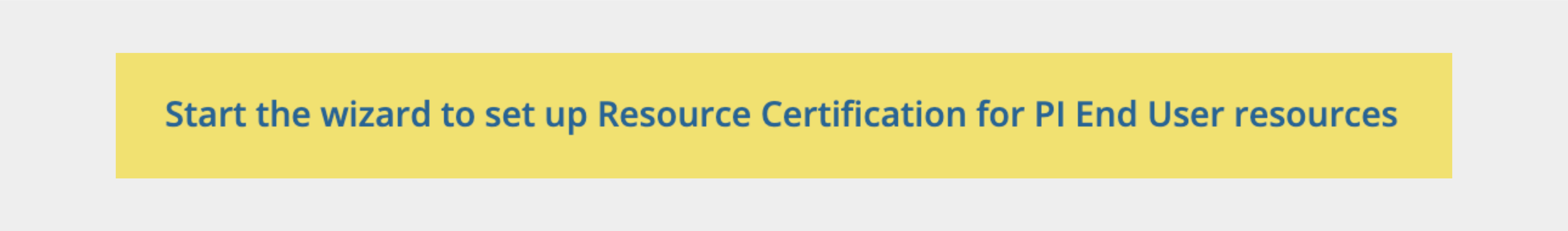
Please choose all that apply.

1 min.

Certifying PI Resources

Requested and managed by PI End User or by Sponsoring LIR

1. Complete the wizard successfully


Start the wizard to set up Resource Certification for PI End User resources

2. Login to https://my.ripe.net and request a certificate
   - Sign in with your RIPE NCC Access account
3. Manage your ROAs

Questions ?

Demo!

Creating ROAs

It’s time to try this yourself!

3 min.

Connect to Localcert:

https://localcert.ripe.net/#/

Let’s take a
5 minutes
break!

WELCOME
WE ARE
OPEN
PLEASE COME IN

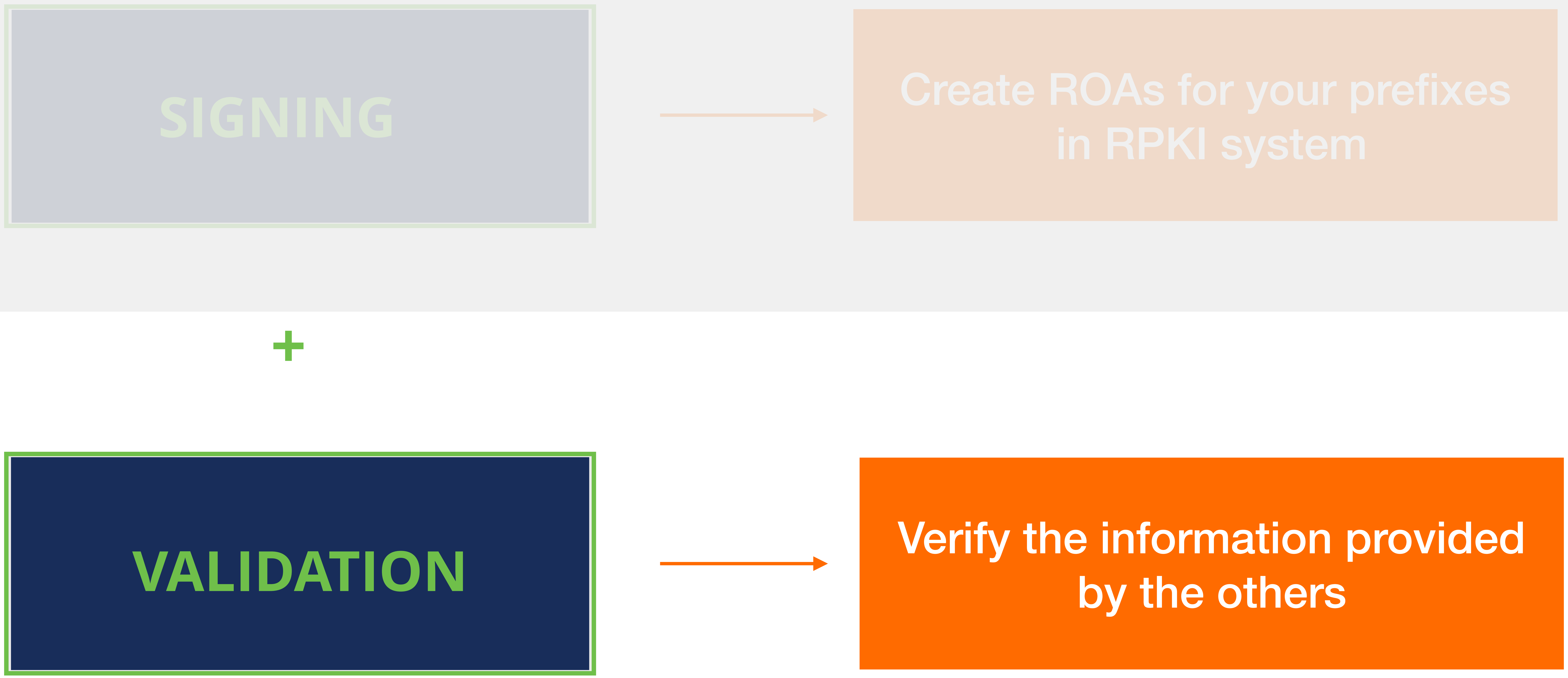
Questions

RPKI Validation

Deploying RPKI Validators

Elements of RPKI

- RPKI system consists of two parts …



SIGNING → Create ROAs for your prefixes in RPKI system

+

VALIDATION → Verify the information provided by the others

RPKI Validation

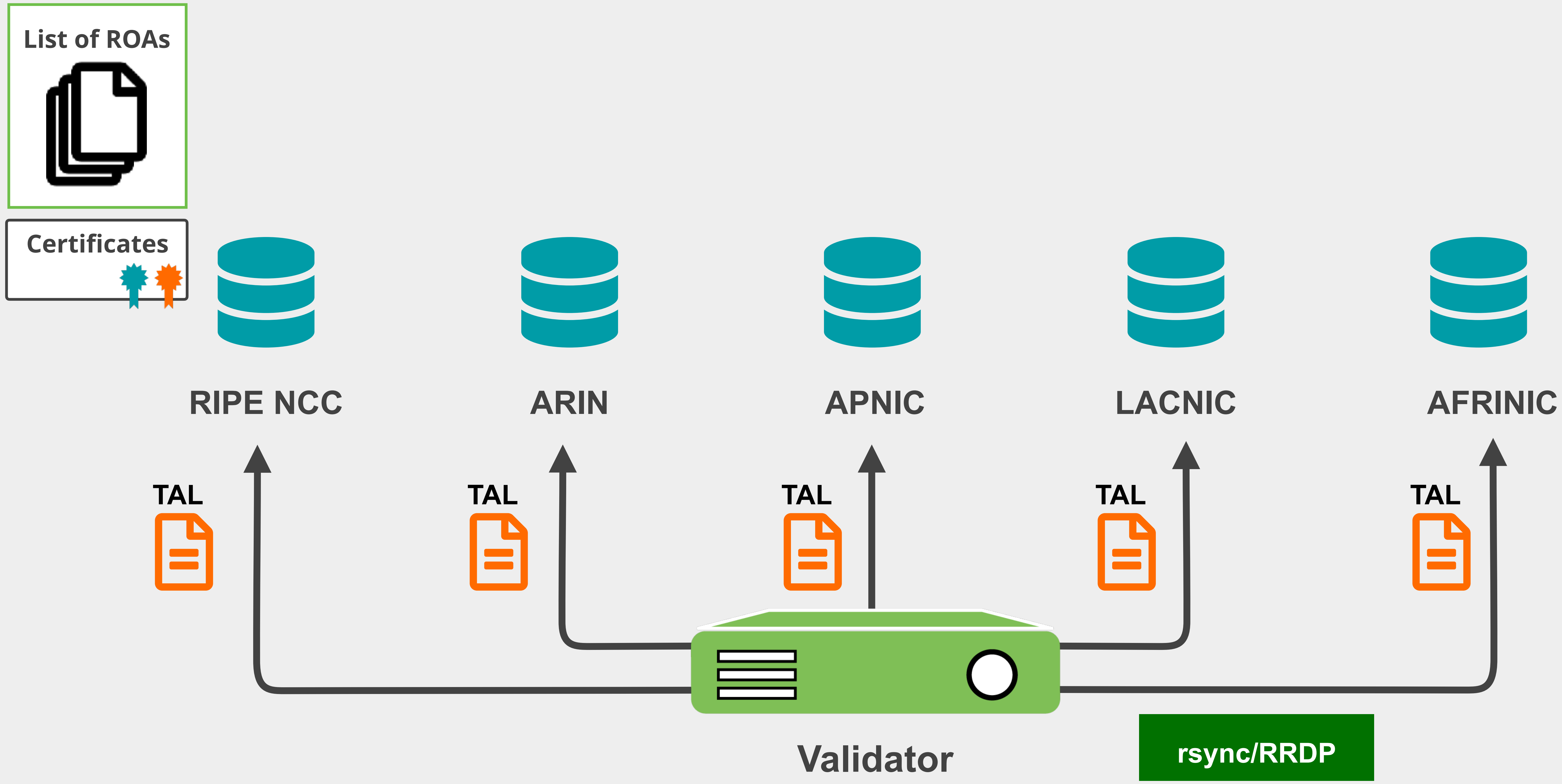
- Verifying the information provided by others
  - Proves holdership through a public key and certificate infrastructure
- In order to validate RPKI data, you need to …
  - install a validator software locally in your network

RPKI Validators

- Also known as Relying Party Software
- Downloads the RPKI repository from the RIRs
- Verifies the certificates and ROAs in the RIR repositories
- Creates a local “validated cache” with all the valid ROAs
- Talks to routers using RPKI-RTR protocol

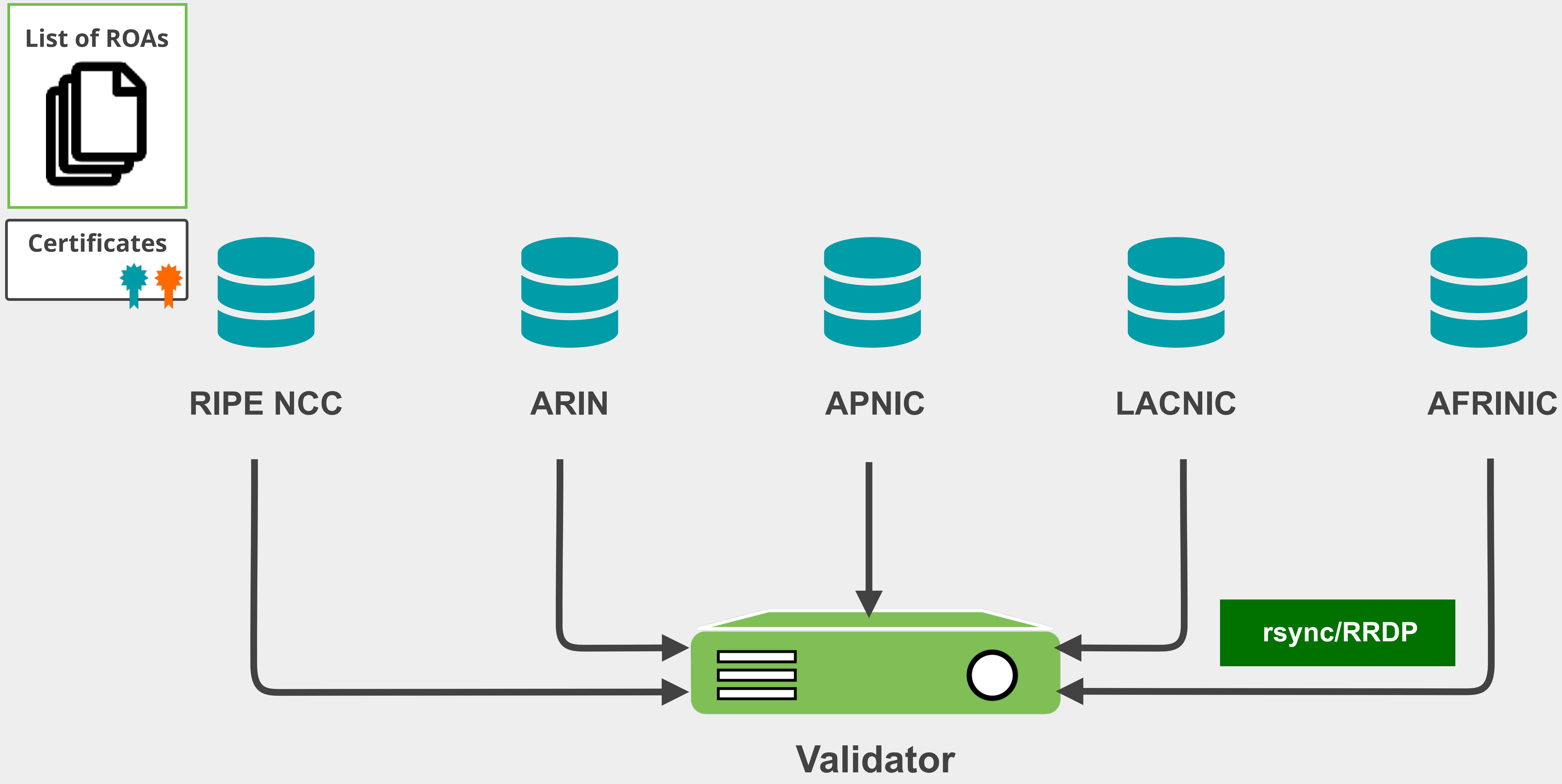
Trust Anchor Locator (TAL)

- Validator checks the information in TALs to connect to the repositories
  - URL to retrieve trust anchor certificate
  - Root’s public key



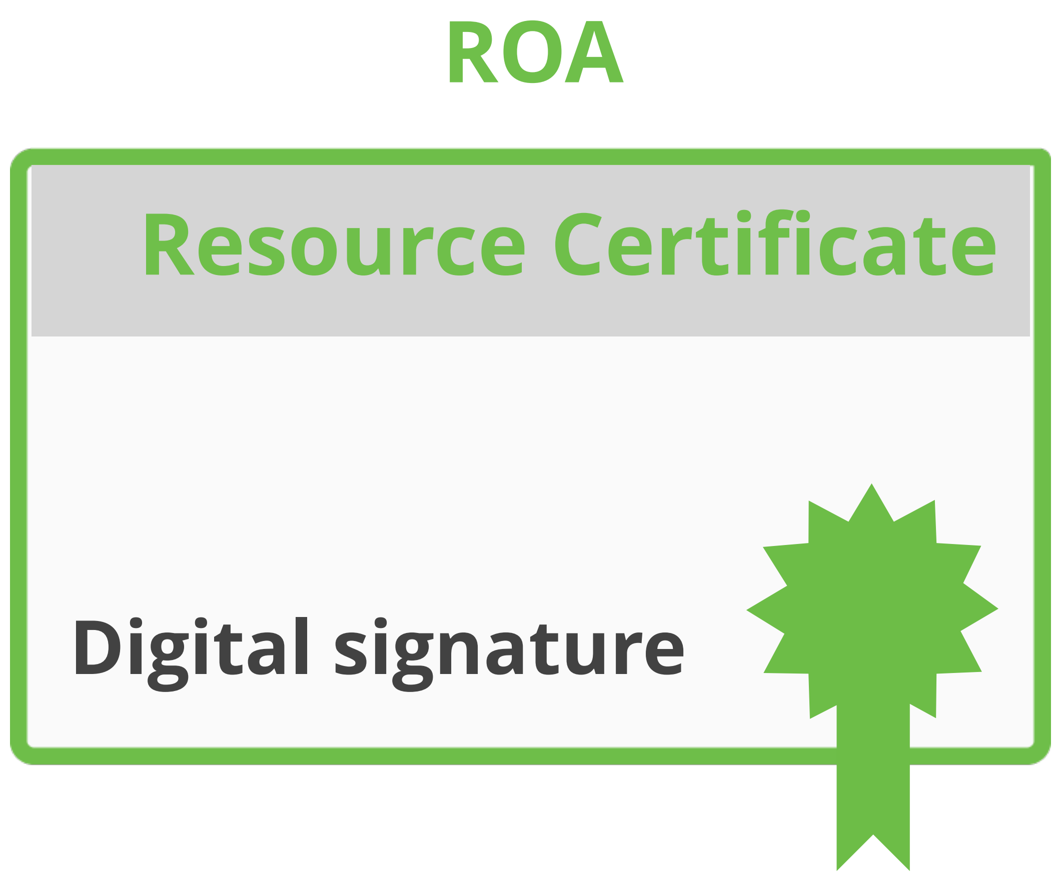
RPKI Validators

- Validator
  - Downloads the RPKI repository from the RIRs
  - Validates the chain of trust



ROA Validation Process

ROA Validation Process

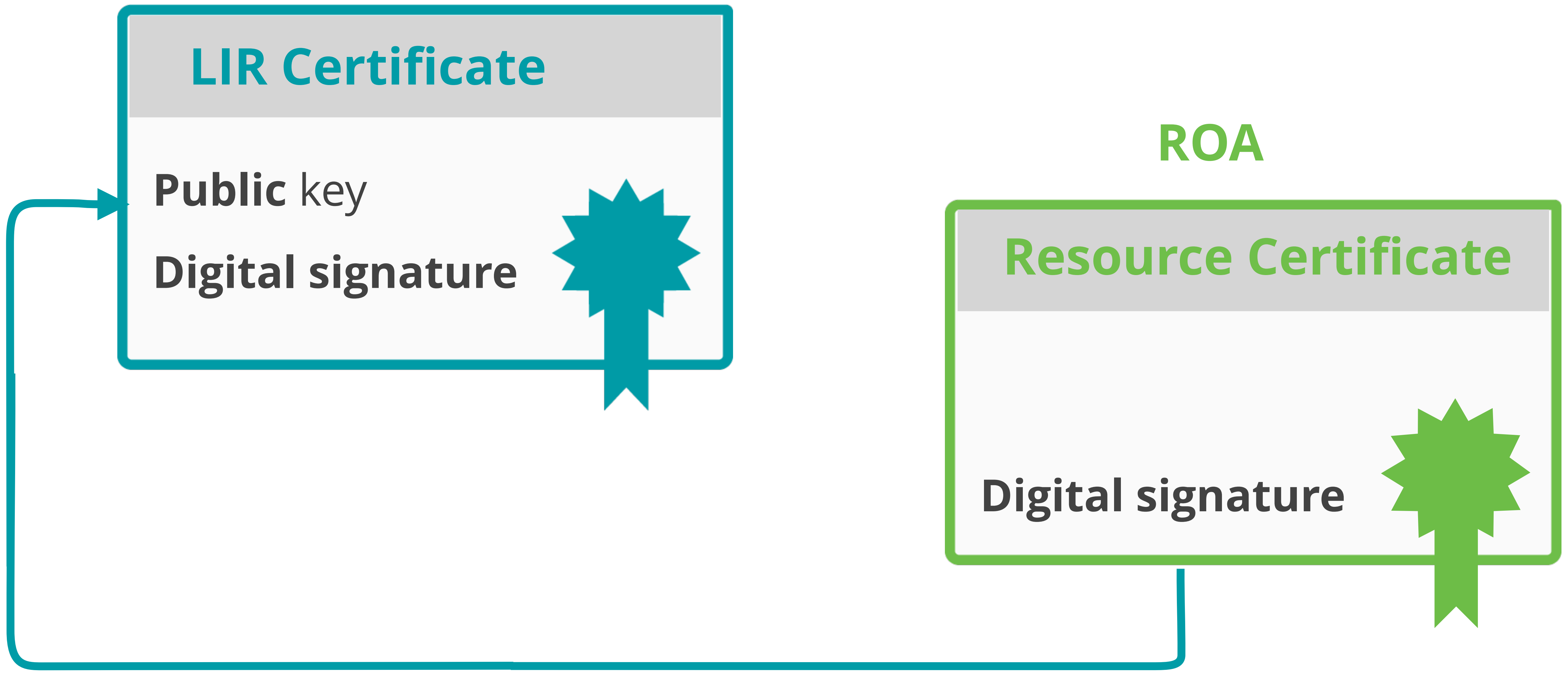


ROA

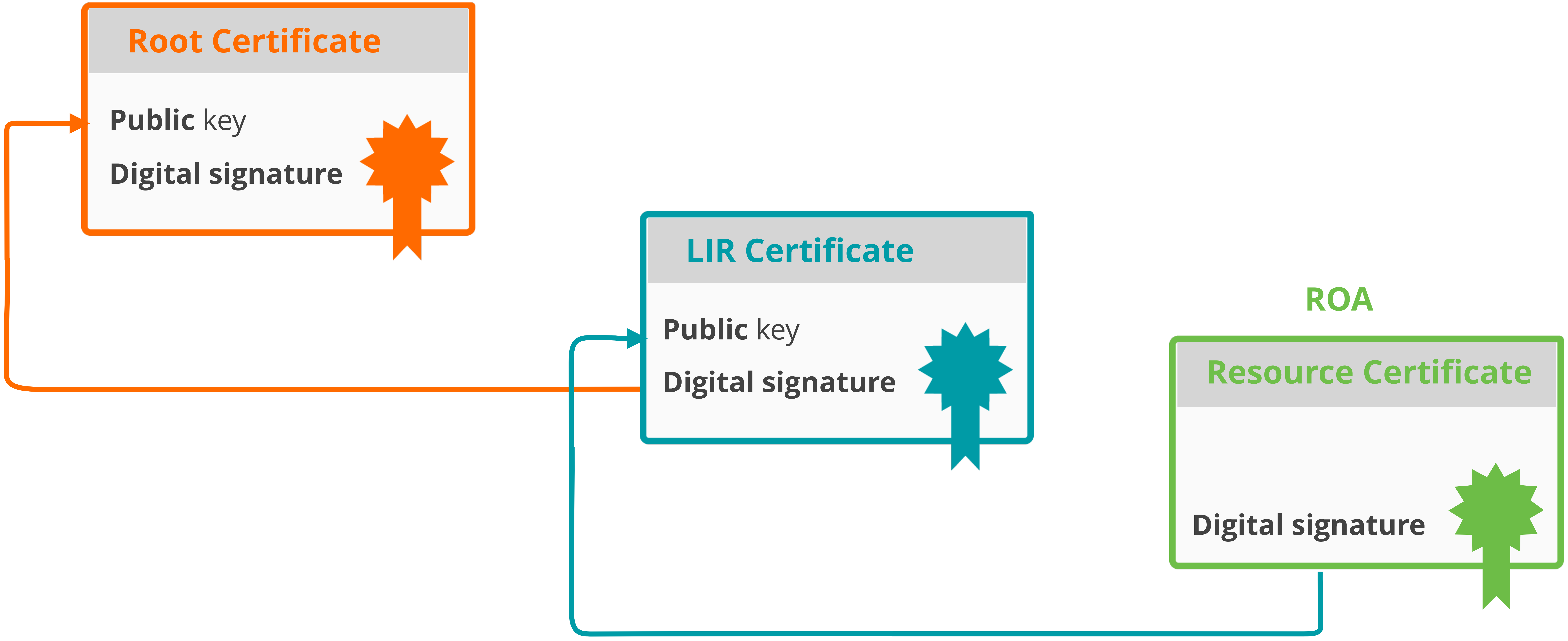
Resource Certificate

Digital signature

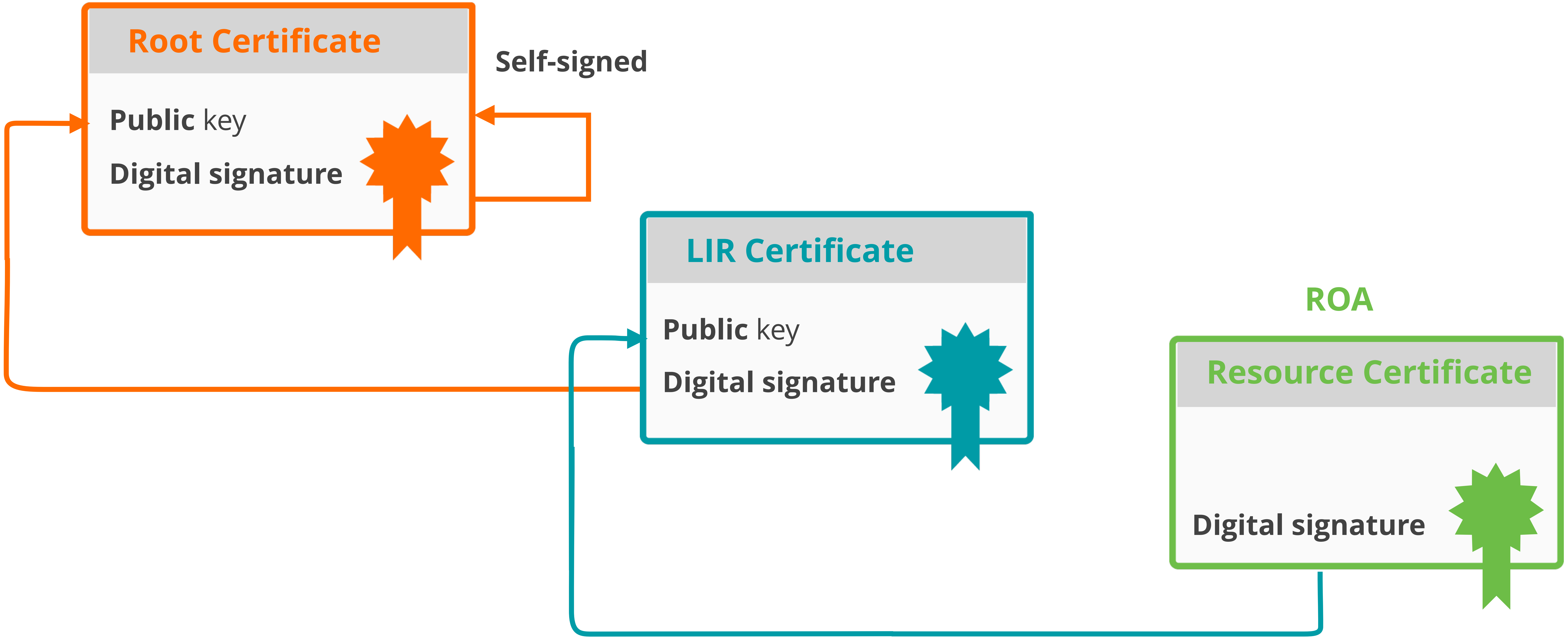
ROA Validation Process



ROA Validation Process

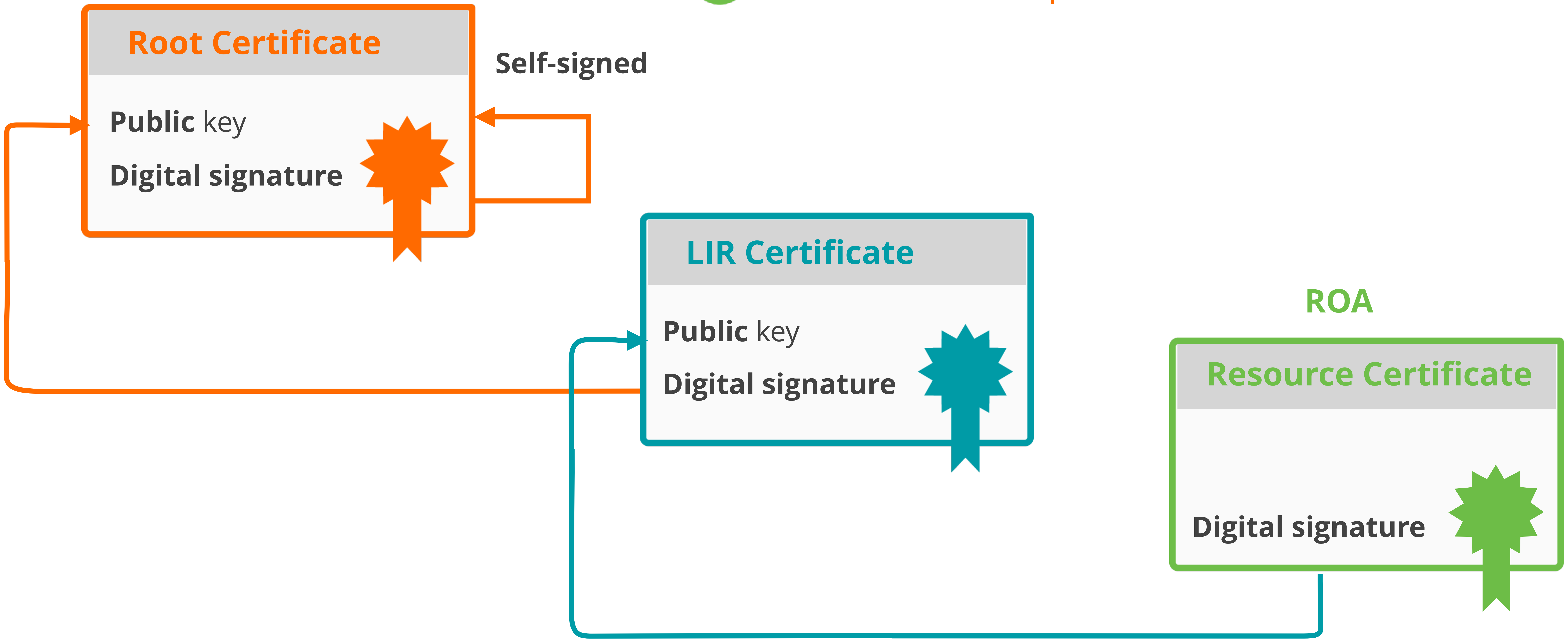


ROA Validation Process

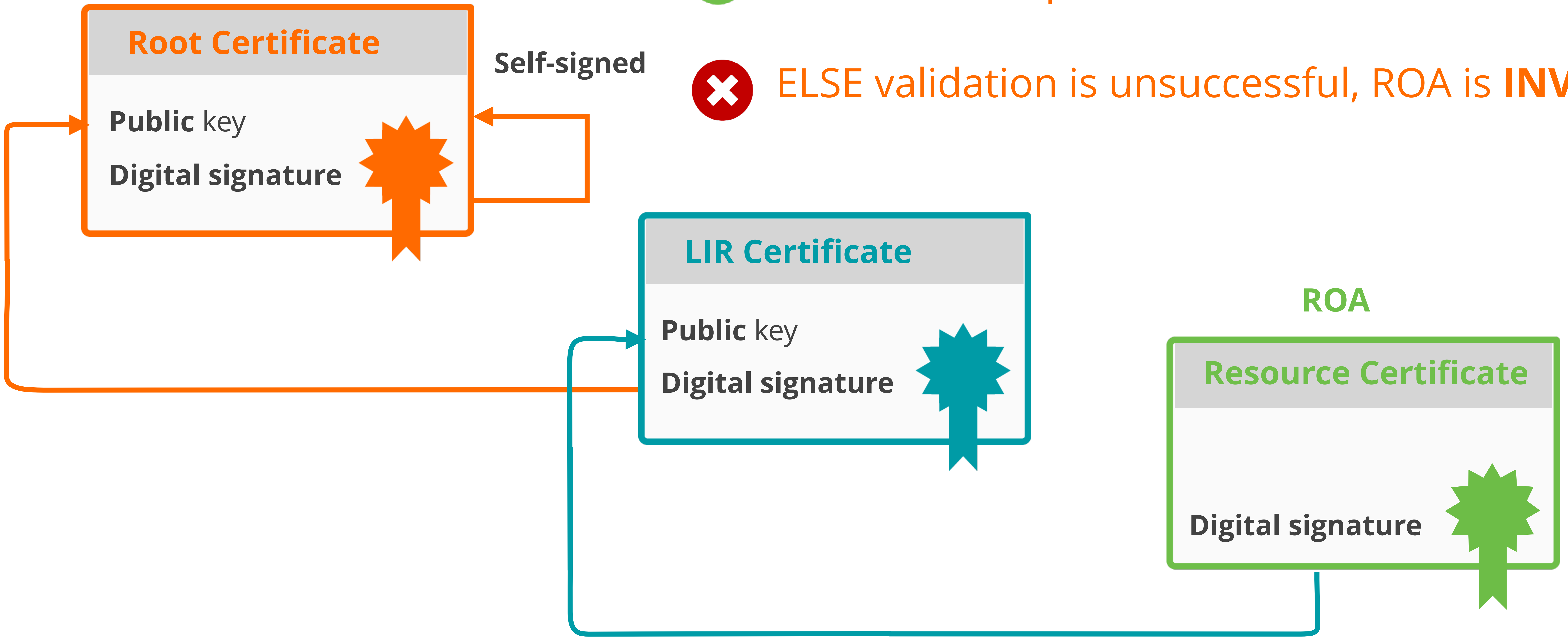


ROA Validation Process

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



ROA Validation Process



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

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

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

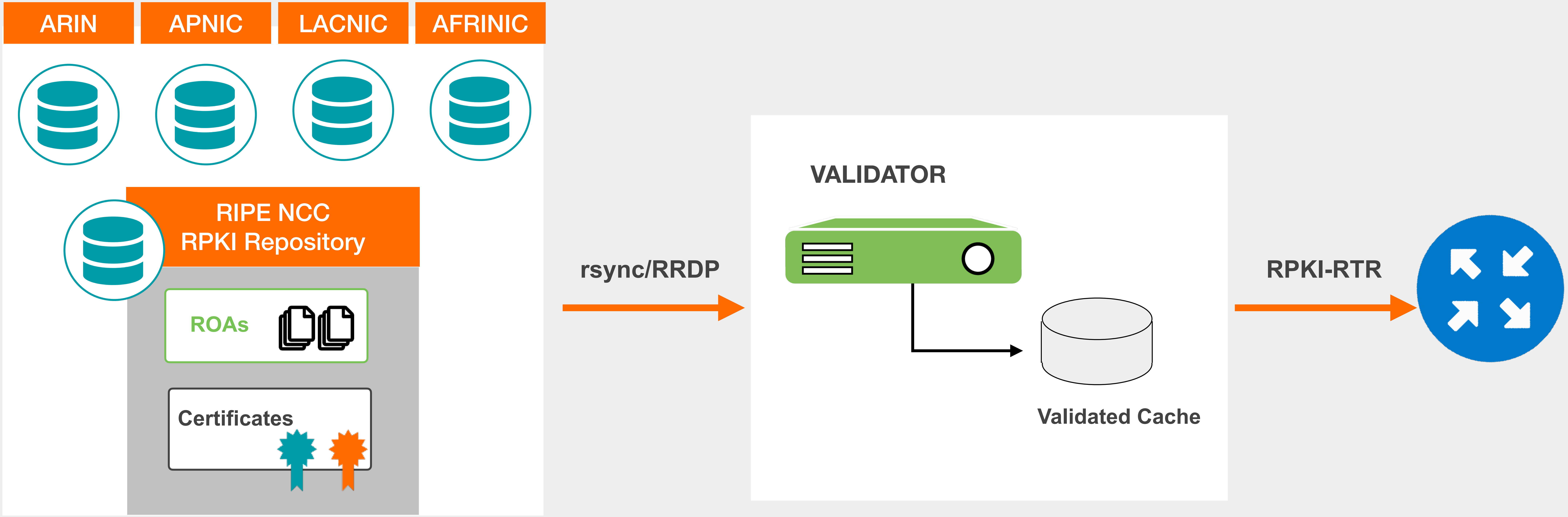
https://github.com/NICMx/FORT-validator/

https://github.com/rpki-client/rpki-client-portable

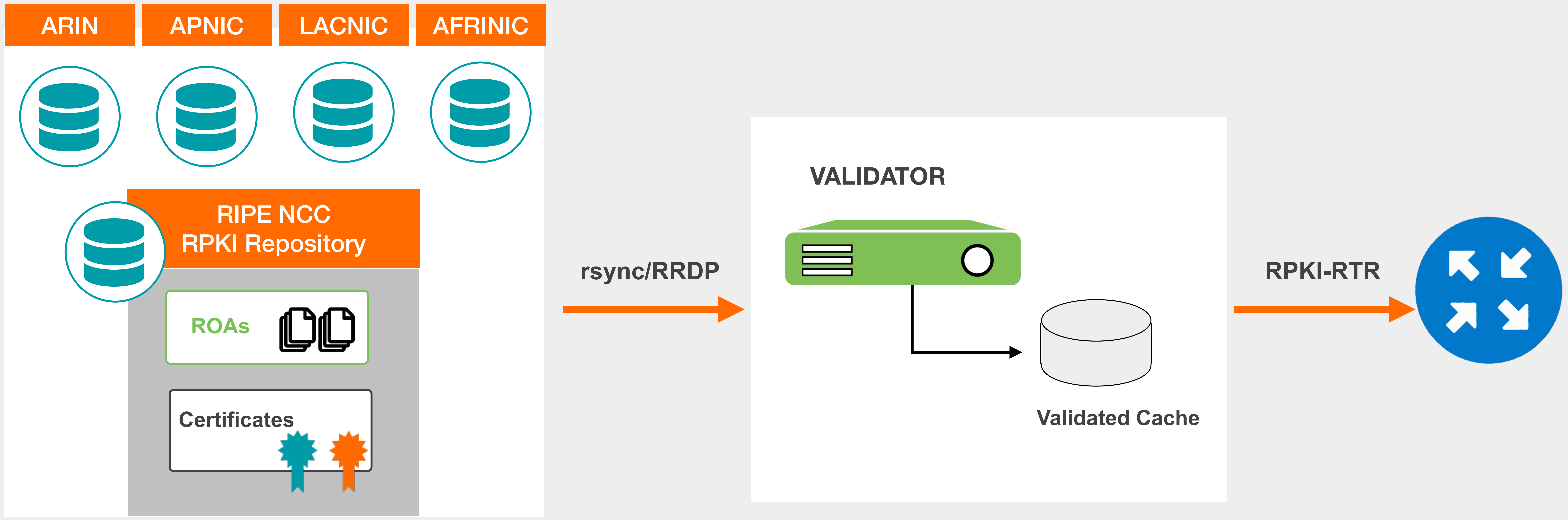
For more info...

https://rpki.readthedocs.io

Valid ROAs are sent to the router!



Valid ROAs are sent to the router!



Router uses this information to make better routing decisions!

✓ OR ✗

Take the poll!

What does it mean if a ROA is **“invalid”**?

Please choose all the options that apply.

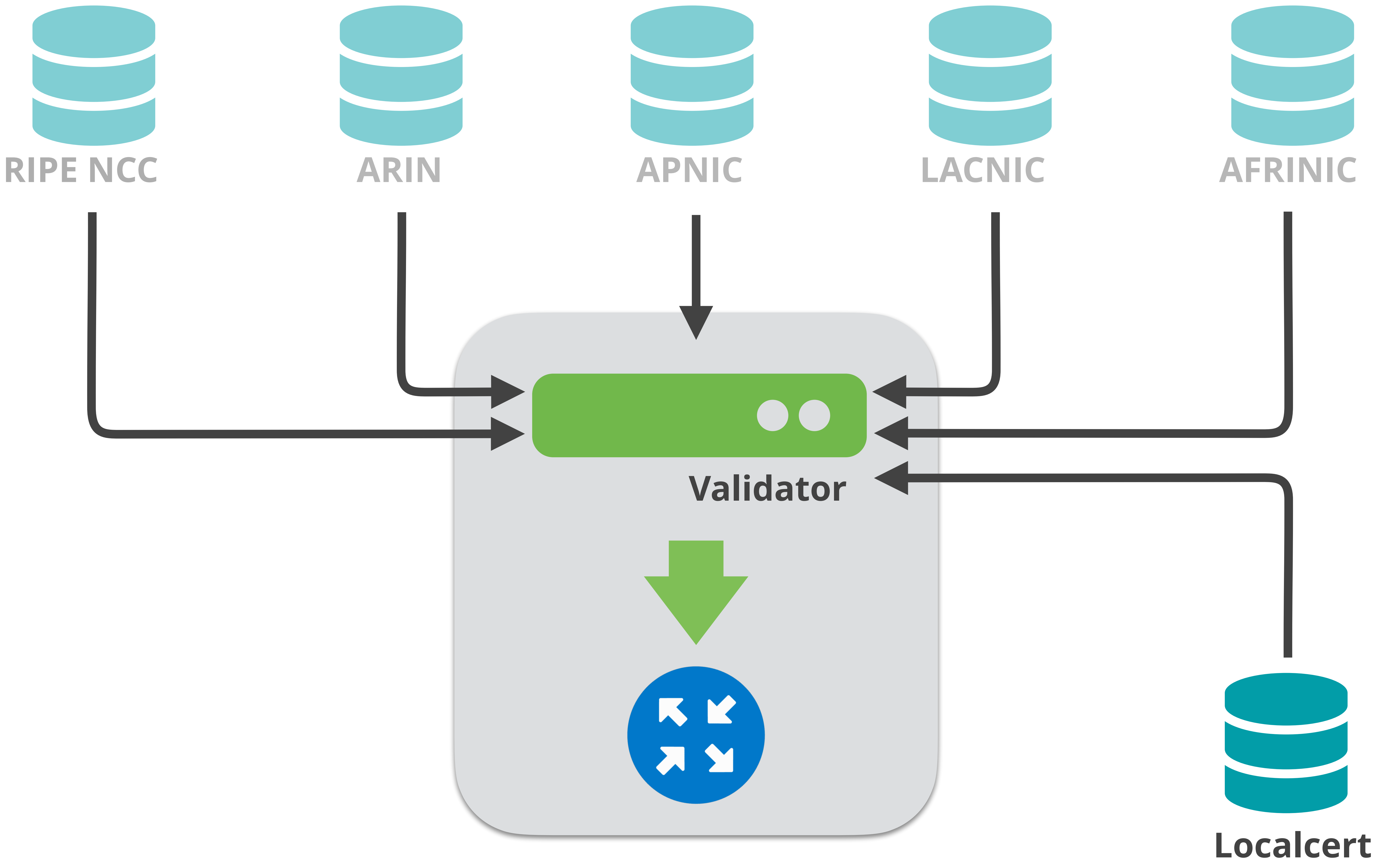
1 min.

Questions

Demo!

Running Validators

Demo Setup



Running Validators

- Before running a validator, initialisation might be required
  - Prepares directory for local RPKI cache
  - Prepares TAL directory
- TALs are bundled with validator software
  - May need to be installed by the “init” command
  - Do not forget to accept ARIN RPA (Relying Party Agreement)
- Run at least two validators

Running Validators

- In the demo, the following validators will be used:
  - Routinator (0.12.1)
  - FORT (1.5.3)
- Validators are already installed and preconfigured

Start the Routinator

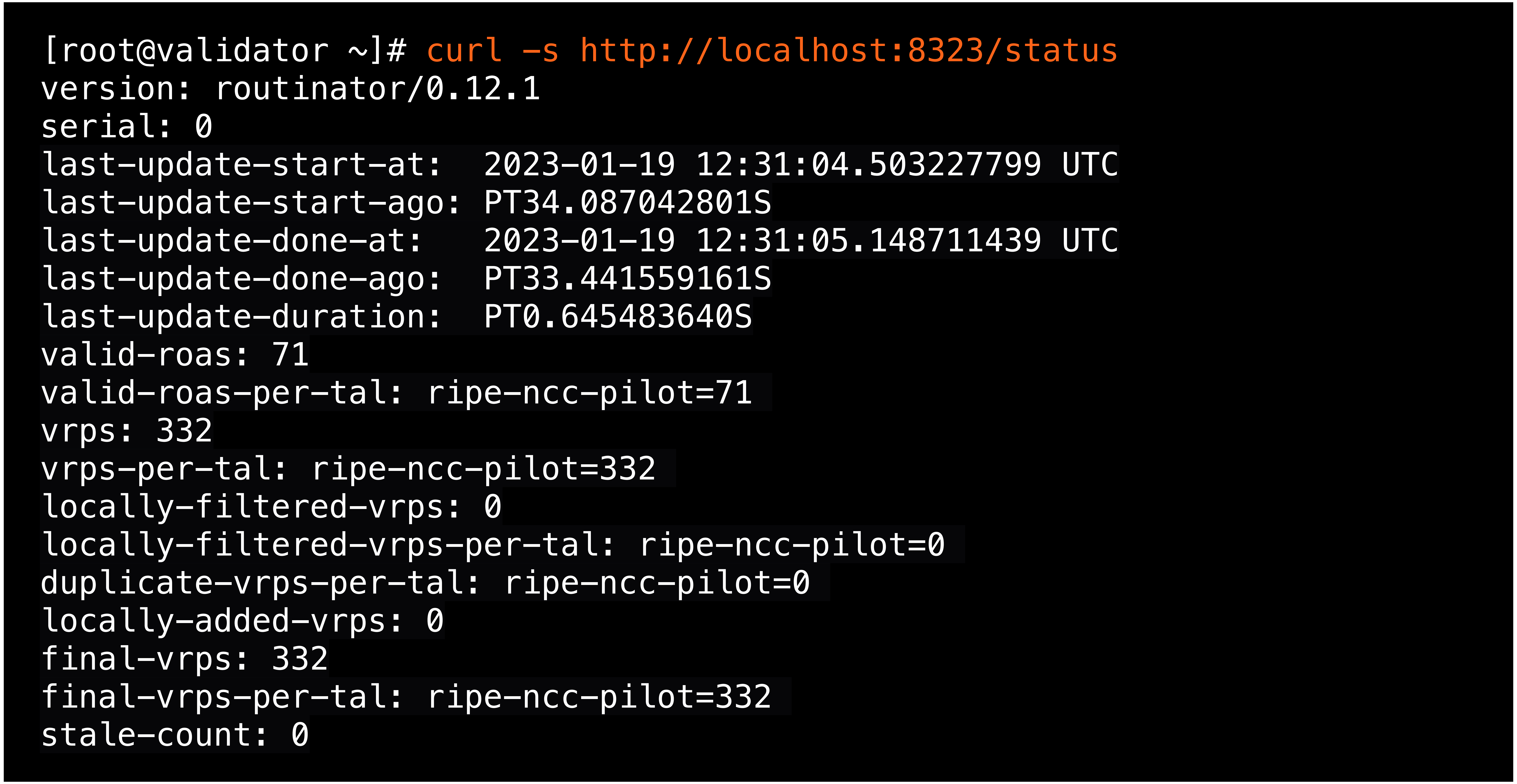
On the Server:

```
systemctl enable --now routinator
```

Check if it’s running

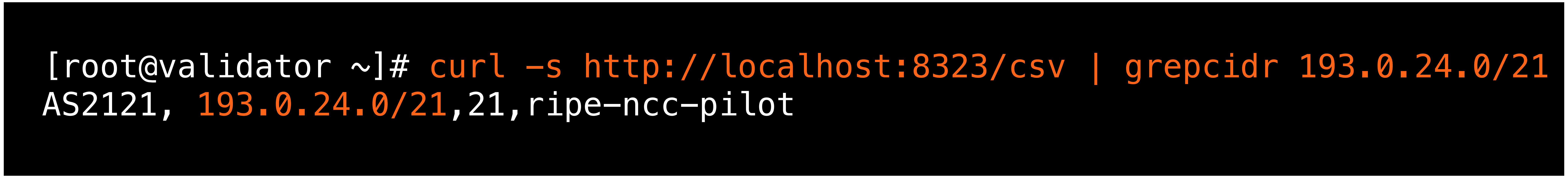
```
ps aux | grep routinator
```

Check the status and VRPs



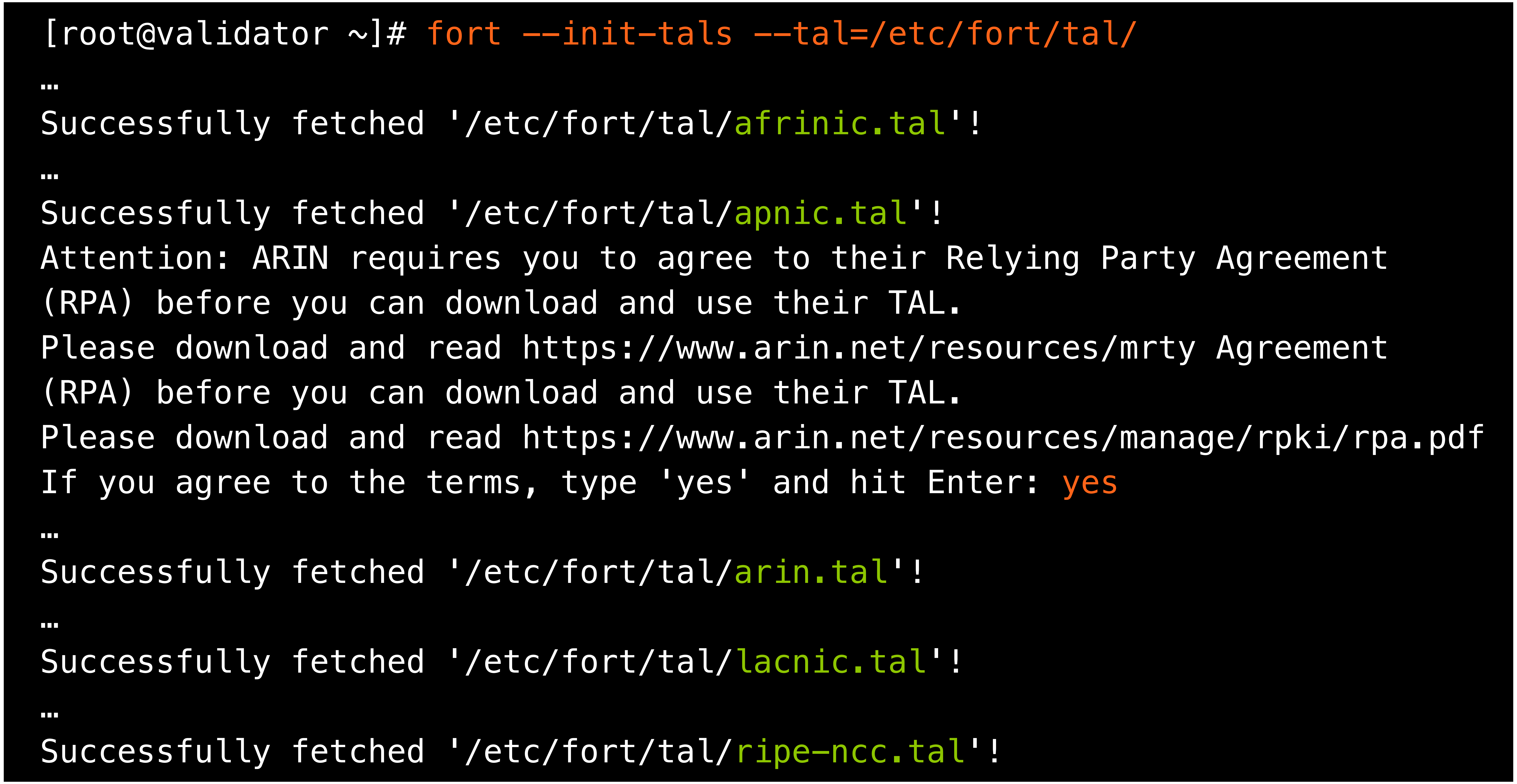
```
[root@validator ~]# curl -s http://localhost:8323/status
version: routinator/0.12.1
serial: 0
last-update-start-at:  2023-01-19 12:31:04.503227799 UTC
last-update-start-ago: PT34.087042801S
last-update-done-at:   2023-01-19 12:31:05.148711439 UTC
last-update-done-ago:  PT33.441559161S
last-update-duration:  PT0.645483640S
valid-roas: 71
valid-roas-per-tal: ripe-ncc-pilot=71
vrps: 332
vrps-per-tal: ripe-ncc-pilot=332
locally-filtered-vrps: 0
locally-filtered-vrps-per-tal: ripe-ncc-pilot=0
duplicate-vrps-per-tal: ripe-ncc-pilot=0
locally-added-vrps: 0
final-vrps: 332
final-vrps-per-tal: ripe-ncc-pilot=332
stale-count: 0
```

Check the status and VRPs



```
[root@validator ~]# curl -s http://localhost:8323/csv | grepcidr 193.0.24.0/21
AS2121, 193.0.24.0/21,21,ripe-ncc-pilot
```

Initialize the FORT validator



```
[root@validator ~]# fort --init-tals --tal=/etc/fort/tal/
…
Successfully fetched '/etc/fort/tal/afrinic.tal'!
…
Successfully fetched '/etc/fort/tal/apnic.tal'!
Attention: ARIN requires you to agree to their Relying Party Agreement
(RPA) before you can download and use their TAL.
Please download and read https://www.arin.net/resources/mrty Agreement
(RPA) before you can download and use their TAL.
Please download and read https://www.arin.net/resources/manage/rpki/rpa.pdf
If you agree to the terms, type 'yes' and hit Enter: yes
…
Successfully fetched '/etc/fort/tal/arin.tal'!
…
Successfully fetched '/etc/fort/tal/lacnic.tal'!
…
Successfully fetched '/etc/fort/tal/ripe-ncc.tal'!
```

Start FORT validator

```
systemctl enable --now fort
```

Check if it is running and the logs (exit with ctrl-c):

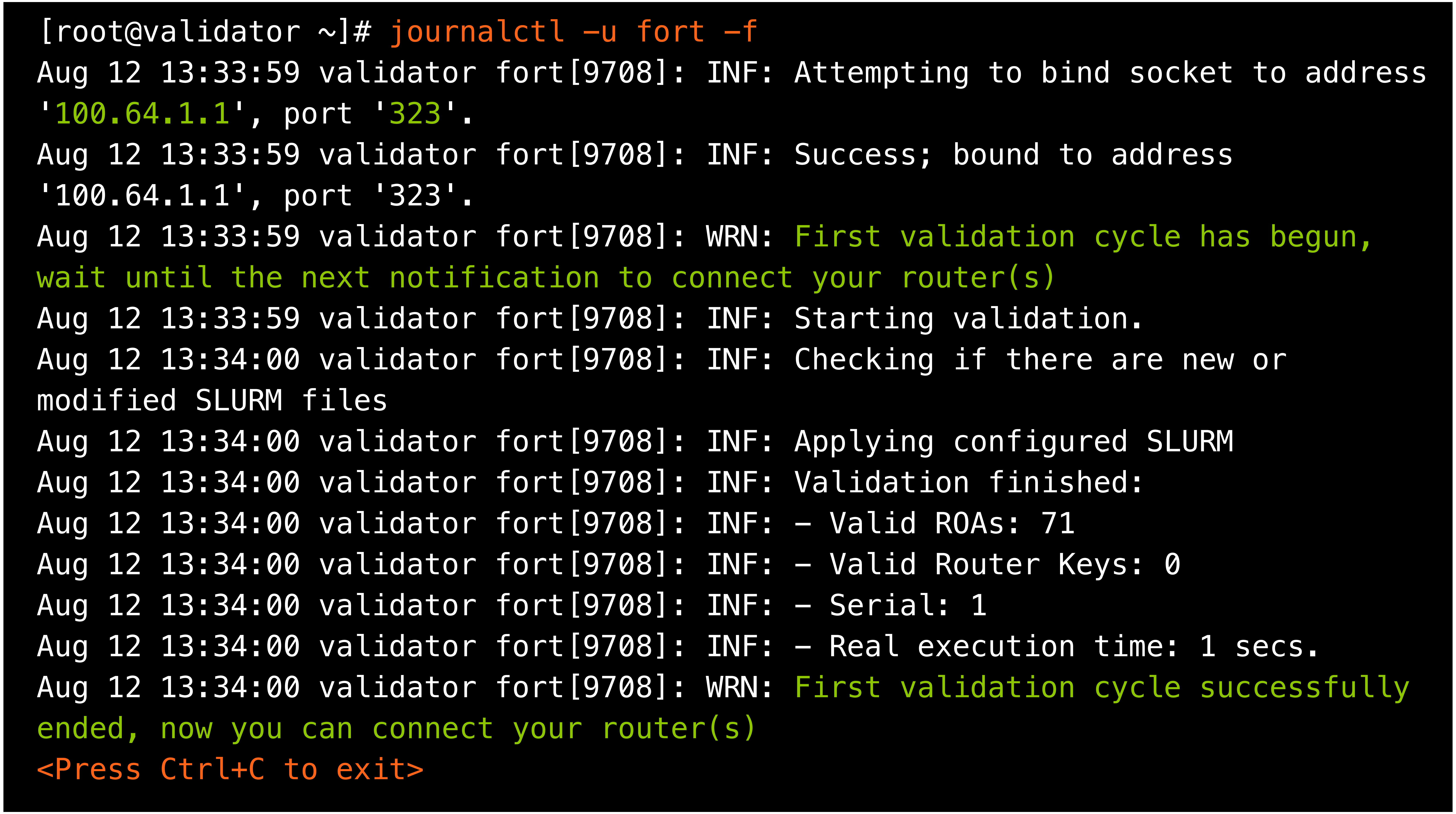
```
Systemctl status fort

journalctl -u fort
```

Check the status

- FORT will not start RTR server before it does the validation for the first time.
- It listens on port **323** by default.
- Configuration is in **/etc/fort/config.json**
- To check whether FORT is listening

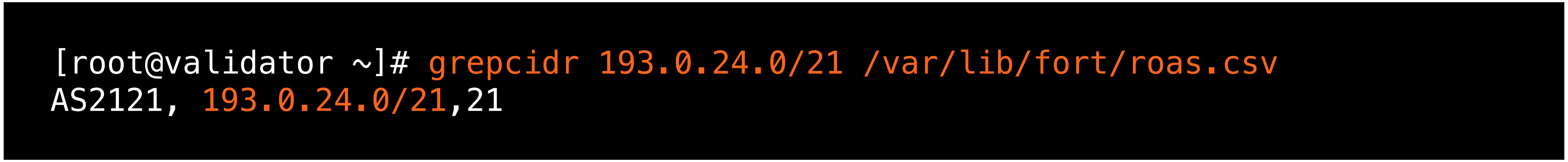
```
[root@validator ~]# ss -tlnp | grep fort
LISTEN     0      128    100.64.1.1:323                                    *:*
users:(("fort",pid=1009,fd=4))
```

Check the logs



```
[root@validator ~]# journalctl –u fort –f
Aug 12 13:33:59 validator fort[9708]: INF: Attempting to bind socket to address
'100.64.1.1', port '323'.
Aug 12 13:33:59 validator fort[9708]: INF: Success; bound to address
'100.64.1.1', port '323'.
Aug 12 13:33:59 validator fort[9708]: WRN: First validation cycle has begun,
wait until the next notification to connect your router(s)
Aug 12 13:33:59 validator fort[9708]: INF: Starting validation.
Aug 12 13:34:00 validator fort[9708]: INF: Checking if there are new or
modified SLURM files
Aug 12 13:34:00 validator fort[9708]: INF: Applying configured SLURM
Aug 12 13:34:00 validator fort[9708]: INF: Validation finished:
Aug 12 13:34:00 validator fort[9708]: INF: – Valid ROAs: 71
Aug 12 13:34:00 validator fort[9708]: INF: – Valid Router Keys: 0
Aug 12 13:34:00 validator fort[9708]: INF: – Serial: 1
Aug 12 13:34:00 validator fort[9708]: INF: – Real execution time: 1 secs.
Aug 12 13:34:00 validator fort[9708]: WRN: First validation cycle successfully
ended, now you can connect your router(s)
<Press Ctrl+C to exit>
```

Check the VRPs



```
[root@validator ~]# grepcidr 193.0.24.0/21 /var/lib/fort/roas.csv
AS2121, 193.0.24.0/21,21
```

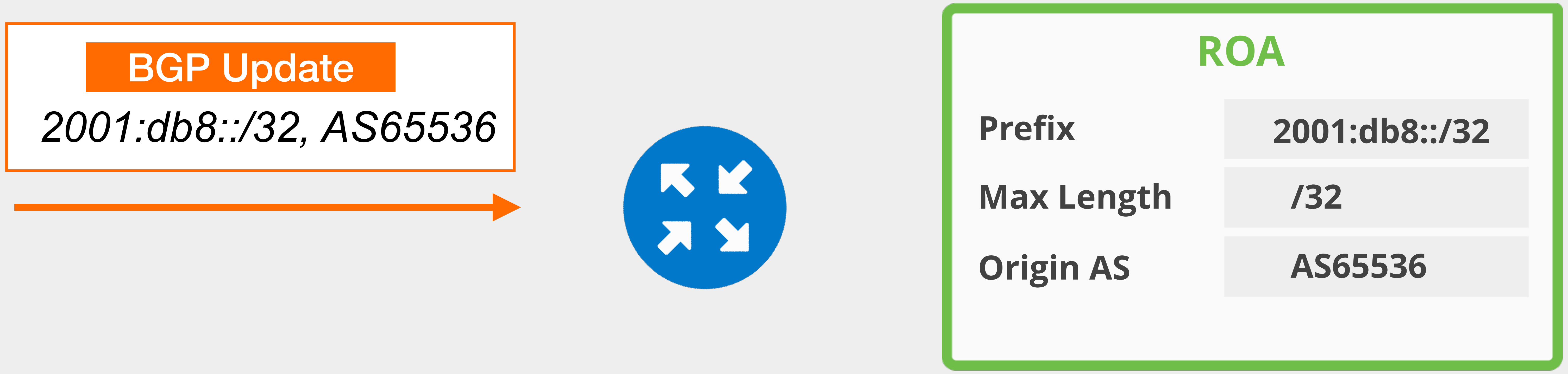
Questions

Secure routing with RPKI

Validating BGP Announcements

BGP Origin Validation (BGP OV)

- RPKI based route filtering, RFC#6811
- BGP announcements are compared against the **valid** ROAs
- **origin ASN** and **max-length** must match!
- Router decides the validation states of routes: Valid, Invalid and Not Found



BGP Update

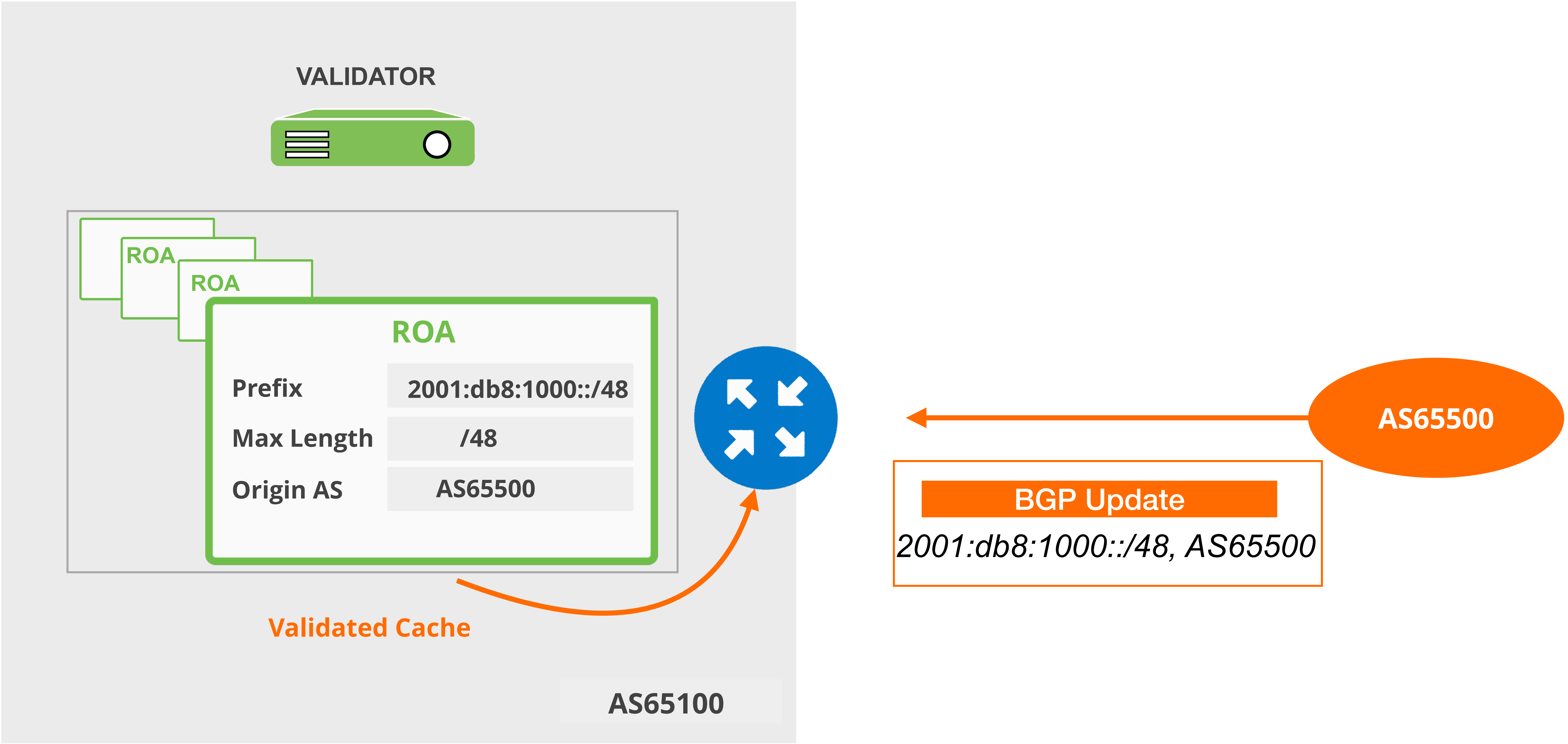
2001:db8::/32, AS65536

ROA

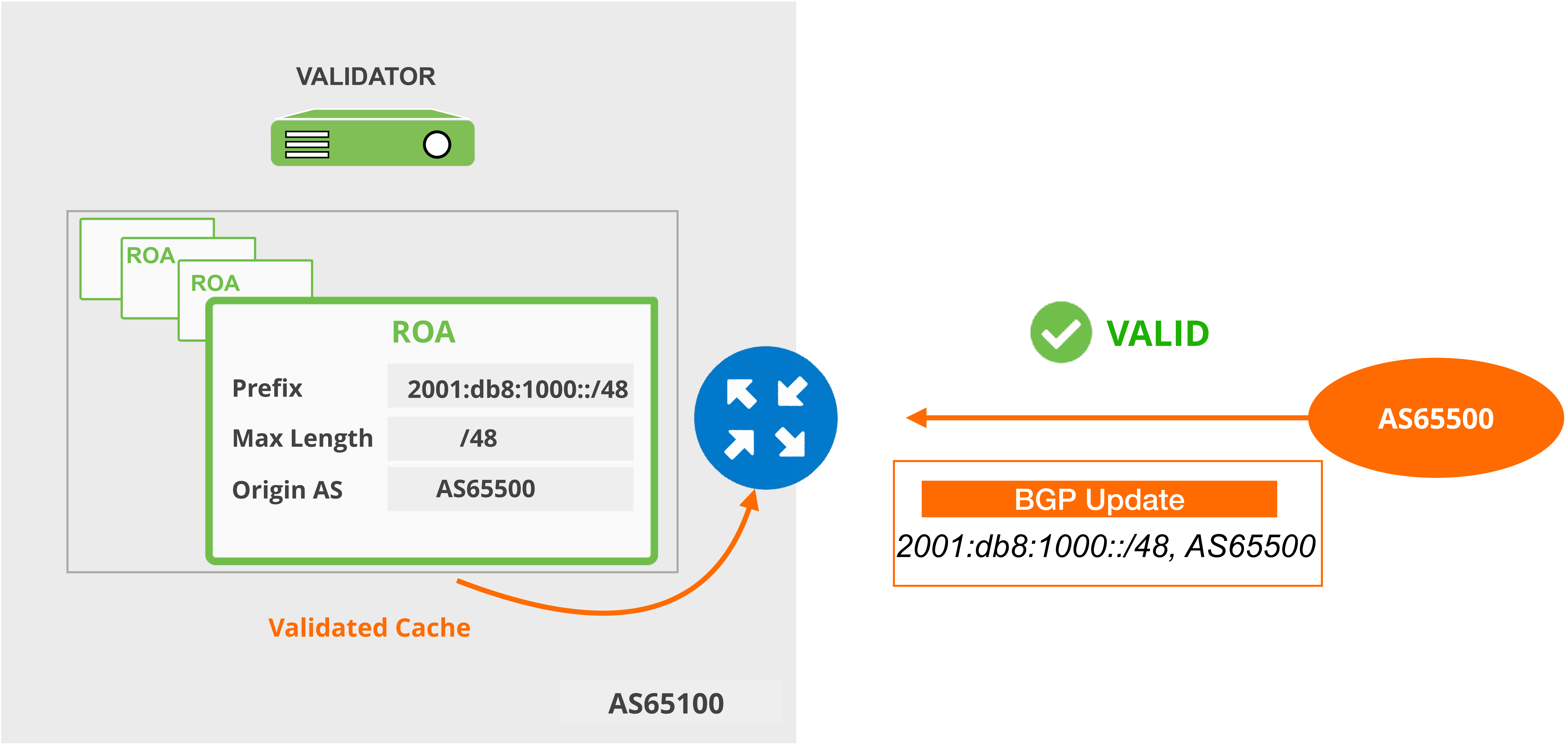
Prefix	2001:db8::/32
Max Length	/32
Origin AS	AS65536

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

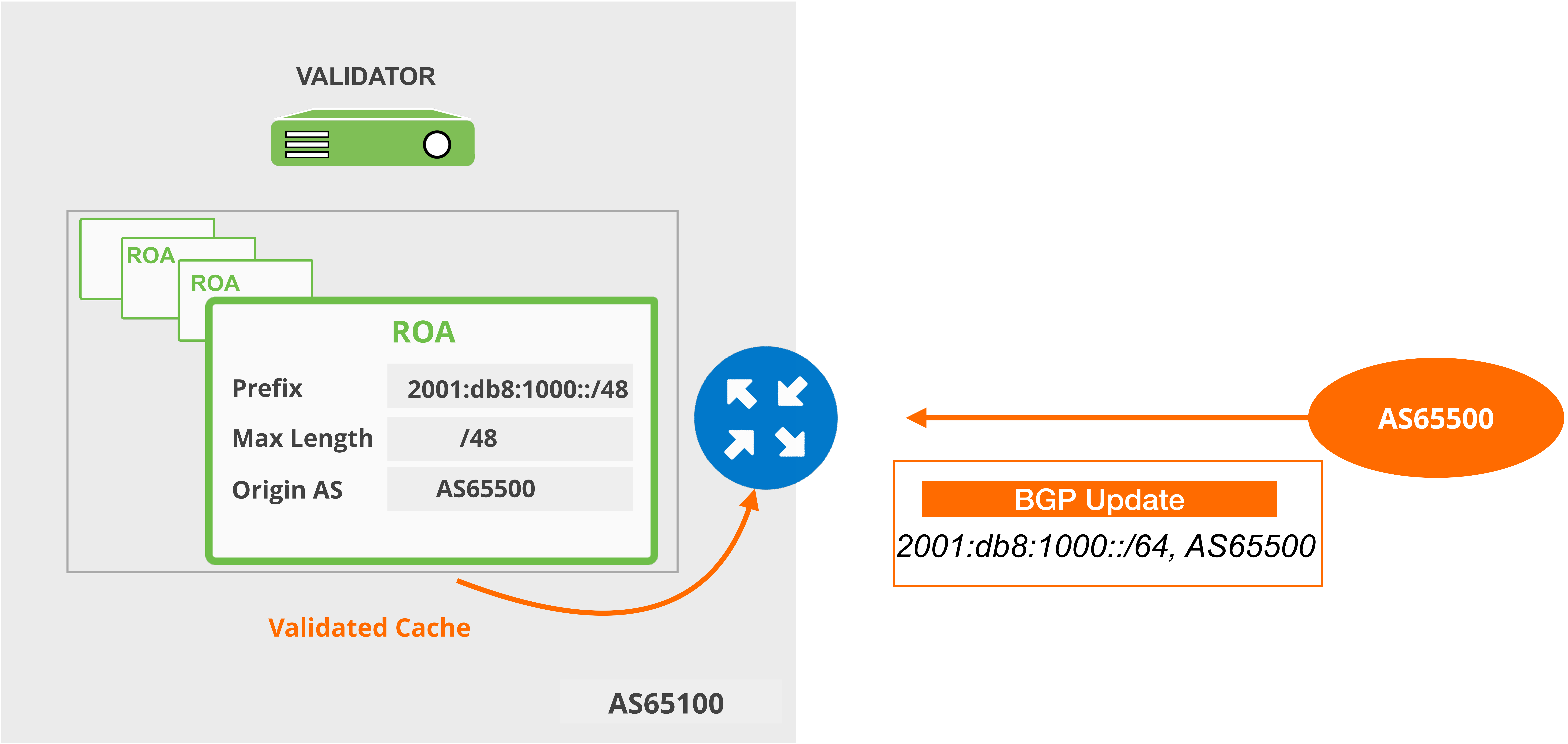
How does RPKI validate the origin?



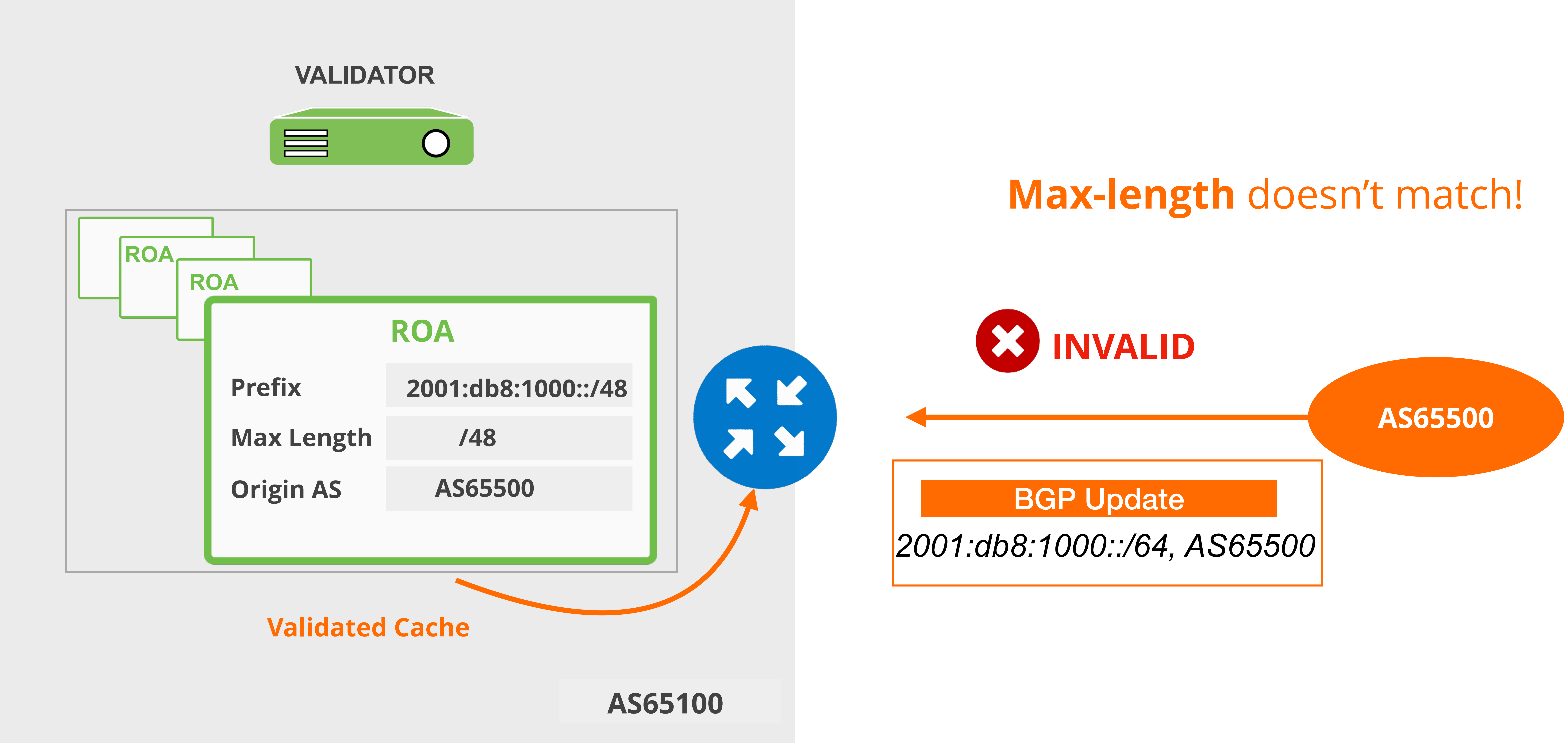
How does RPKI validate the origin?



How does RPKI validate the origin?

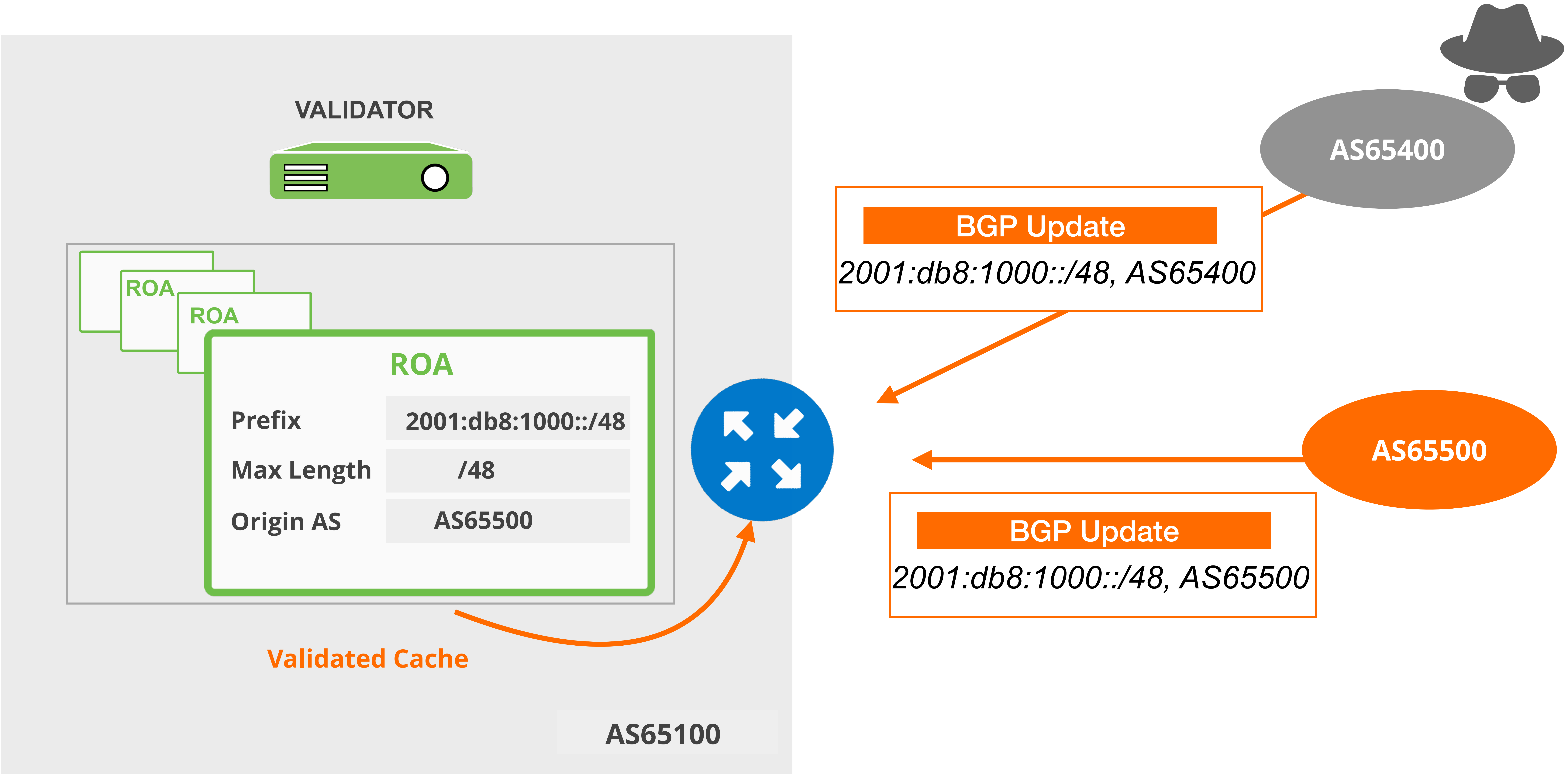


How does RPKI validate the origin?

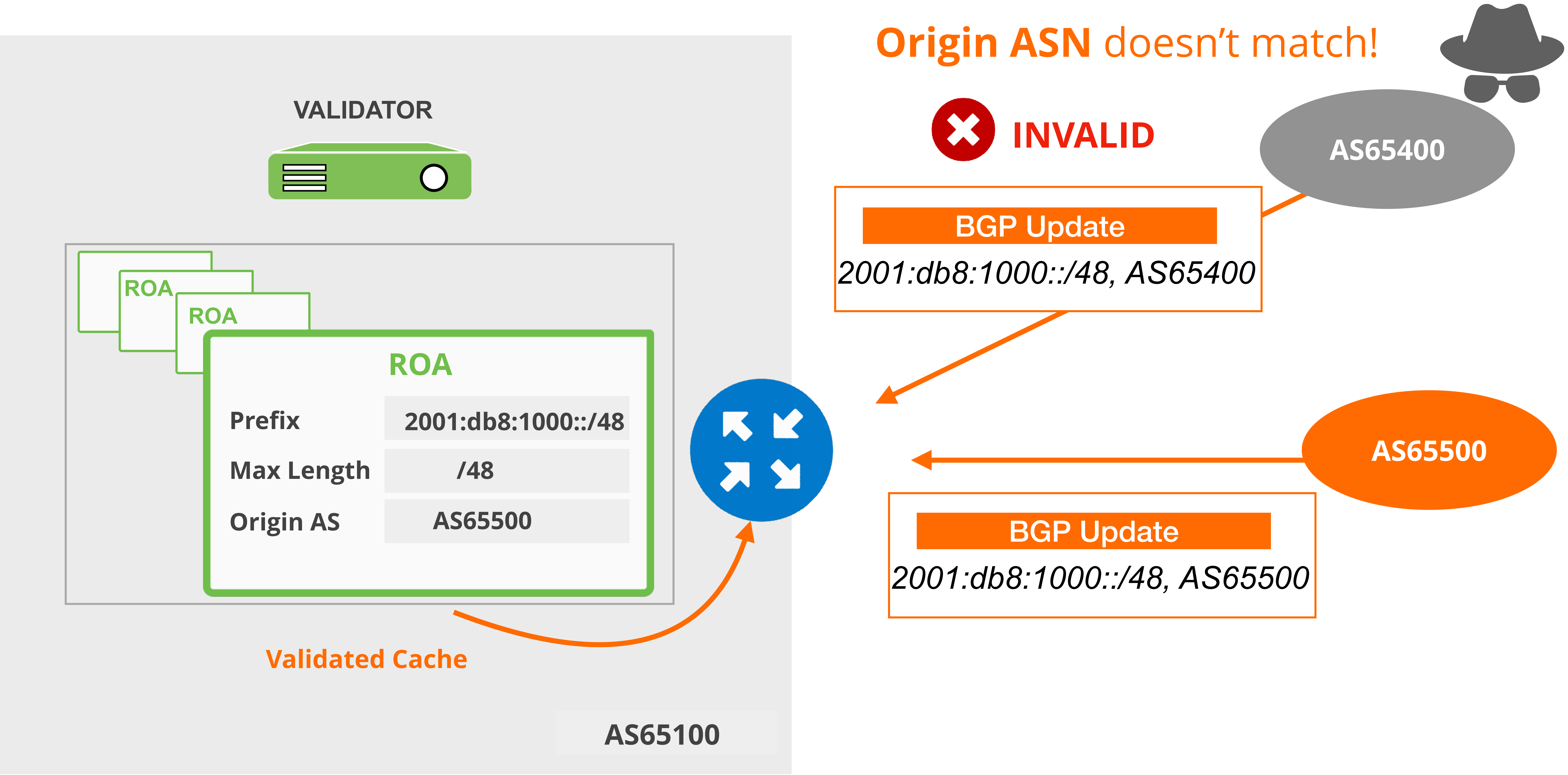


Max-length doesn’t match!

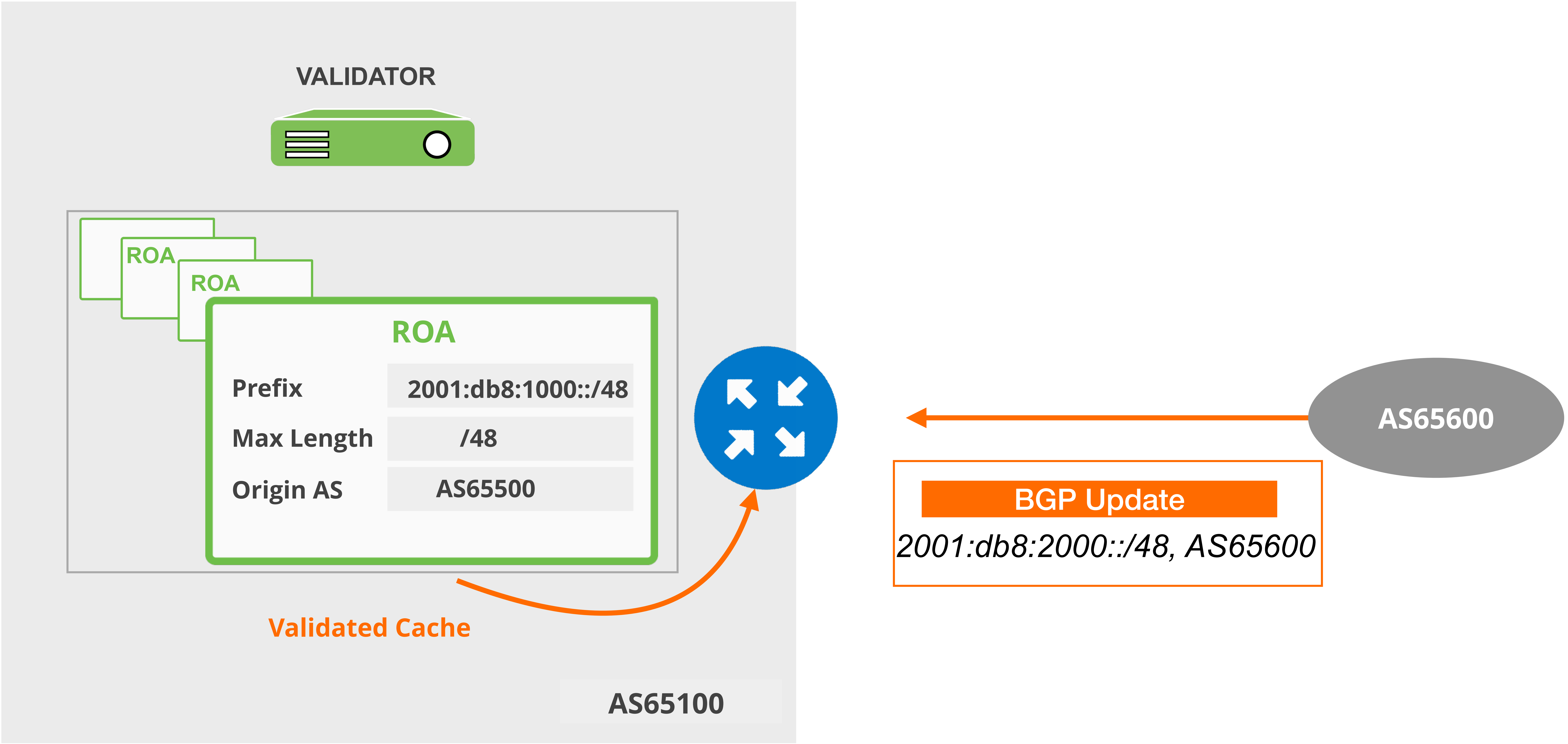
How does RPKI validate the origin?



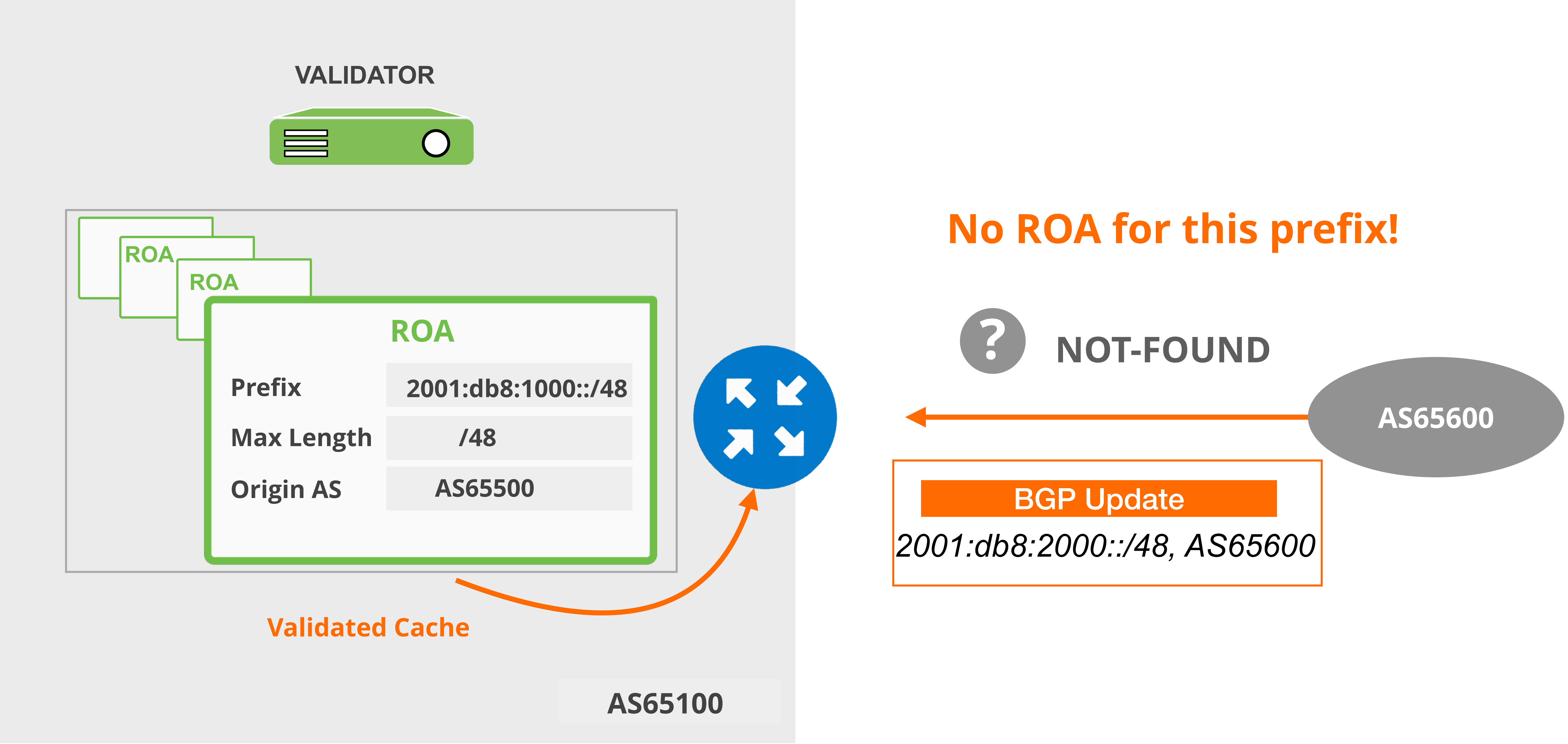
How does RPKI validate the origin?



How does RPKI validate the origin?



How does RPKI validate the origin?



Take the poll!

The RPKI status of a specific prefix in the BGP table is shown as **“Invalid”**.

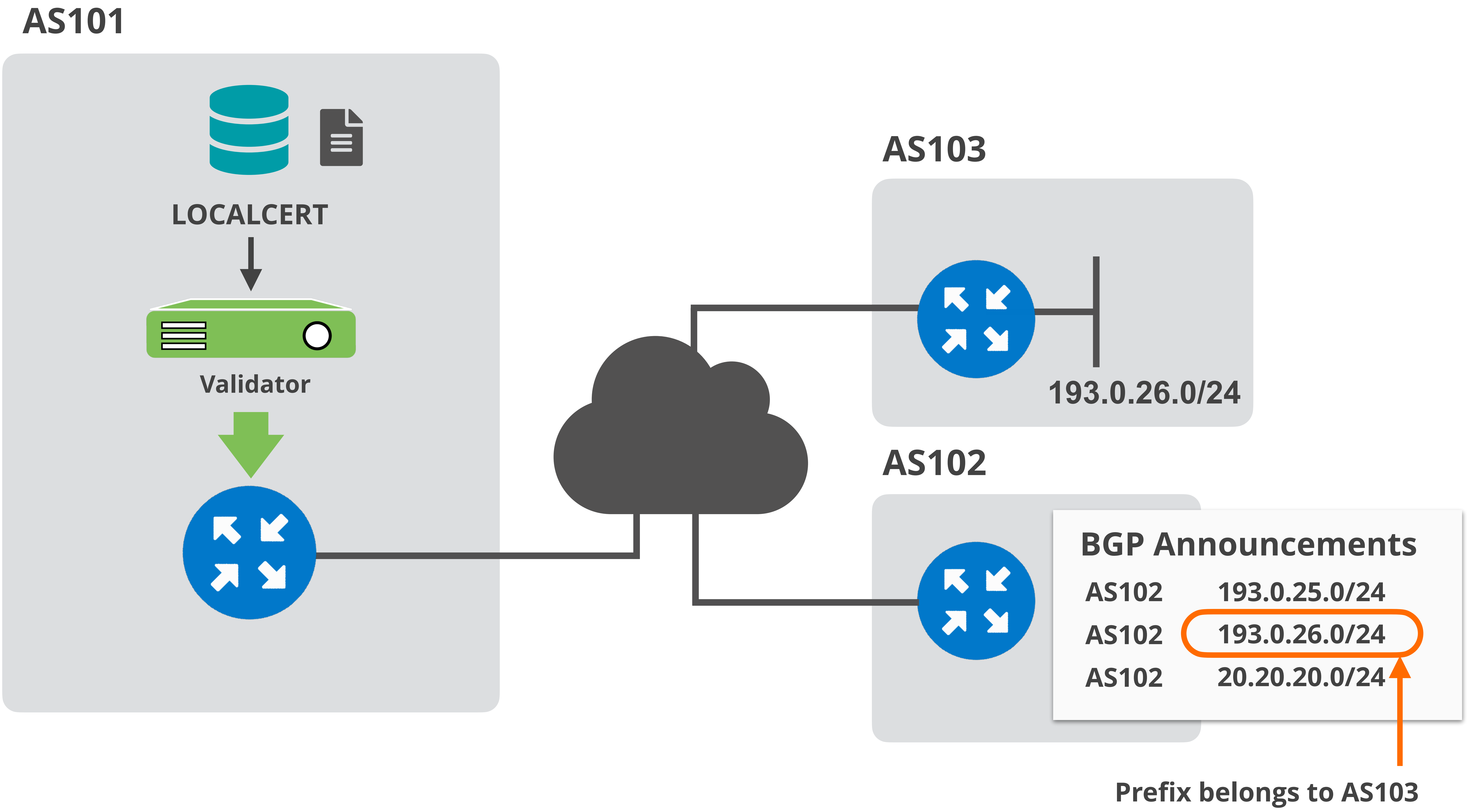
What does this mean?

⏱ 1 min.

Demo!

Setting up BGP Origin Validation

Demo Setup



BGP Announcements

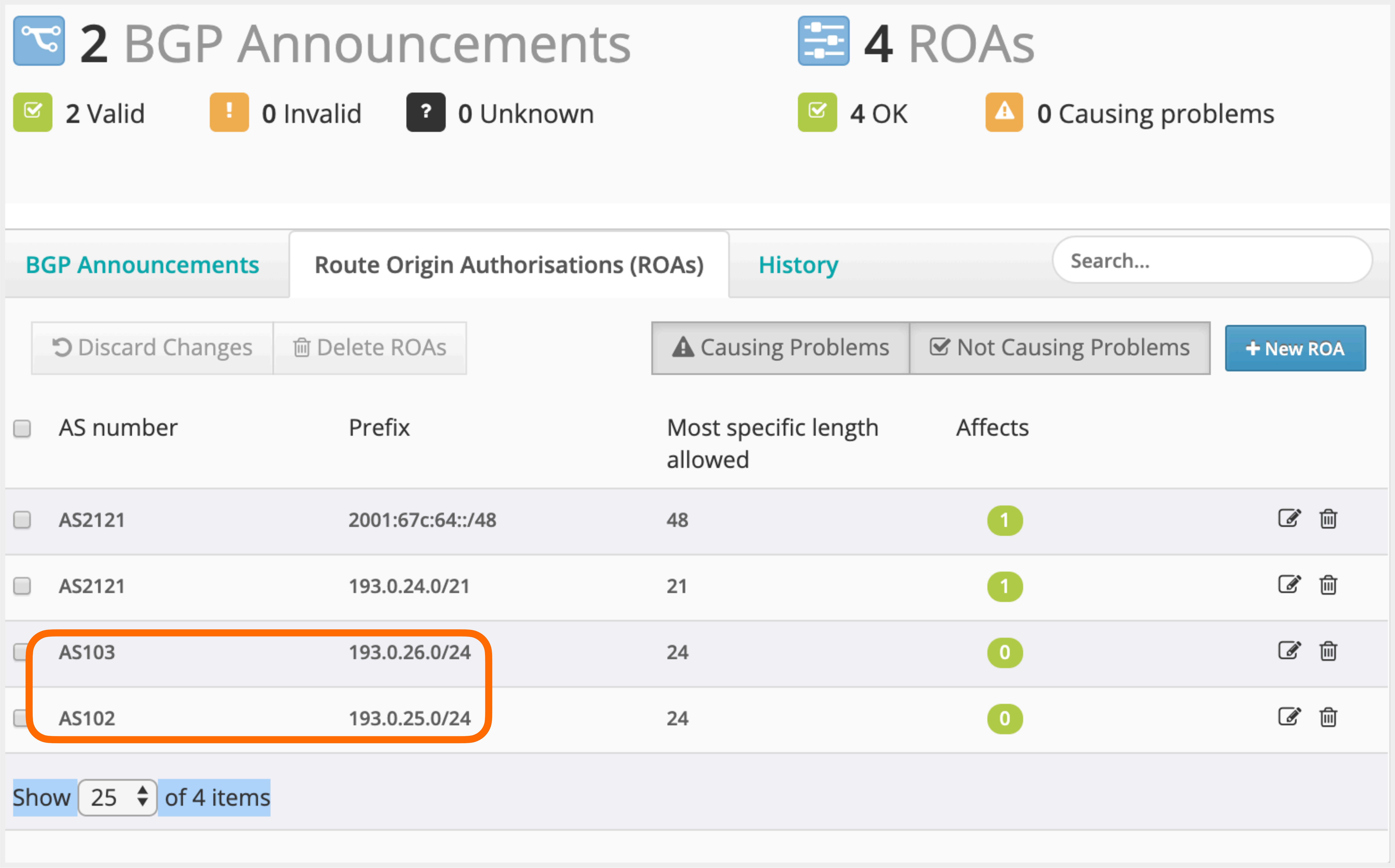
AS102	193.0.25.0/24
AS102	193.0.26.0/24
AS102	20.20.20.0/24

Prefix belongs to AS103

Setup Origin Validation in AS101

- We are using FORT and Routinator validator options
- Both validators are preconfigured and already running!
- RPKI-RTR will be configured on AS101 router
- AS102 router will be configured to announce some prefixes;
  - its own prefix (**193.0.25.0/24**)
  - AS103 prefix (**193.0.26.0/24**) and will cause BGP prefix hijack
  - a prefix without a ROA (**20.20.20.0/24**)

ROAs Created in Previous Demo



2 BGP Announcements

2 Valid ! 0 Invalid ? 0 Unknown

4 ROAs

4 OK 0 Causing problems

□	AS number	Prefix	Most specific length allowed	Affects
□	AS2121	2001:67c:64::/48	48	1
□	AS2121	193.0.24.0/21	21	1
□	AS103	193.0.26.0/24	24	0
□	AS102	193.0.25.0/24	24	0

Show 25 of 4 items

Configure Validator Connection

- Configure validators as “RPKI servers” on the router
  - Router talks to validator via RPKI-RTR (RPKI to Router Protocol)

```
(config)# conf t
(config)# router bgp 101
(config-router)# bgp rpki server tcp 100.64.1.1 port 3323 refresh 300
(config-router)# bgp rpki server tcp 100.64.1.1 port 323 refresh 300
```

Routinator

FORT

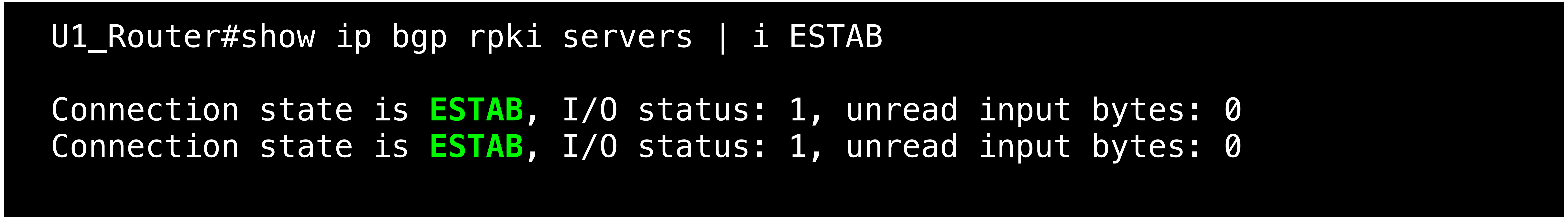
```
# show ip bgp rpki servers | i ESTAB
# show ip bgp rpki table
```

RPKI Router Configurations...

https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/router-configuration

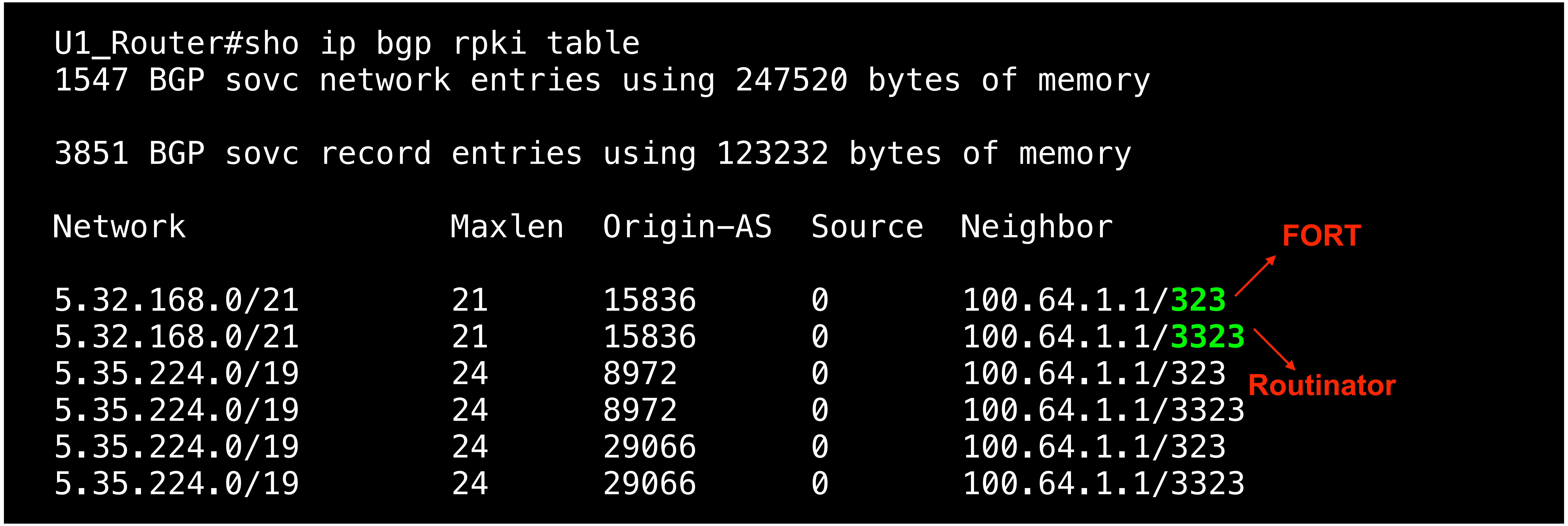
Verify the connection

- Verify the connection to the RPKI Validator service



```
U1_Router#show ip bgp rpki servers | i ESTAB

Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

- Verify that AS101 router is receiving consistent VRPs



```
U1_Router#sho ip bgp rpki table
1547 BGP sovc network entries using 247520 bytes of memory

3851 BGP sovc record entries using 123232 bytes of memory

Network                Maxlen  Origin-AS  Source  Neighbor

5.32.168.0/21          21      15836      0       100.64.1.1/323
5.32.168.0/21          21      15836      0       100.64.1.1/3323
5.35.224.0/19          24      8972       0       100.64.1.1/323
5.35.224.0/19          24      8972       0       100.64.1.1/3323
5.35.224.0/19          24      29066      0       100.64.1.1/323
5.35.224.0/19          24      29066      0       100.64.1.1/3323
```

FORT

Routinator

Configure BGP announcements

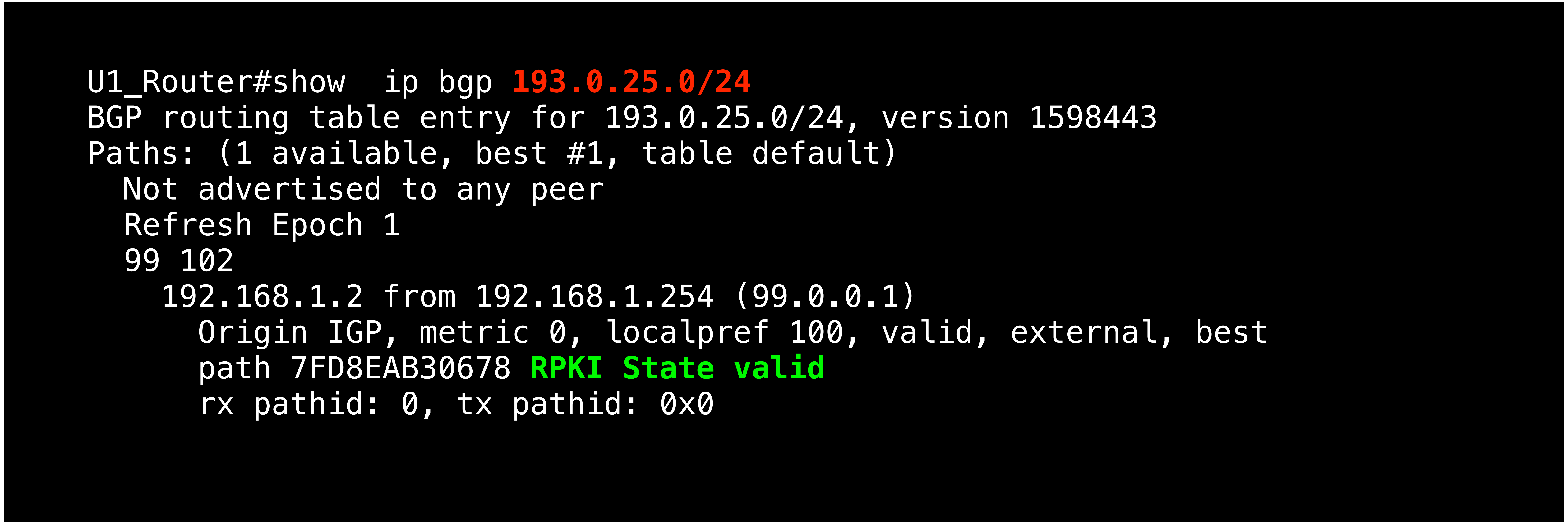
- Let’s configure the router in AS102 to announce prefixes!
- Afterwards, check for BGP origin validation result on AS101 router!

```
(config)# router bgp 102
(config-router)# address-family ipv4
(config-router)# network 20.20.20.0 mask 255.255.255.0
(config-router)# network 193.0.25.0
(config-router)# network 193.0.26.0

(config-router)# ip route 20.20.20.0 255.255.255.0 null0
(config-router)# ip route 193.0.25.0 255.255.255.0 null0
(config-router)# ip route 193.0.26.0 255.255.255.0 null0
```

No ROA for this one!

Prefix belongs to AS103!

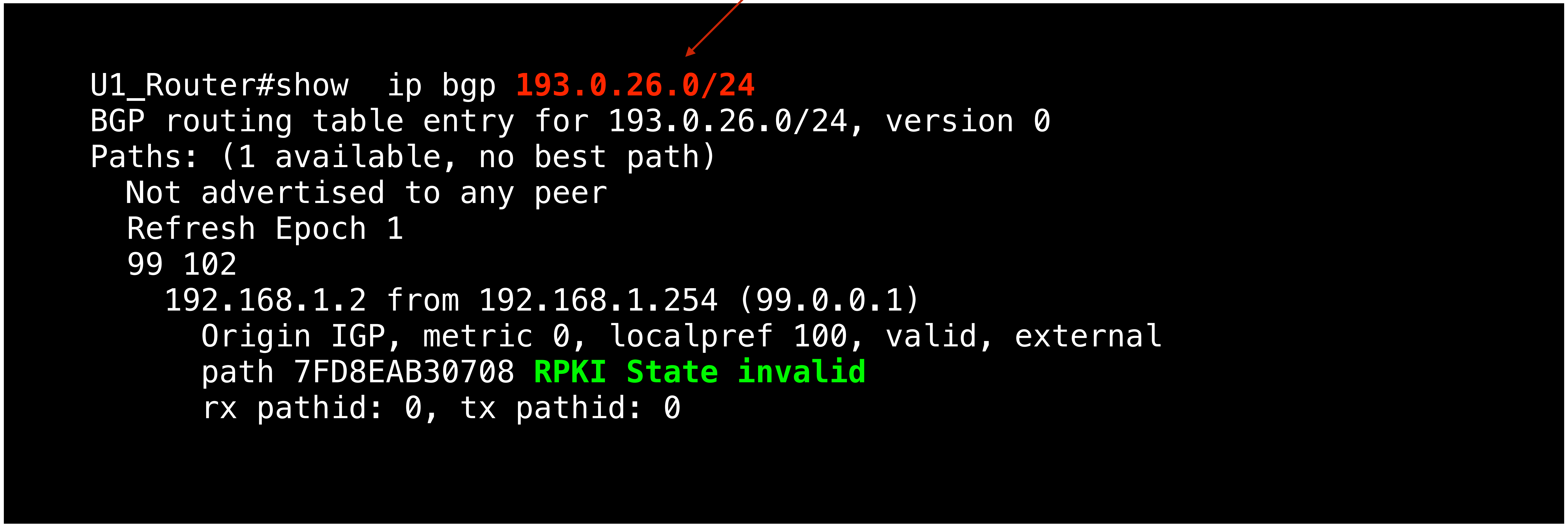
RPKI Valid



```
U1_Router#show  ip bgp 193.0.25.0/24
BGP routing table entry for 193.0.25.0/24, version 1598443
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
  99 102
    192.168.1.2 from 192.168.1.254 (99.0.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      path 7FD8EAB30678 RPKI State valid
      rx pathid: 0, tx pathid: 0x0
```

RPKI Invalid

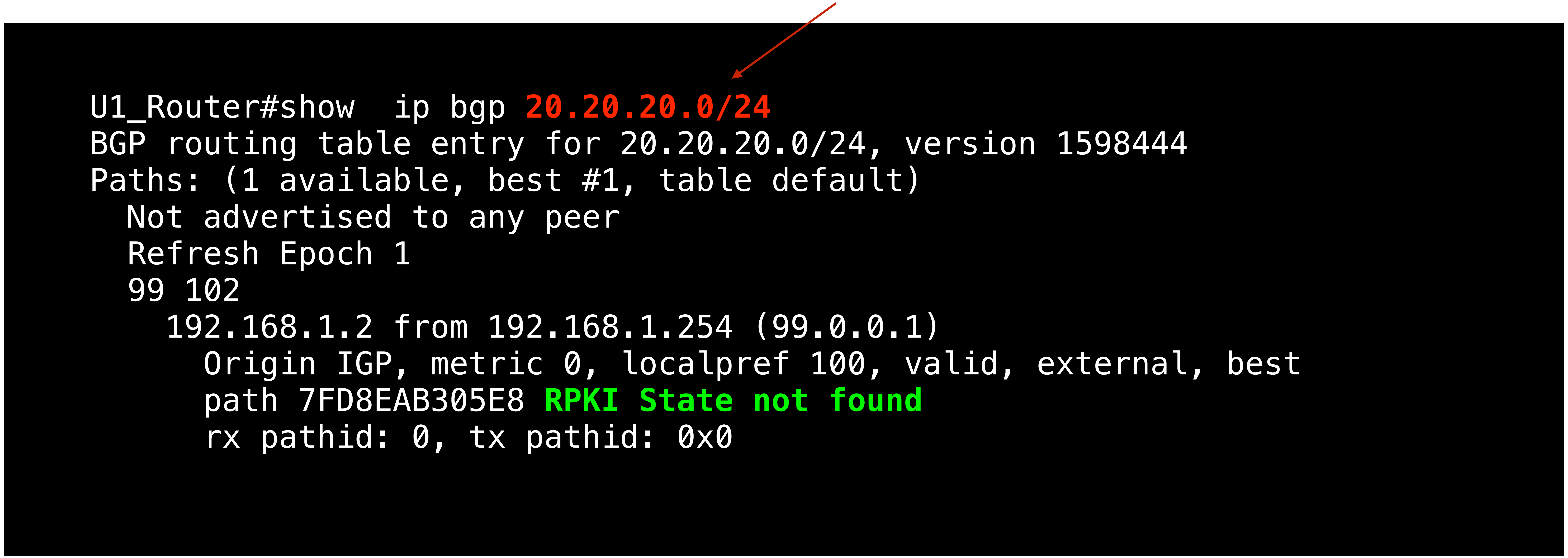
Prefix belongs to AS103!



```
U1_Router#show  ip bgp 193.0.26.0/24
BGP routing table entry for 193.0.26.0/24, version 0
Paths: (1 available, no best path)
  Not advertised to any peer
  Refresh Epoch 1
  99 102
    192.168.1.2 from 192.168.1.254 (99.0.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      path 7FD8EAB30708 RPKI State invalid
      rx pathid: 0, tx pathid: 0
```

Prefix Without a ROA

No ROA for this one!



```
U1_Router#show  ip bgp 20.20.20.0/24
BGP routing table entry for 20.20.20.0/24, version 1598444
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
  99 102
    192.168.1.2 from 192.168.1.254 (99.0.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      path 7FD8EAB305E8 RPKI State not found
      rx pathid: 0, tx pathid: 0x0
```

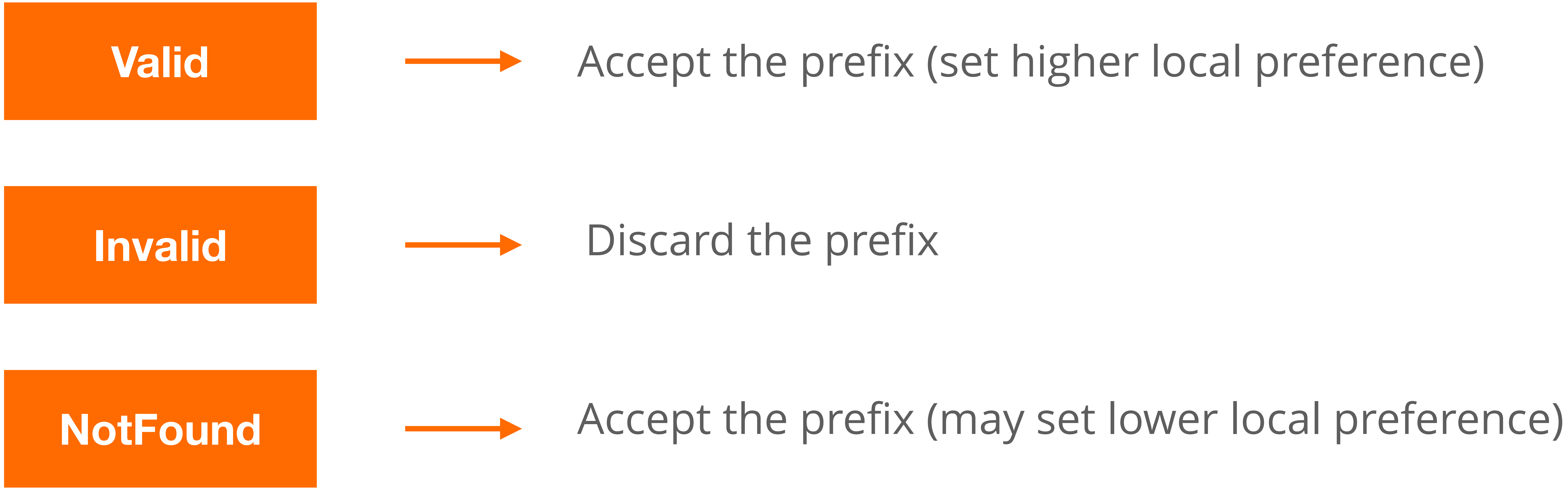
Questions

Secure Routing with RPKI

Discarding BGP Invalids

After Validating …

- You have to make a decision : “Accept” or “Discard”



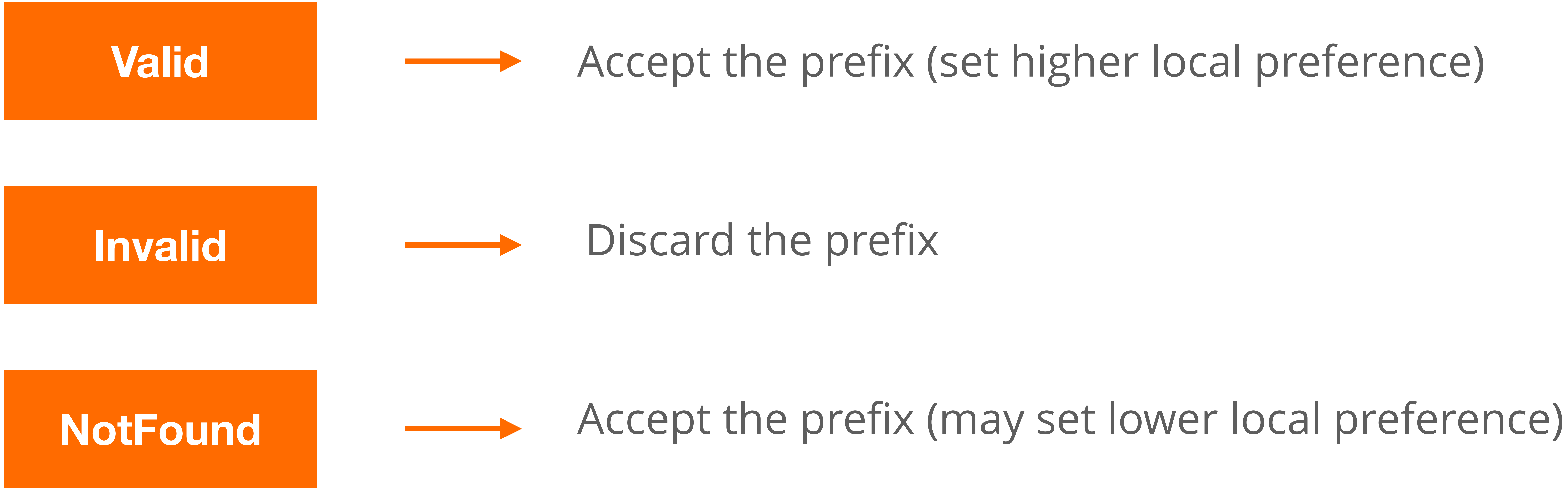
Valid → Accept the prefix (set higher local preference)

Invalid → Discard the prefix

NotFound → Accept the prefix (may set lower local preference)

After Validating ...

- You have to make a decision : “Accept” or “Discard”



Valid → Accept the prefix (set higher local preference)

Invalid → Discard the prefix

NotFound → Accept the prefix (may set lower local preference)

Do not consider dropping prefixes with “NotFound” RPKI validation state!

Discarding BGP Invalids

- For BGP origin validation (BGP OV) to achieve its goal…
  - Invalids should be dropped!
- Tag the invalids with a BGP communities
  - or set lower local preference (not a long term solution)
- After analysing the effect, you can start dropping invalids

Discarding BGP Invalids

- Major networks are dropping invalid BGP prefixes!
  - Telia, AT&T, Cloudflare, Netflix, Swisscom, Cogent, …
- April 2021, RIPE NCC (AS3333) started dropping invalids too!
  - only networks with RPKI Valid or Unknown announcements are allowed
  - K-Root (AS25152) is not part of AS3333

Let’s deploy RPKI today!

Give support for secure Internet routing and help to mitigate routing incidents globally

Questions ?

We want your feedback!

What did you think about this session? Take our survey at:

https://www.ripe.net/feedback/bgp2

RIPE NCC
Academy

Learn something new today!

academy.ripe.net

RIPE NCC Certified Professionals

RIPE NCC Certified Professionals
IPv6 Fundamentals
Analyst
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/

Ënn

Vége

Son

Lõpp

Kraj

Fine

Fim

Соңы

Endir

დასასრული

Amaia

Sfârşit

Fin

Slut

An Críoch

Finvezh

הסוף

Loppu

النهاية

Конец

Einde

Fí

پایان

վերջ

Tmiem

Slutt

Край

Ende

Кінець

Liðugt

Konec

Beigas

Y Diwedd

Koniec

Finis

Kpaj

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