RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RPKI Operations

for Ukraine

Webinar

RIPE NCC Learning & Development


This session is
being recorded

Overview

BGP & Routing Security

-Is BGP Secure?

What is RPKI?

-Resource Certification

Route Origin Authorisation (ROA)

-What is a ROA?

How to create a ROA?

-Registering routing info in the RPKI system

RPKI Validation

-Deploying RPKI Validators

-Validating BGP Announcements

-Discarding BGP Invalids

RPKI Statistics for Ukraine

-Review RPKI statistics in RIPEstat

Demos

-Creating ROAs

-Running Validators

-Setting up BGP Origin Validation

-Discarding BGP Invalids

BGP & Routing Security

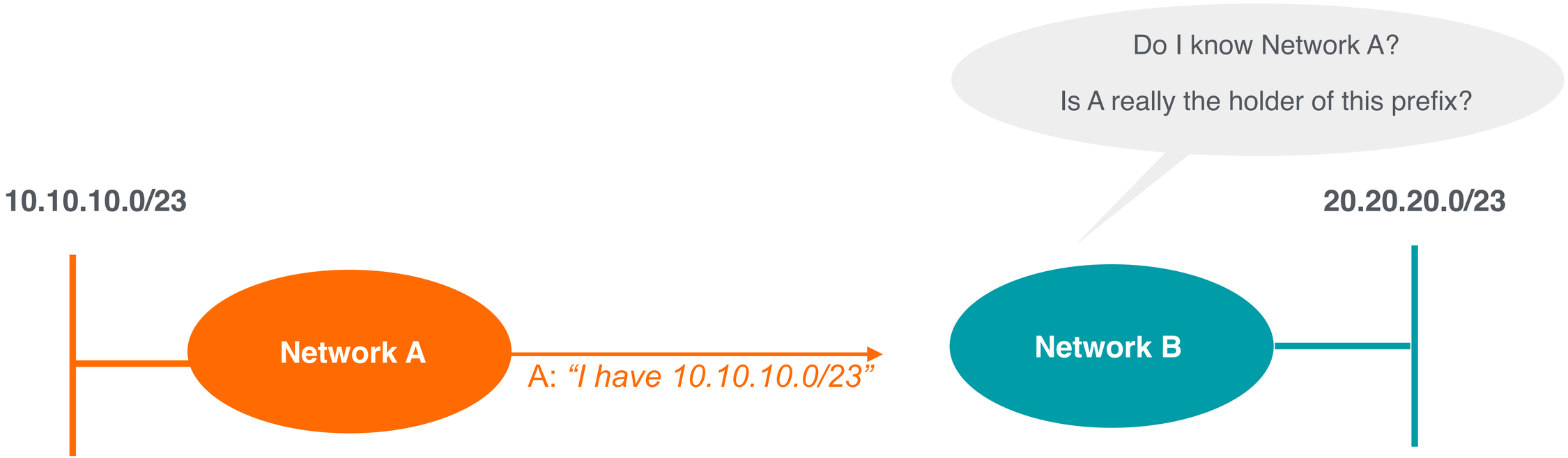
Is BGP secure?

BGP, Protocol of the Internet!

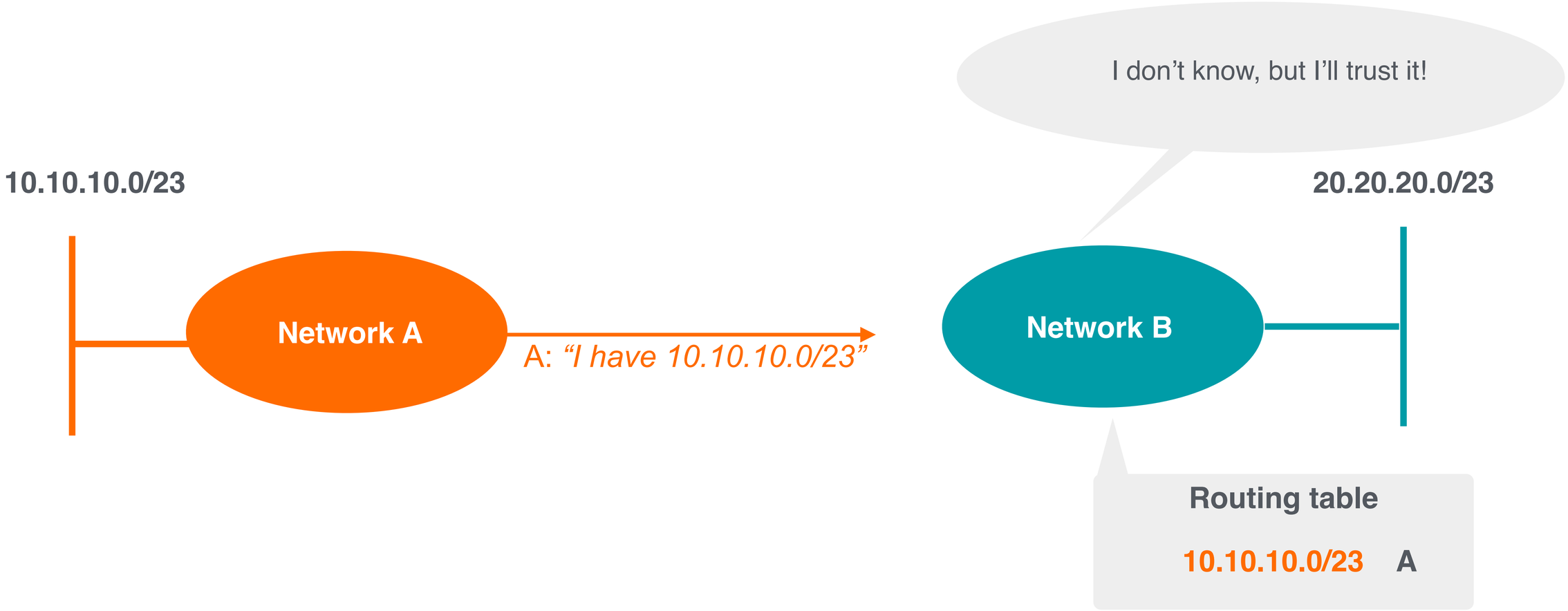
How does it work?

How does it work?

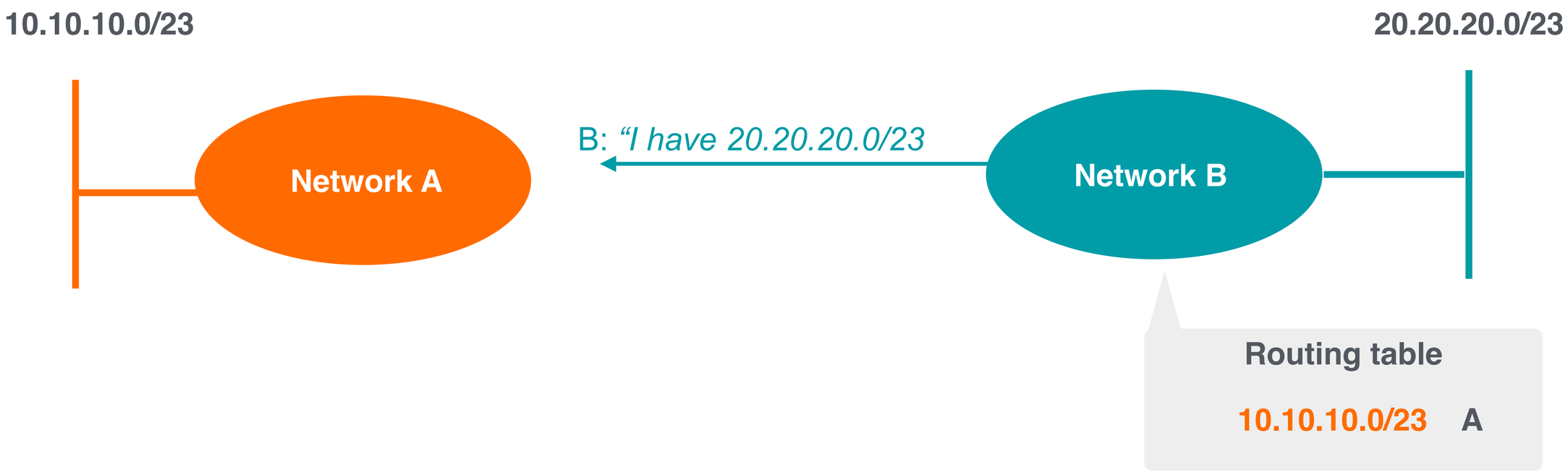
How does it work?



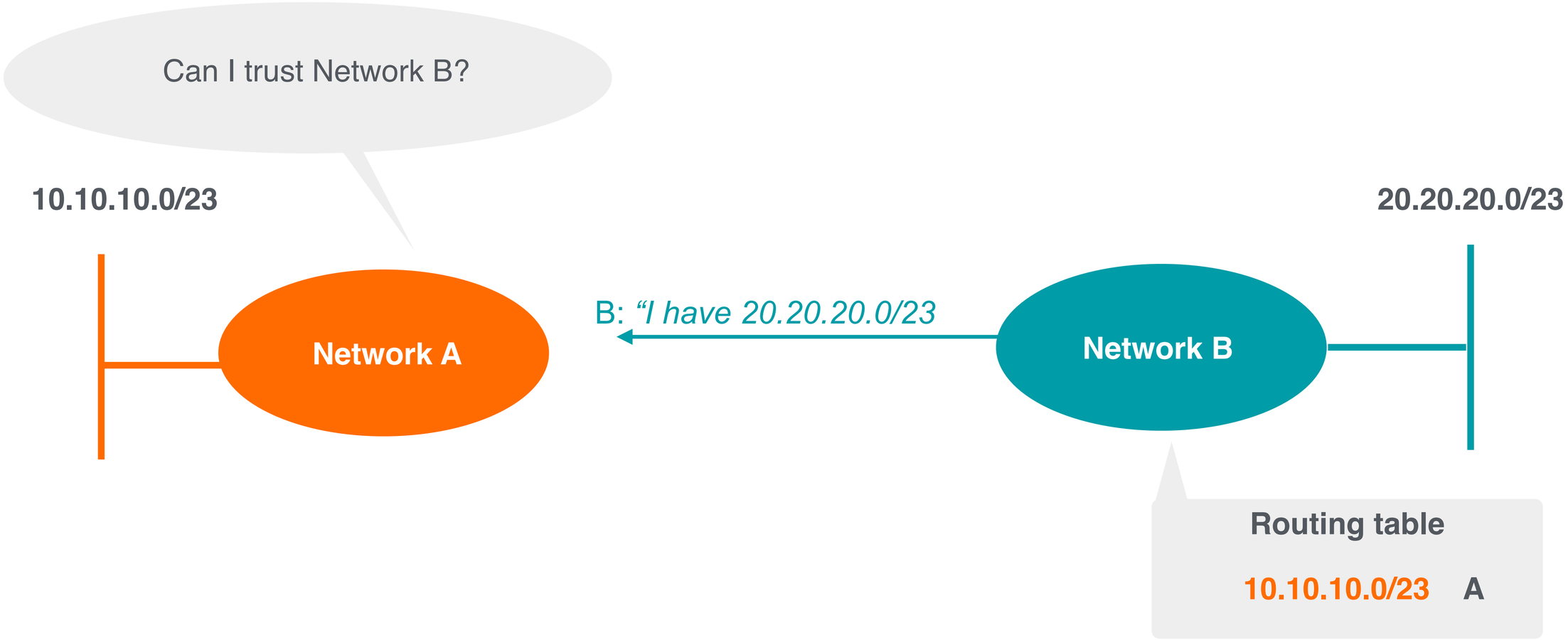
How does it work?



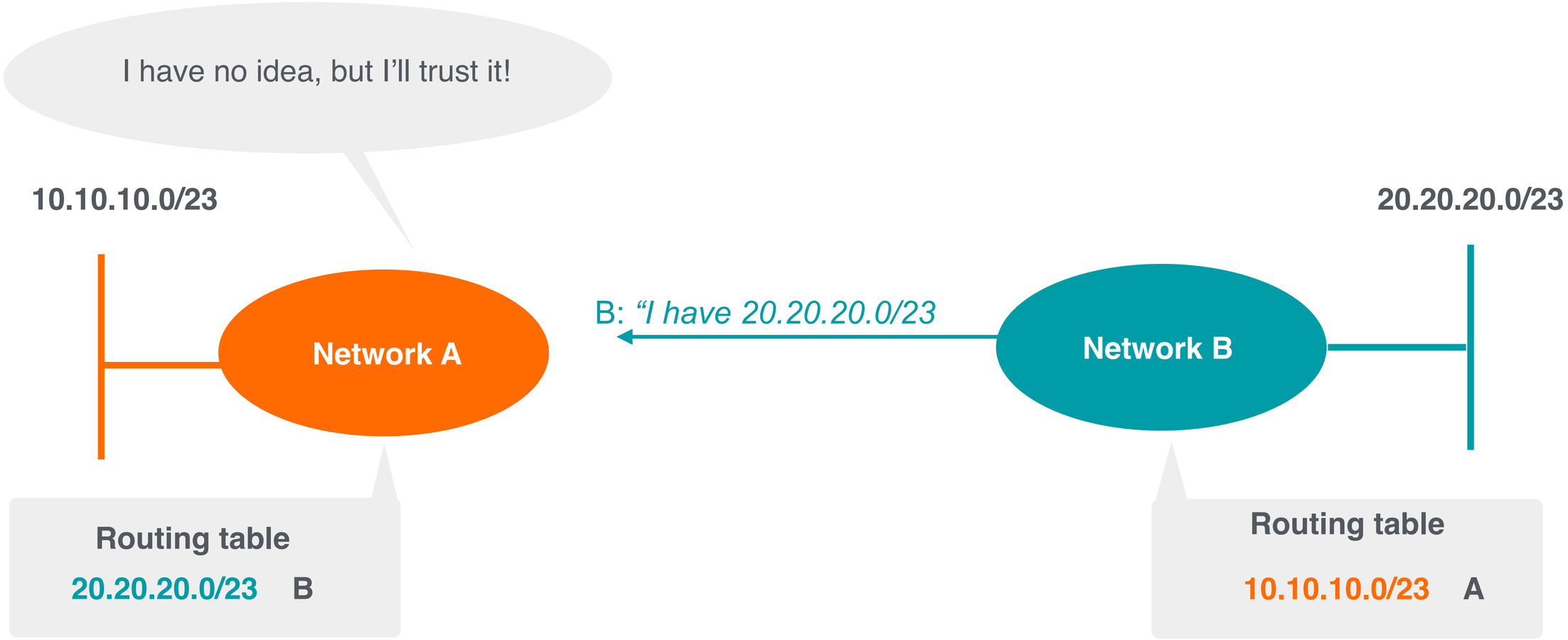
How does it work?



How does it work?



How does it work?



BGP is just based on **trust!**

No built-in security in BGP!

- Any AS can announce any prefix
- Anyone can prepend any ASN to the BGP path
- BGP announcements are accepted without validation
- BGP packets are transmitted without any encryption or authentication mechanisms
- No single authoritative source for who should be doing what

No built-in security in BGP!

- Any AS can announce any prefix
- Anyone can prepend any ASN to the BGP path
- BGP announcements are accepted without validation
- BGP packets are transmitted without any encryption or authentication mechanisms
- No single authoritative source for who should be doing what

BGP is vulnerable to attacks!

Sometimes it happens accidentally!

- Typing errors
  - Also known as “fat fingers”
  - May cause mis-origination
- Configuration errors
  - Faulty BGP filter configuration
  - AS path prepending mistakes
  - Cause routing policy violations and unintentional route leaks

Accidental or intentional…
Internet routing infrastructure is **affected!**

In order to secure routing…

- We need to verify the routing information (Is it correct or not?)
  - Verify if the prefix is originated by the legitimate holder
- Prevent propagation of incorrect routing information

But how?

1. **Check prefixes** before announcing

2. **Register** your routing information in **IRRs**

3. **Filter** BGP routes from your peers, customers and upstreams

4. Implement BGP filters based on **verifiable information**

IRRs are good, but not enough!

Concerns with the IRR system

1

Not globally deployed

Just distributed databases

2

No central authority

Who will verify the accuracy of the data?

3

No verification of holdership

Anyone can input anything

4

Not updated properly

Information is missing, outdated or incorrect

As a result…

IRRs are not so accurate

Data in IRRs is incomplete

They’re not well-maintained

IRR filters are good **only if the IRR entries are correct!**

That’s why the Internet community came up with the **RPKI** solution!

What is RPKI?

Resource Certification

What is RPKI?

- RPKI is…
  - A resource certification (X.509 PKI certificates)
  - A security framework
- It is used to make Internet routing more secure and reliable

How does RPKI help with routing security?

- Verifies the association between resource holders and their Internet number resources.
  - Proves holdership through a public key and certificate infrastructure
- Used to validate the origin of BGP announcements
  - Is the originating ASN authorised to originate a particular prefix?
- Stepping stone to “Path Validation”

How does it work?

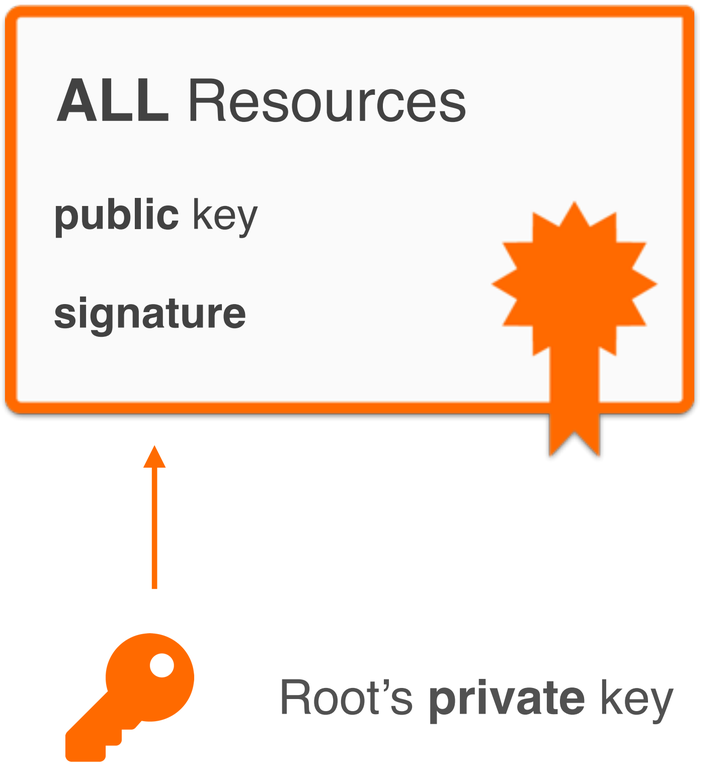
Ties IP addresses and ASNs to public keys

Follows the RIR hierarchy

Authorised statements from resource holders

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

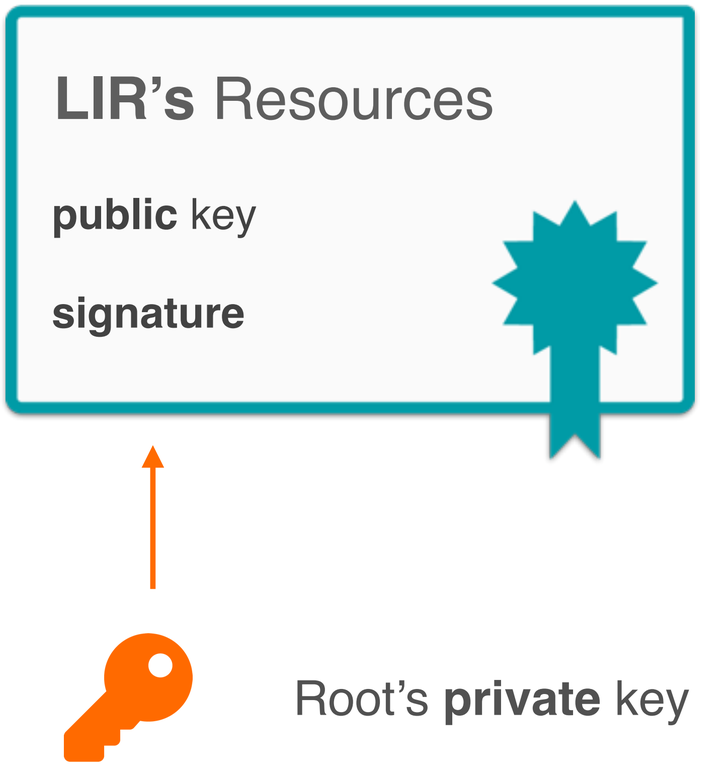
RIPE NCC Root Certificate



Self-signed

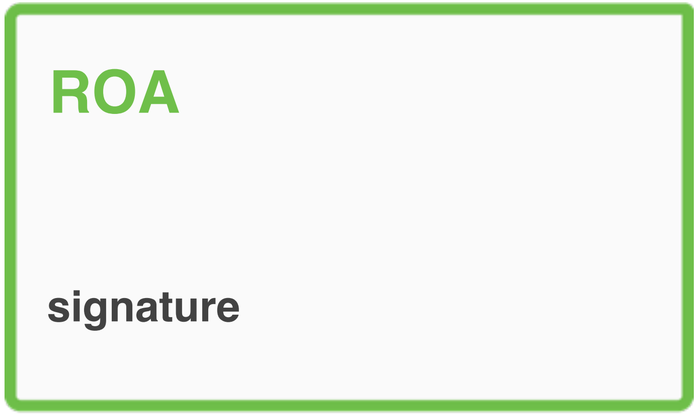
Root's **private** key

LIR Certificate



Signed by the root's private key

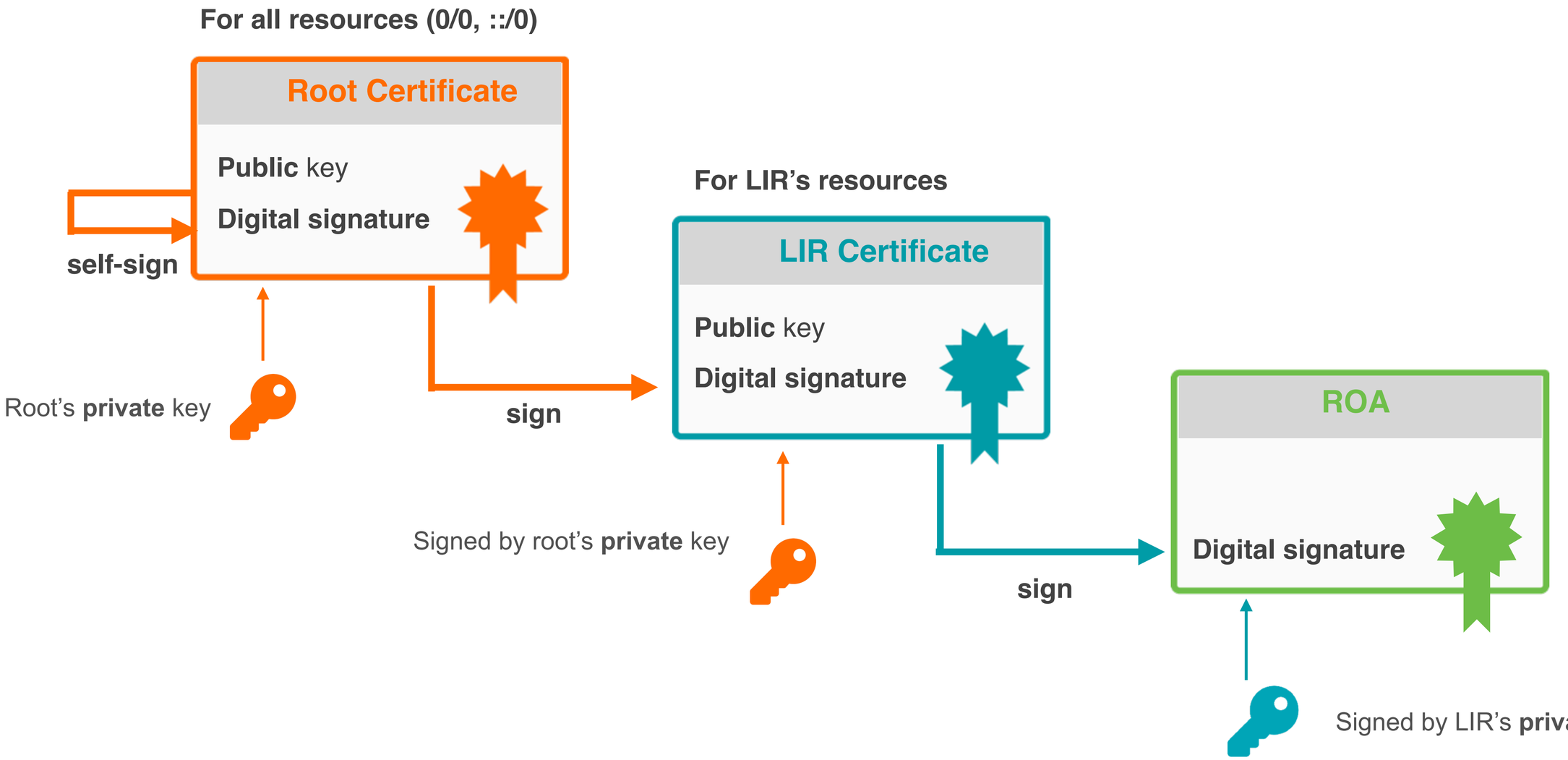
Authorised Statement



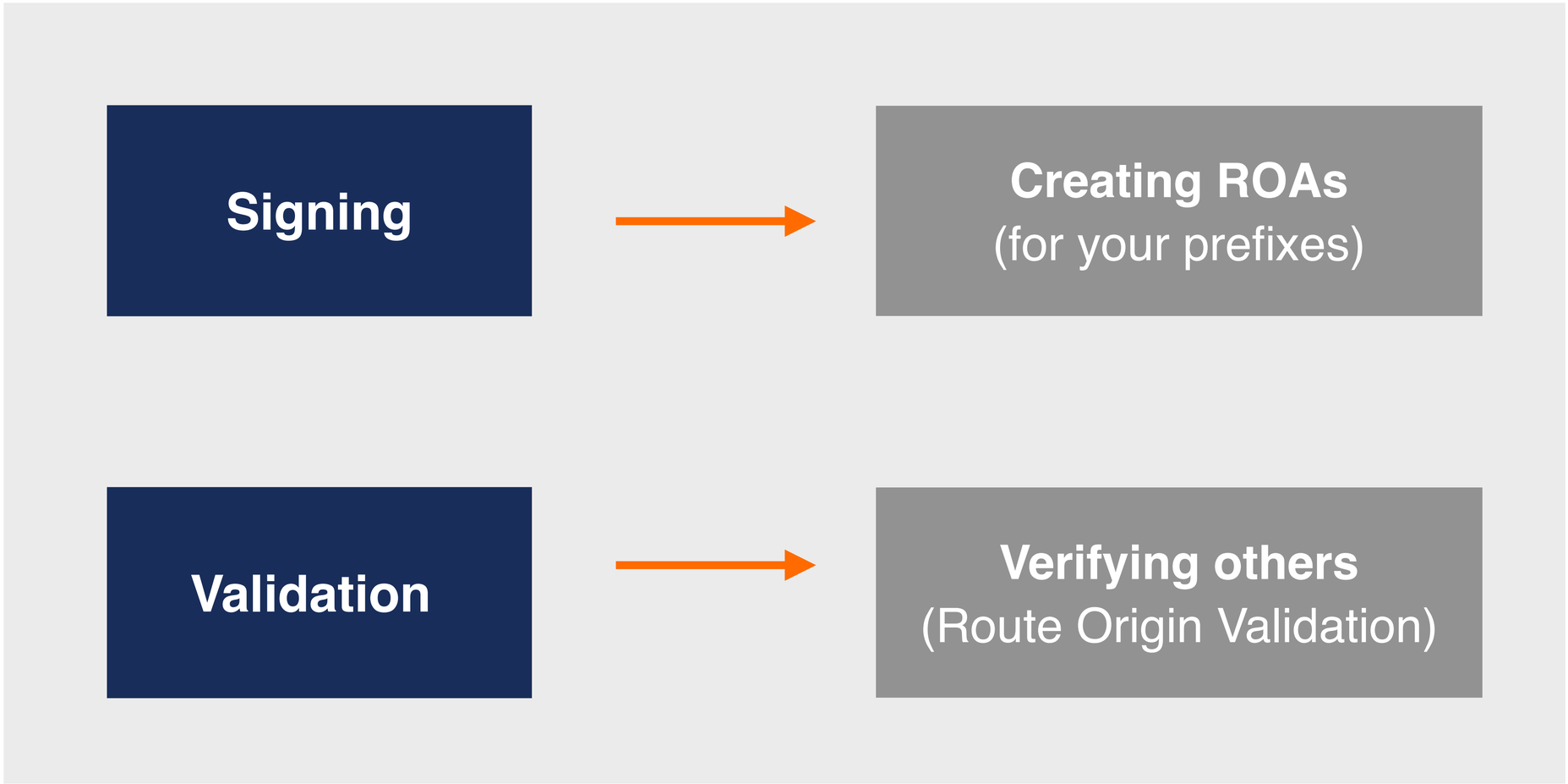
Signed by LIR’s private key

LIR’s **private** key

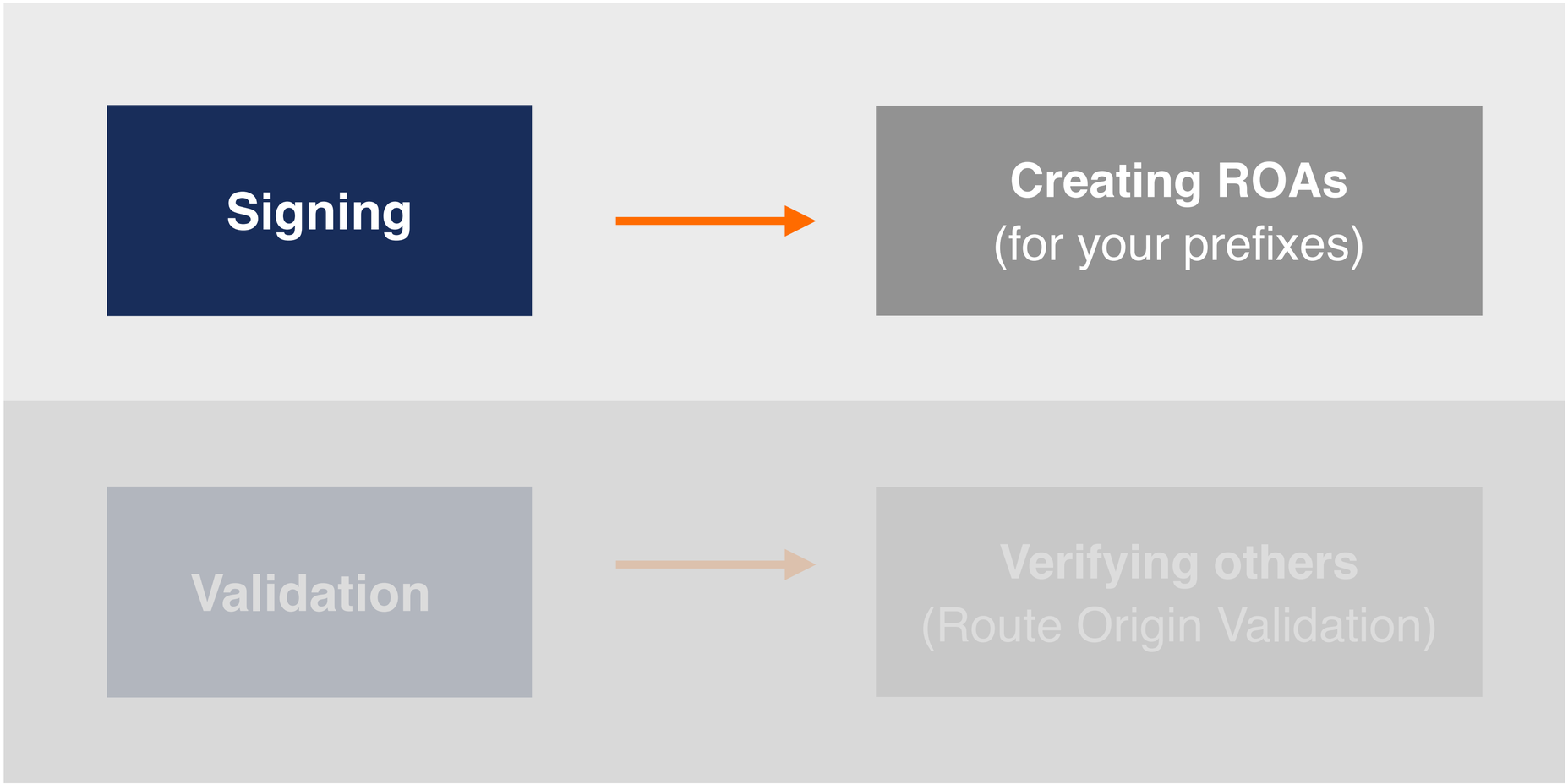
RPKI Chain of Trust



RPKI has two elements



RPKI has two elements

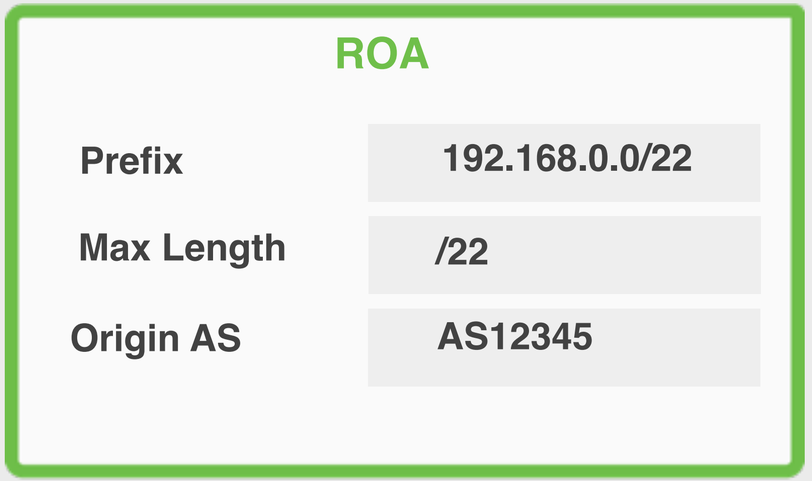


ROA

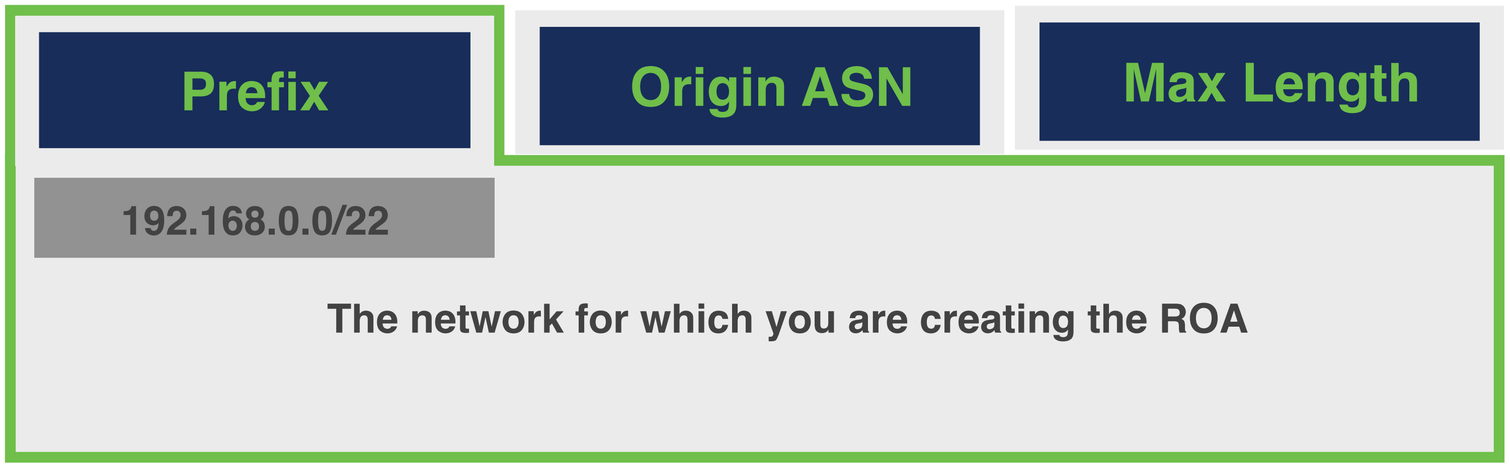
Route Origin Authorisation

ROA (Route Origin Authorisation)

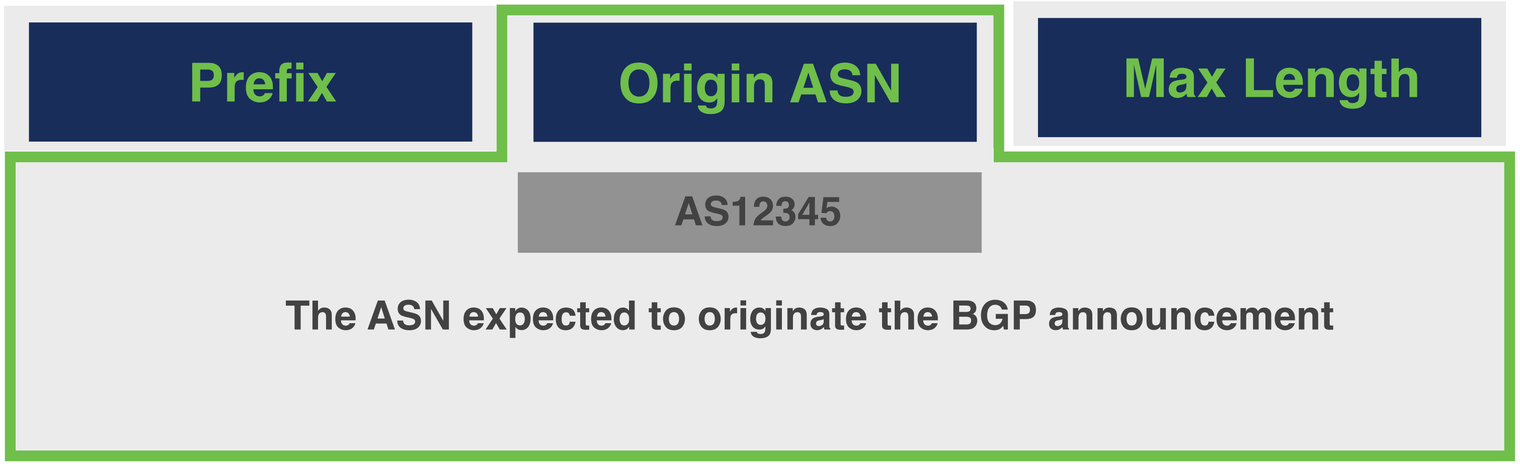
- An authorised statement created by the resource holder
- Contains a list of address prefixes and an AS Number
- LIRs can create a ROA for their resources
- Multiple ROAs can exist for the same prefix
- ROAs can overlap



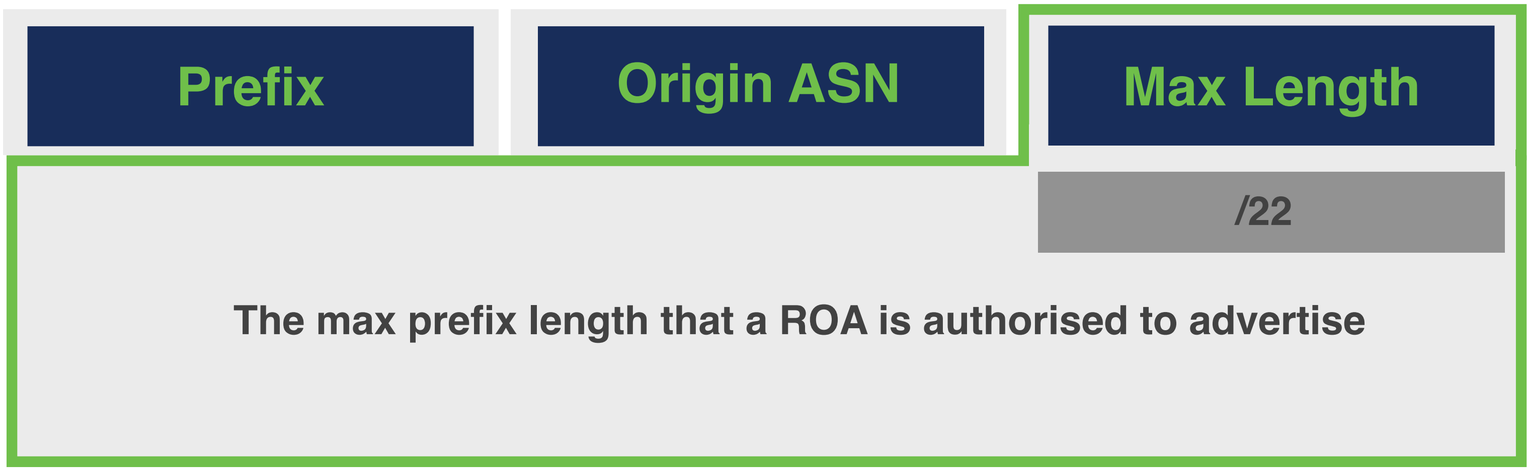
What is in a ROA?



What is in a ROA?



What is in a ROA?



Max Length

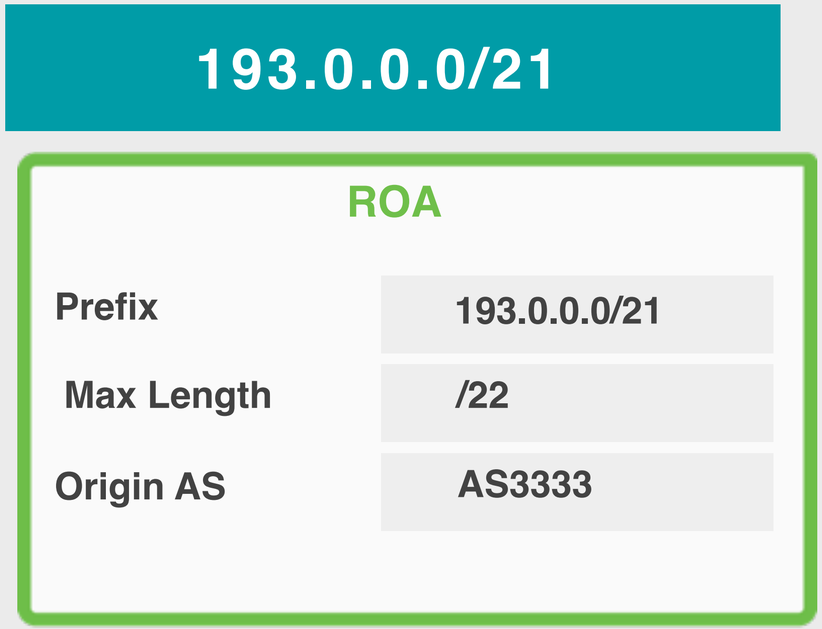
AS3333 has an IP address allocation

193.0.0.0/21

Max Length

AS3333 has an IP address allocation

AS3333 creates this ROA



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

193.0.0.0/21

ROA

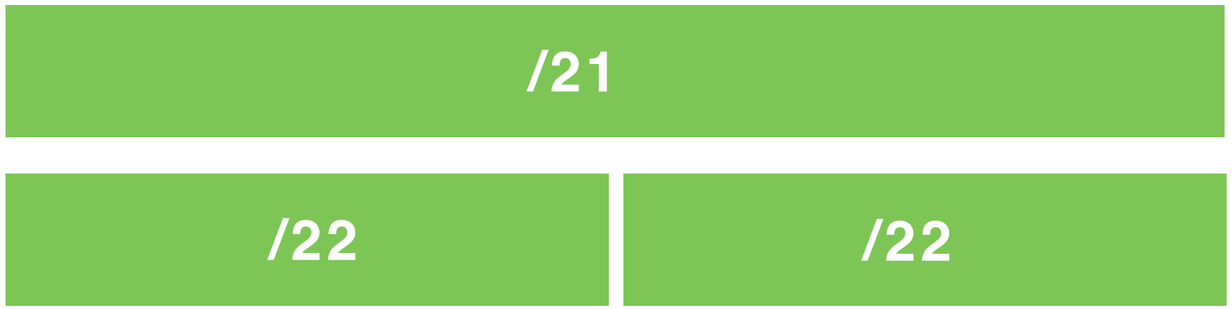
Prefix	**193.0.0.0/21**
Max Length	**/22**
Origin AS	**AS3333**

Max Length

AS3333 has an IP address allocation

AS3333 creates this ROA

According to ROA:



193.0.0.0/21

ROA

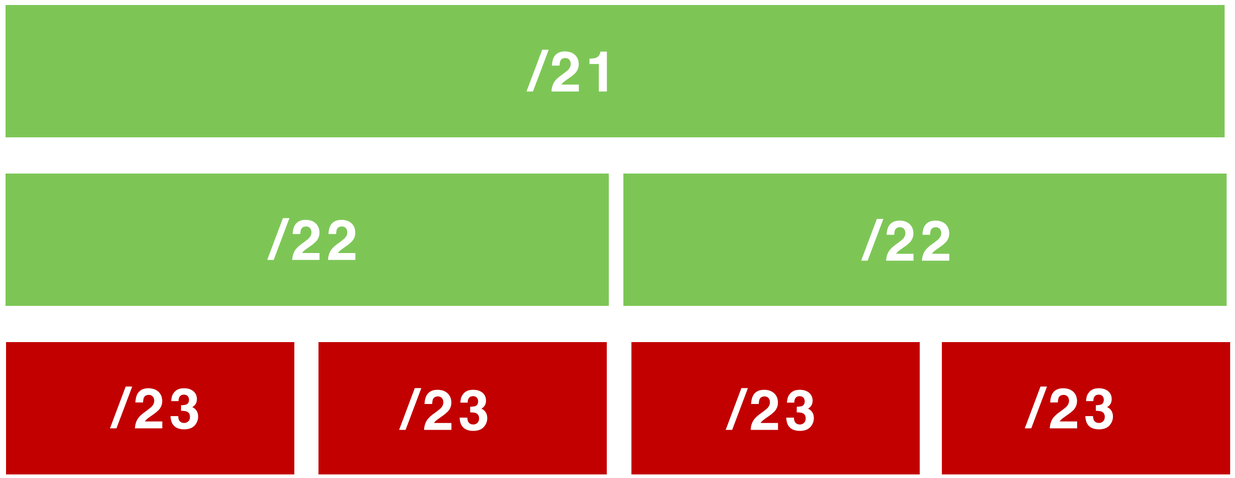
Prefix	193.0.0.0/21
Max Length	/22
Origin AS	AS3333

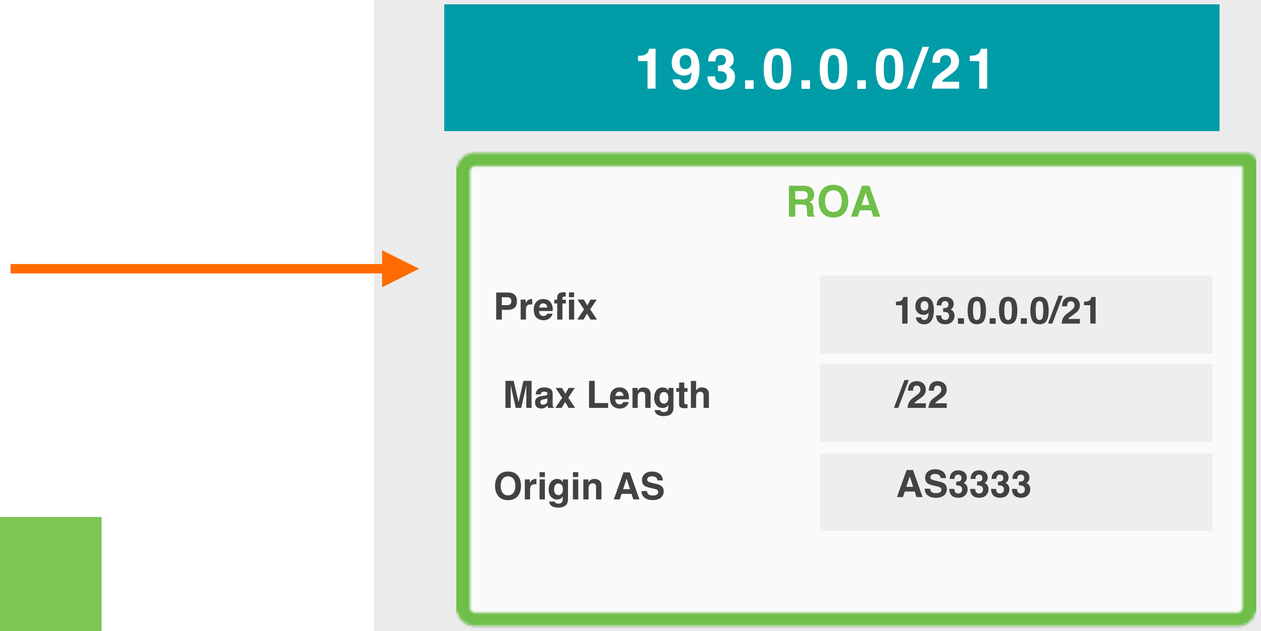
Max Length

AS3333 has an IP address allocation

AS3333 creates this ROA

According to ROA:



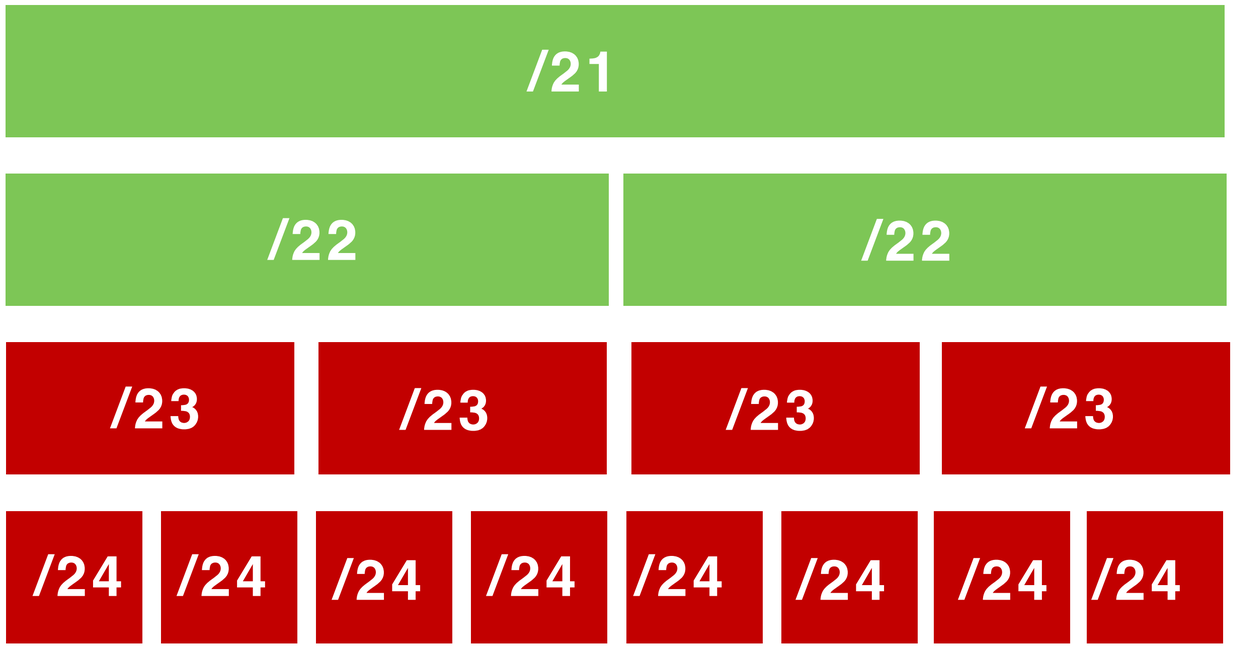


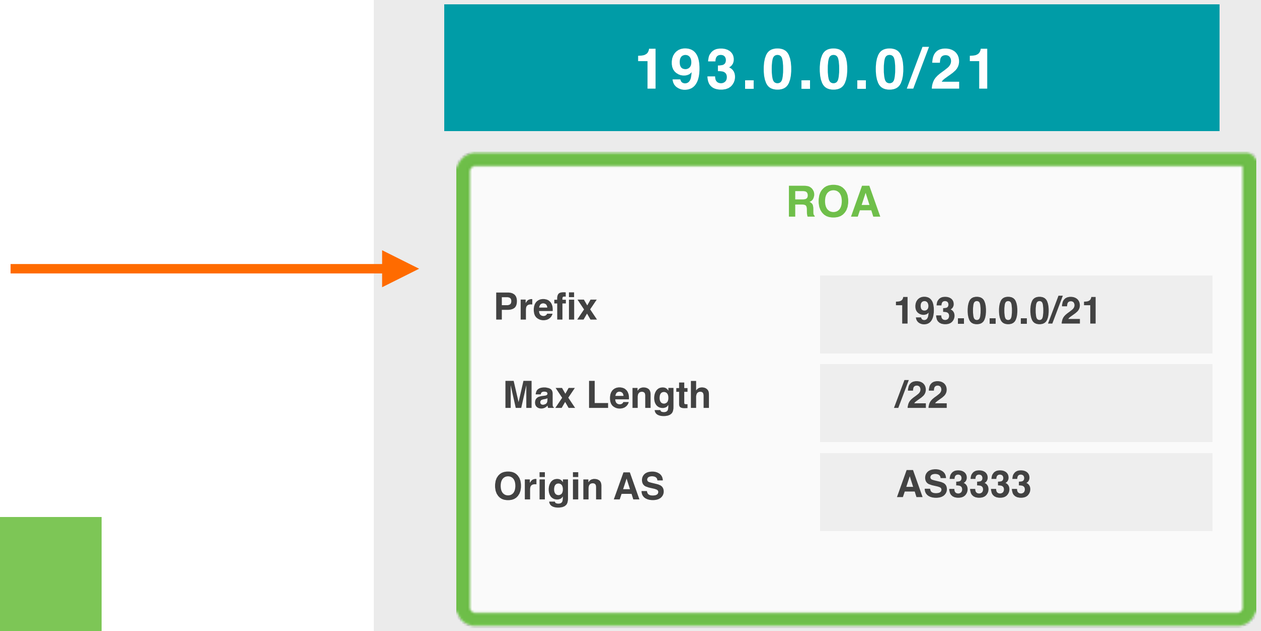
Max Length

AS3333 has an IP address allocation

AS3333 creates this ROA

According to ROA:



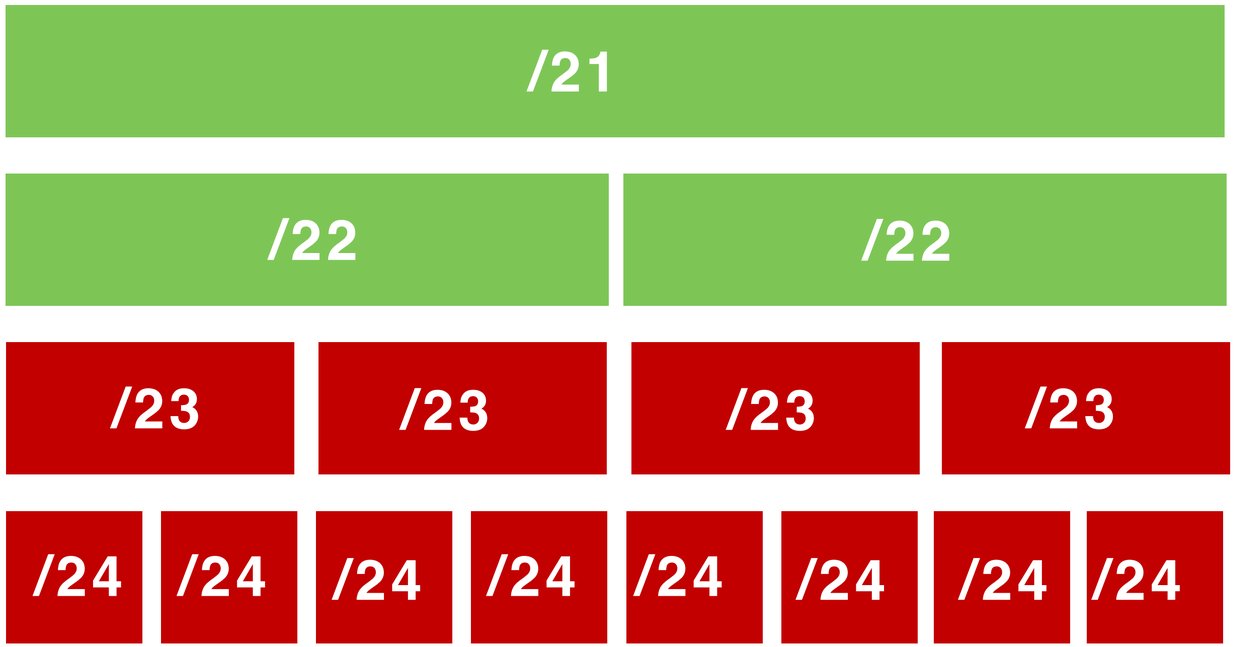


Max Length

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

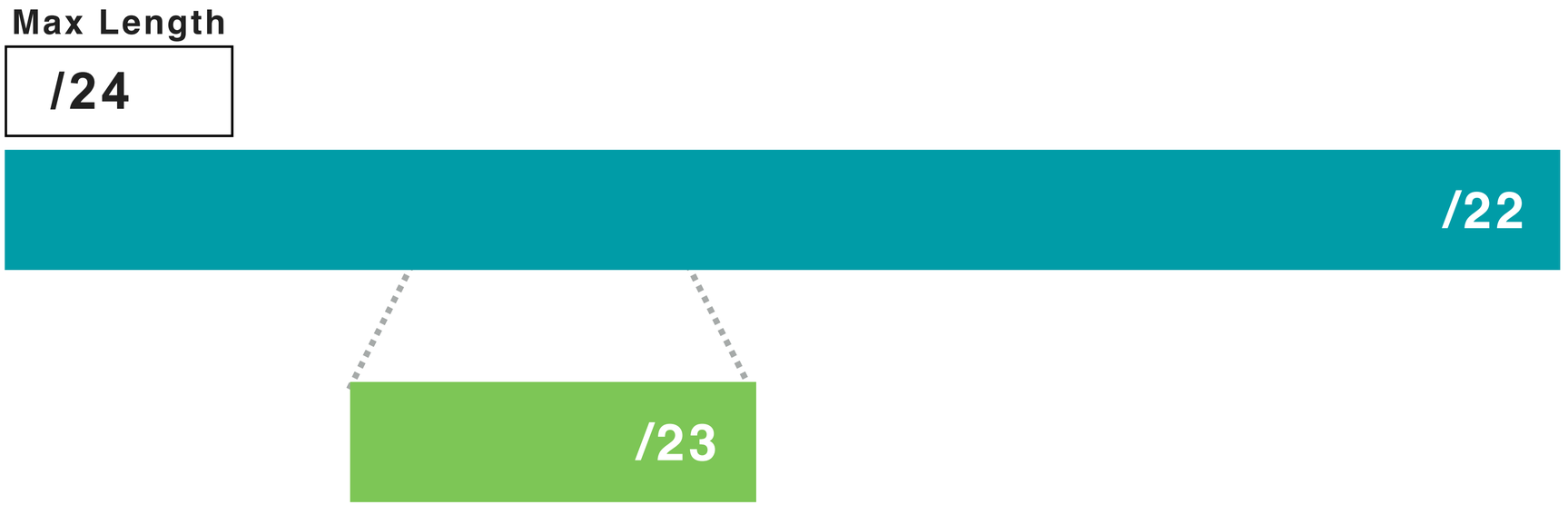
Any more specific announcements are unauthorised by the ROA

How should we use Max Length?

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

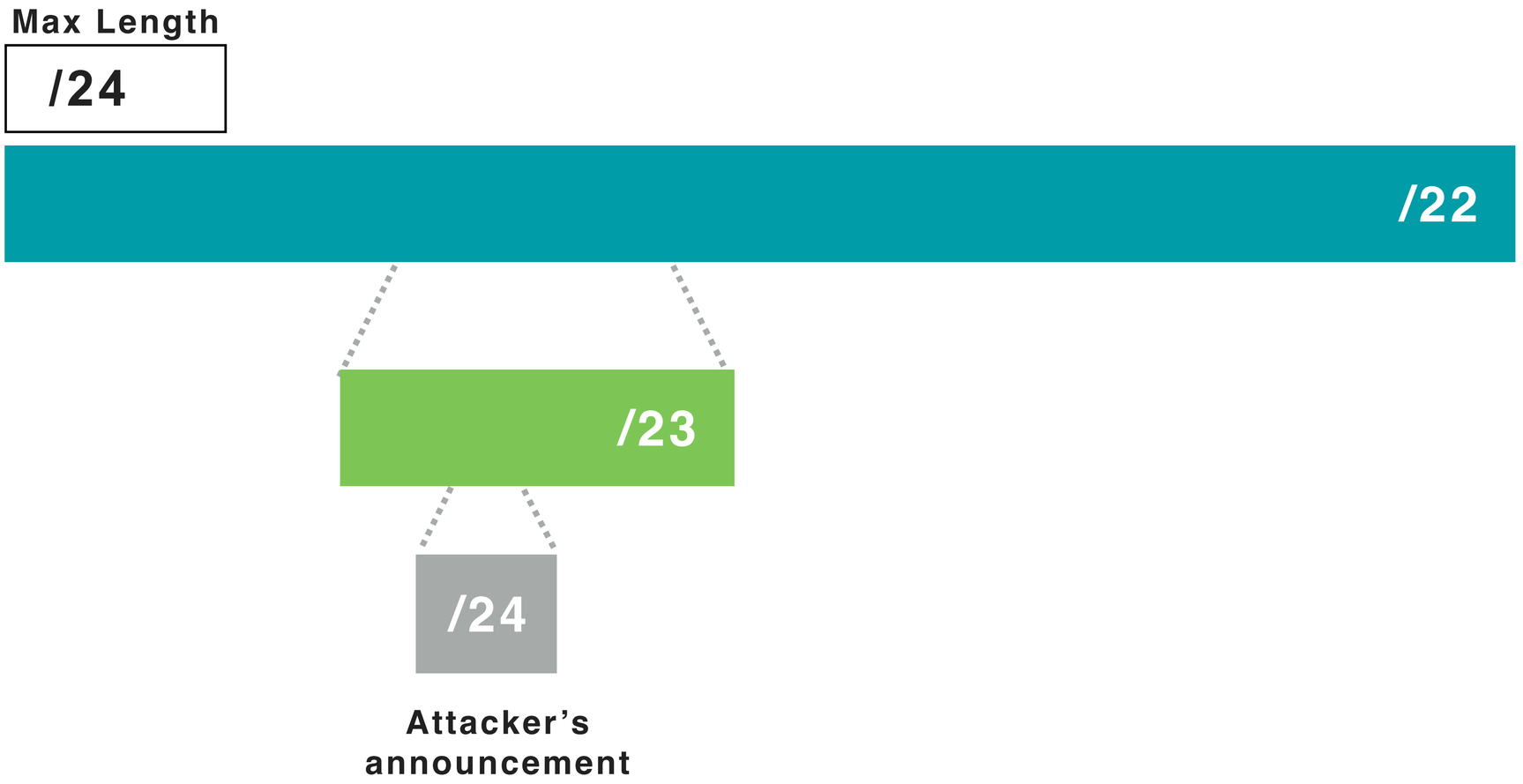
How should we use Max Length?

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



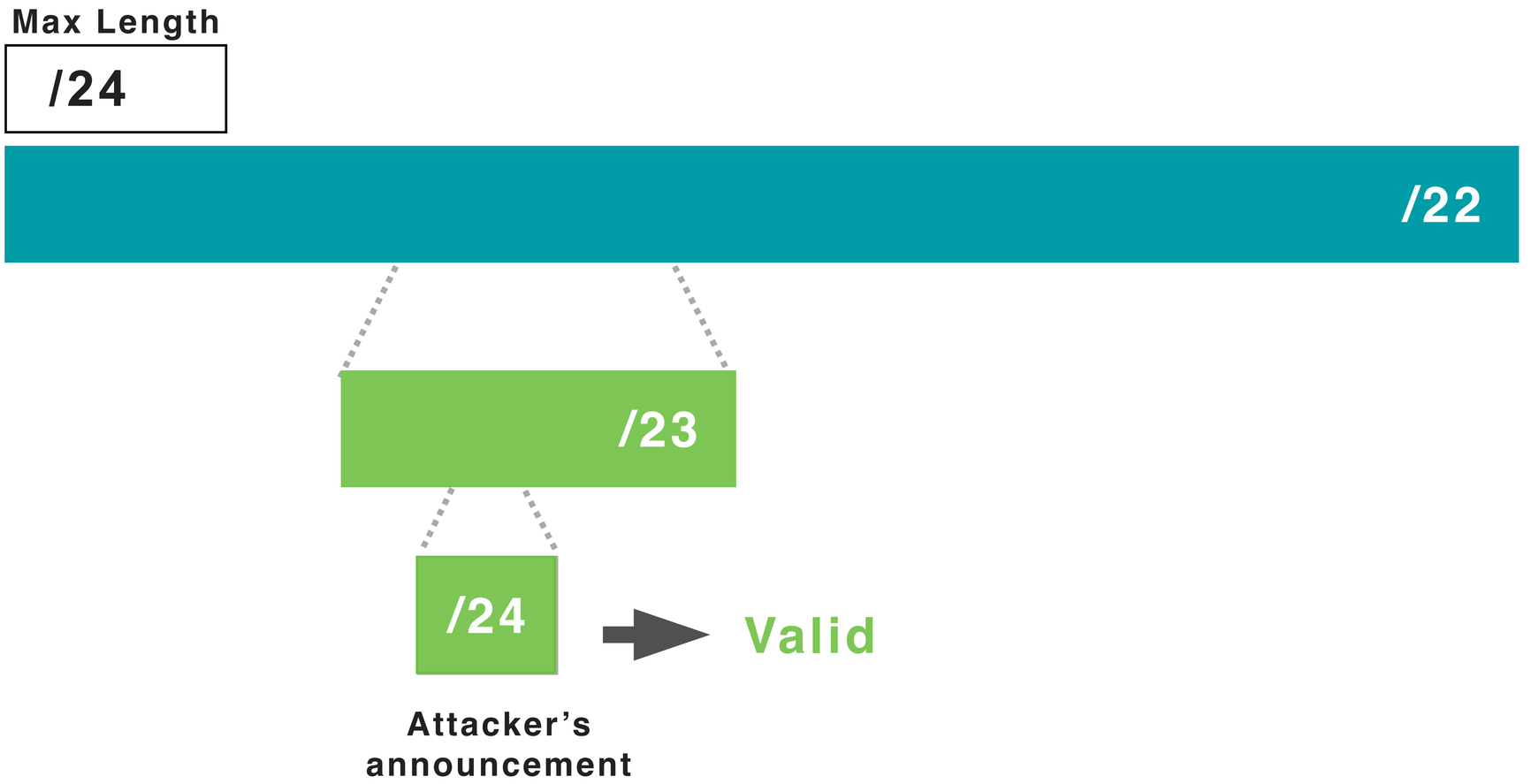
How should we use Max Length?

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

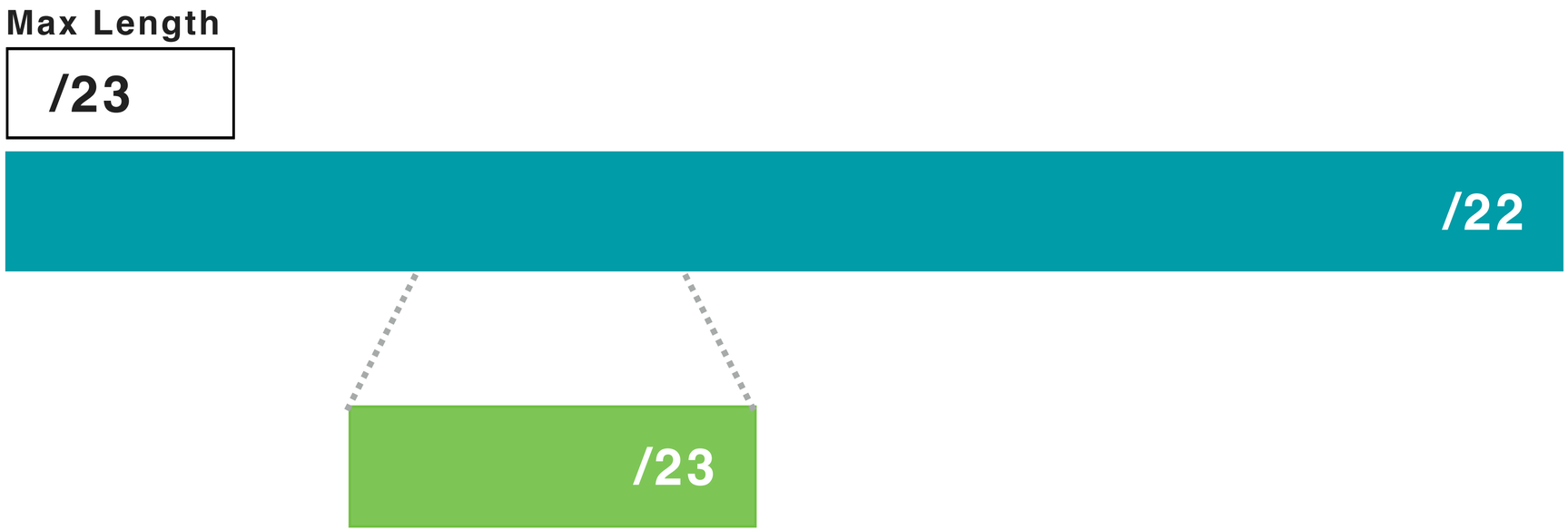


How should we use Max Length?

Case 2: You create a ROA only for your BGP announcements

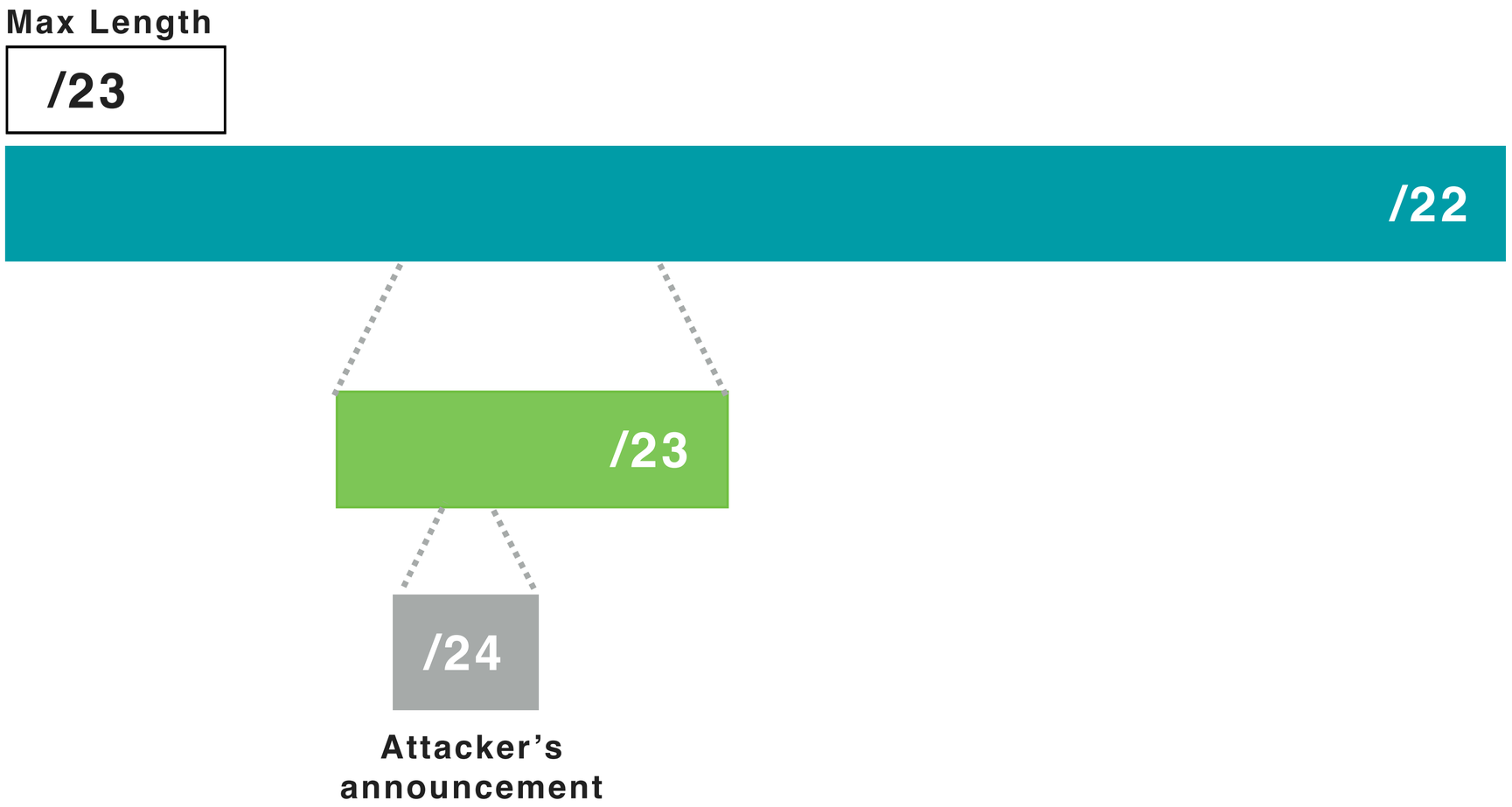
How should we use Max Length?

Case 2: You create a ROA only for your BGP announcements



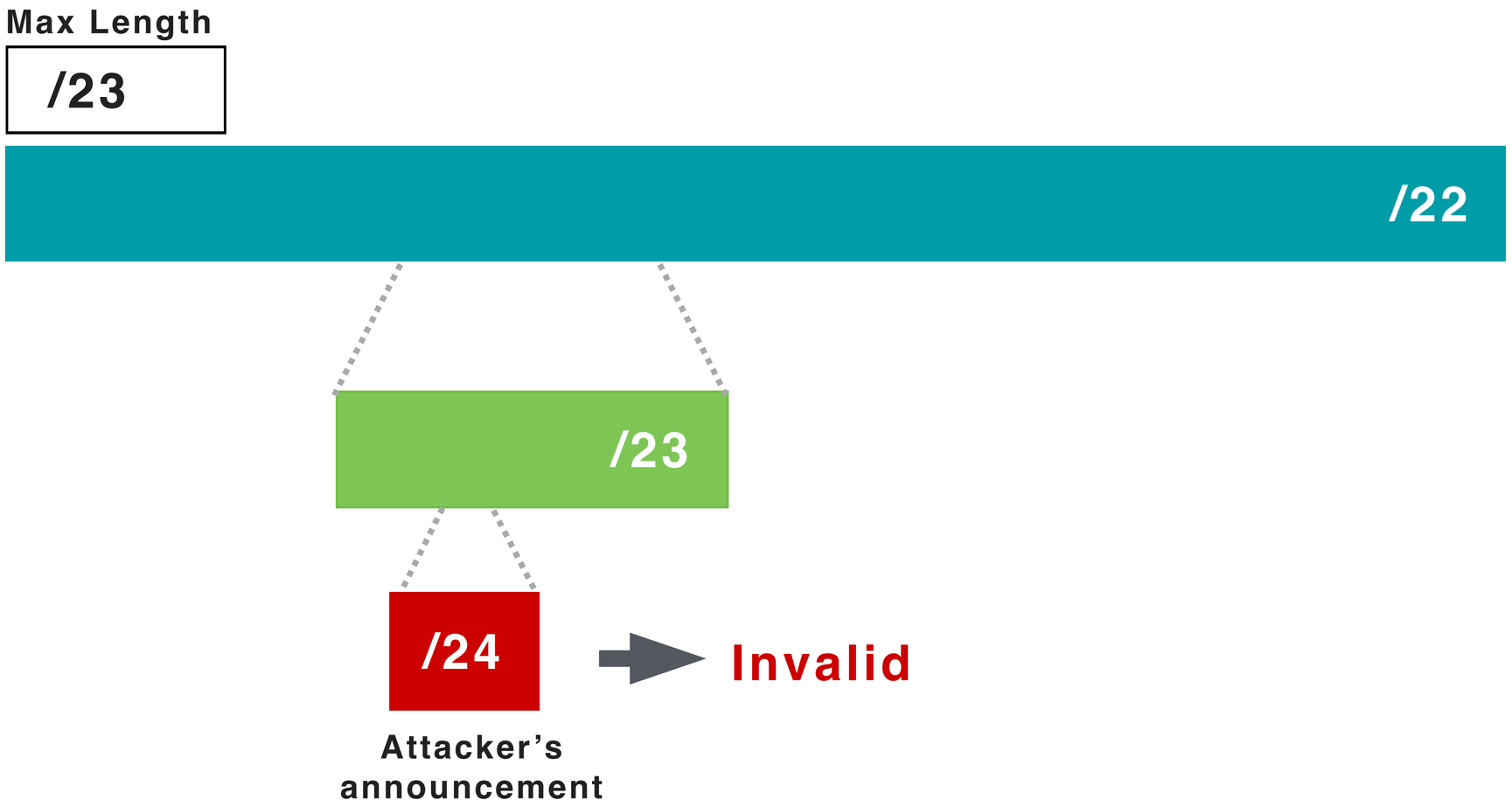
How should we use Max Length?

Case 2: You create a ROA only for your BGP announcements



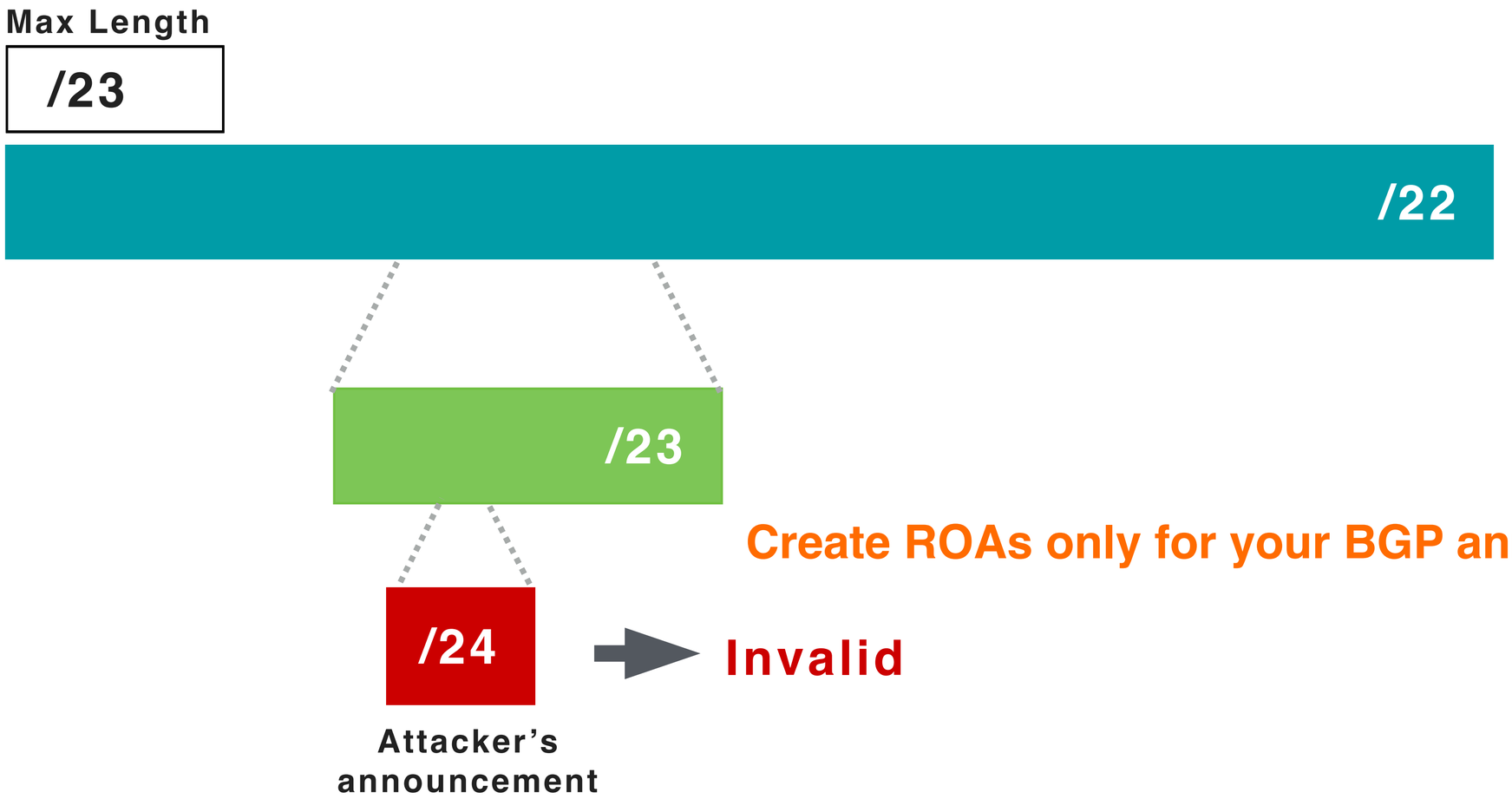
How should we use Max Length?

Case 2: You create a ROA only for your BGP announcements



How should we use Max Length?

Case 2: You create a ROA only for your BGP announcements



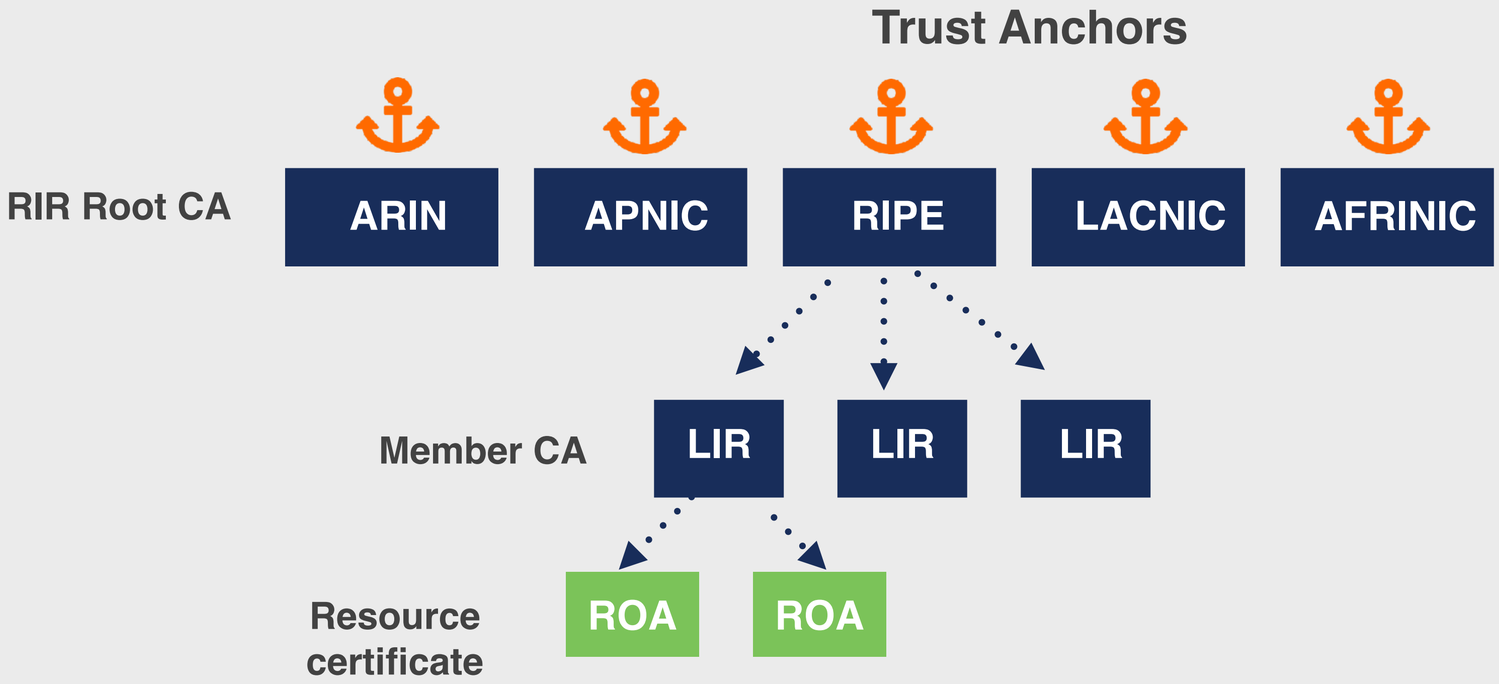
Create ROAs only for your BGP announcements!

How to create a ROA?

Registering routing info in the RPKI system

RPKI Certificate Structure

- RPKI relies on RIRs
- 5 RIRs run a root CA with a Trust Anchor
- RIRs can verify who is creating objects in the RPKI system

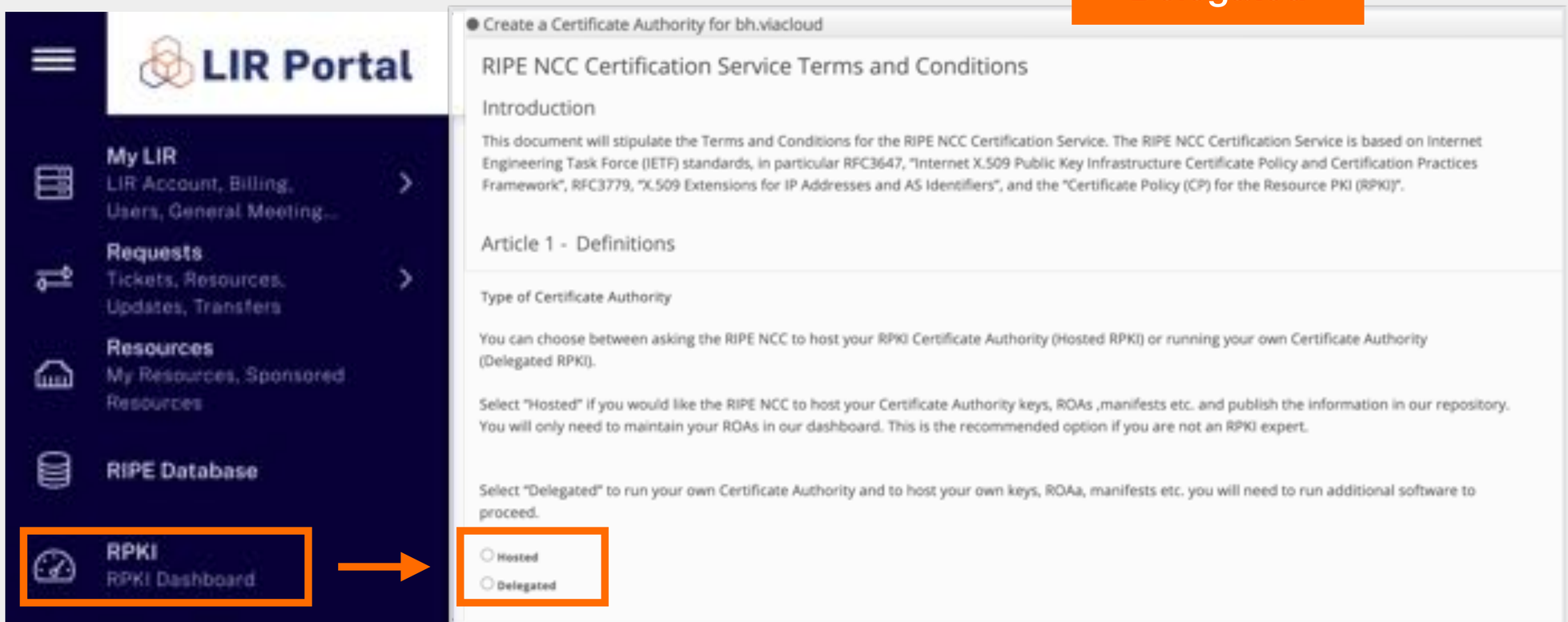


How to create a ROA?

1. Login to LIR Portal (my.ripe.net)
2. Go to the RPKI Dashboard
3. Choose which RPKI model to us

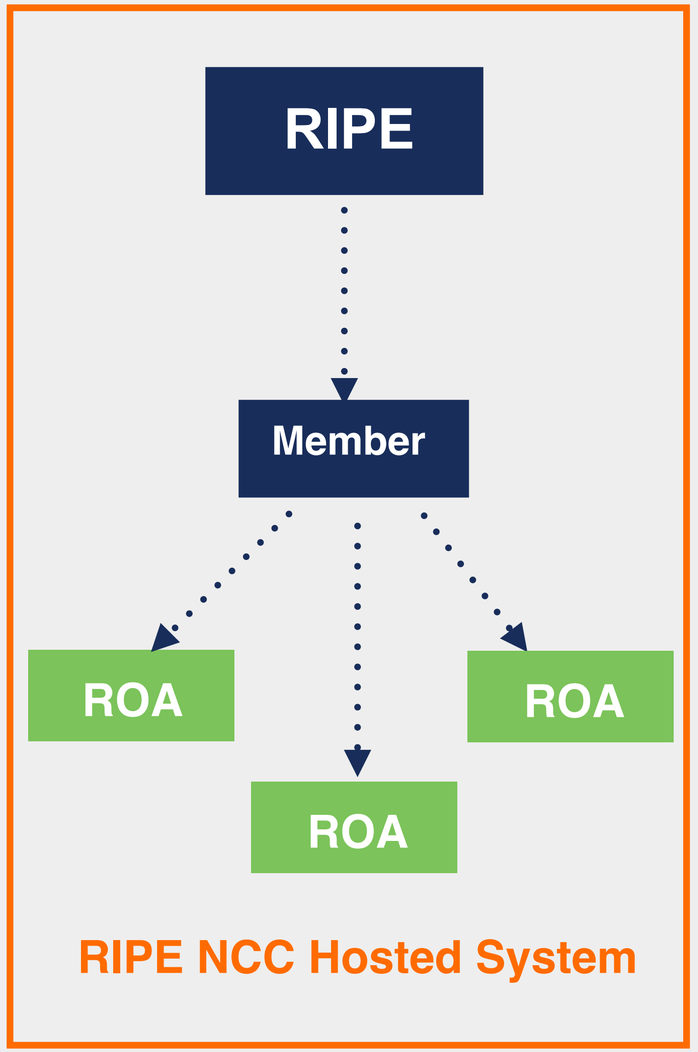
Hosted

Delegated



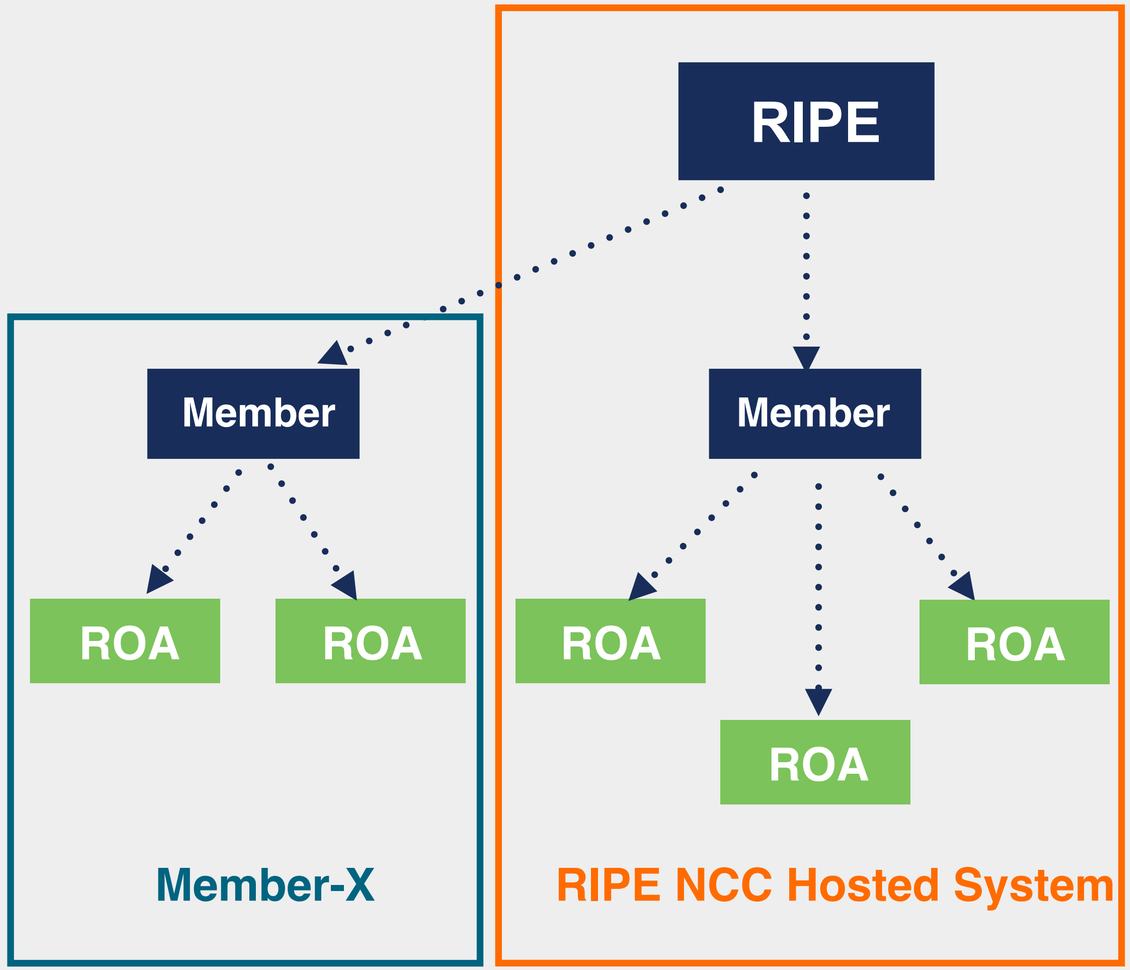
Hosted RPKI

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

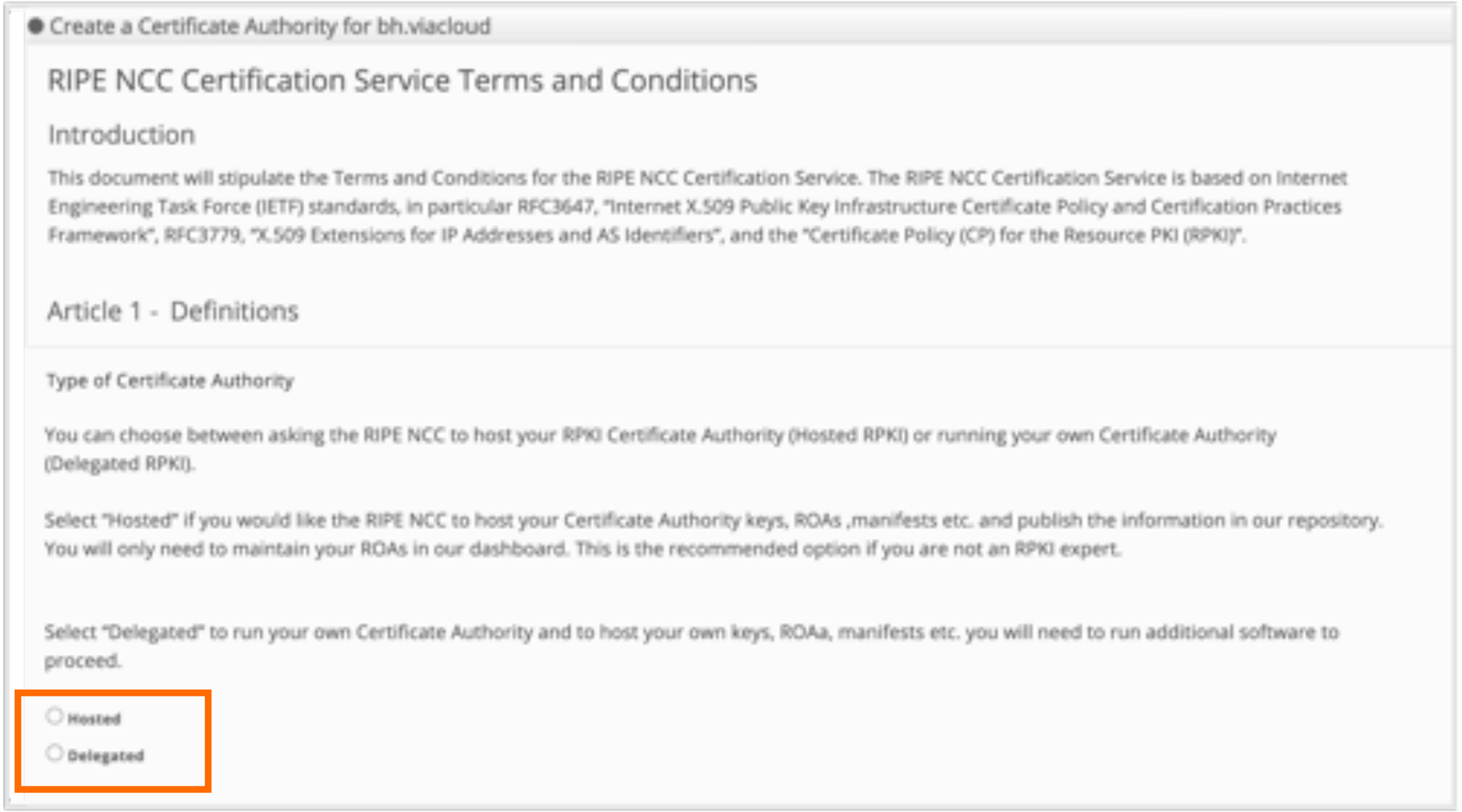


Delegated RPKI

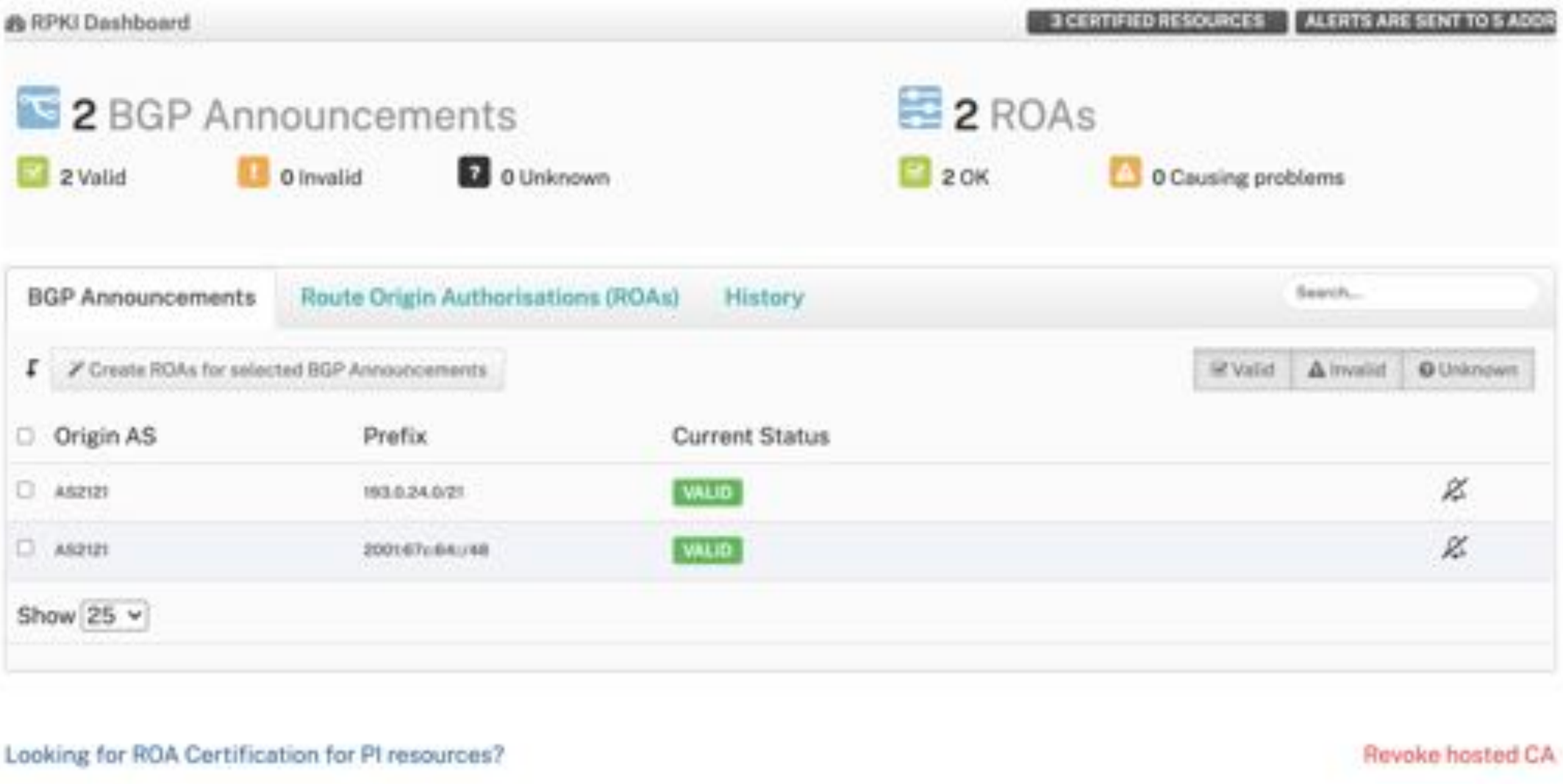
- Run your own Certificate Authority software
  - Dragon Research Labs, RPKI Toolkit
  - NLnet Labs, Krill
- Create ROAs in your own platform
- Manage your own keys/key rollovers
- Set up connection with RIPE NCC CA
- Generate LIR certificate and get it signed by parent CA



RIPE NCC RPKI Dashboard



RIPE NCC Hosted Solution



RIPE NCC Hosted Solution

Certifying PI Resources

Requested and managed by PI End User or by Sponsoring LIR

1. Complete the wizard successfully

2. Log in 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!

Connect to Localcert:
https://localcert.ripe.net/#/

3 min.

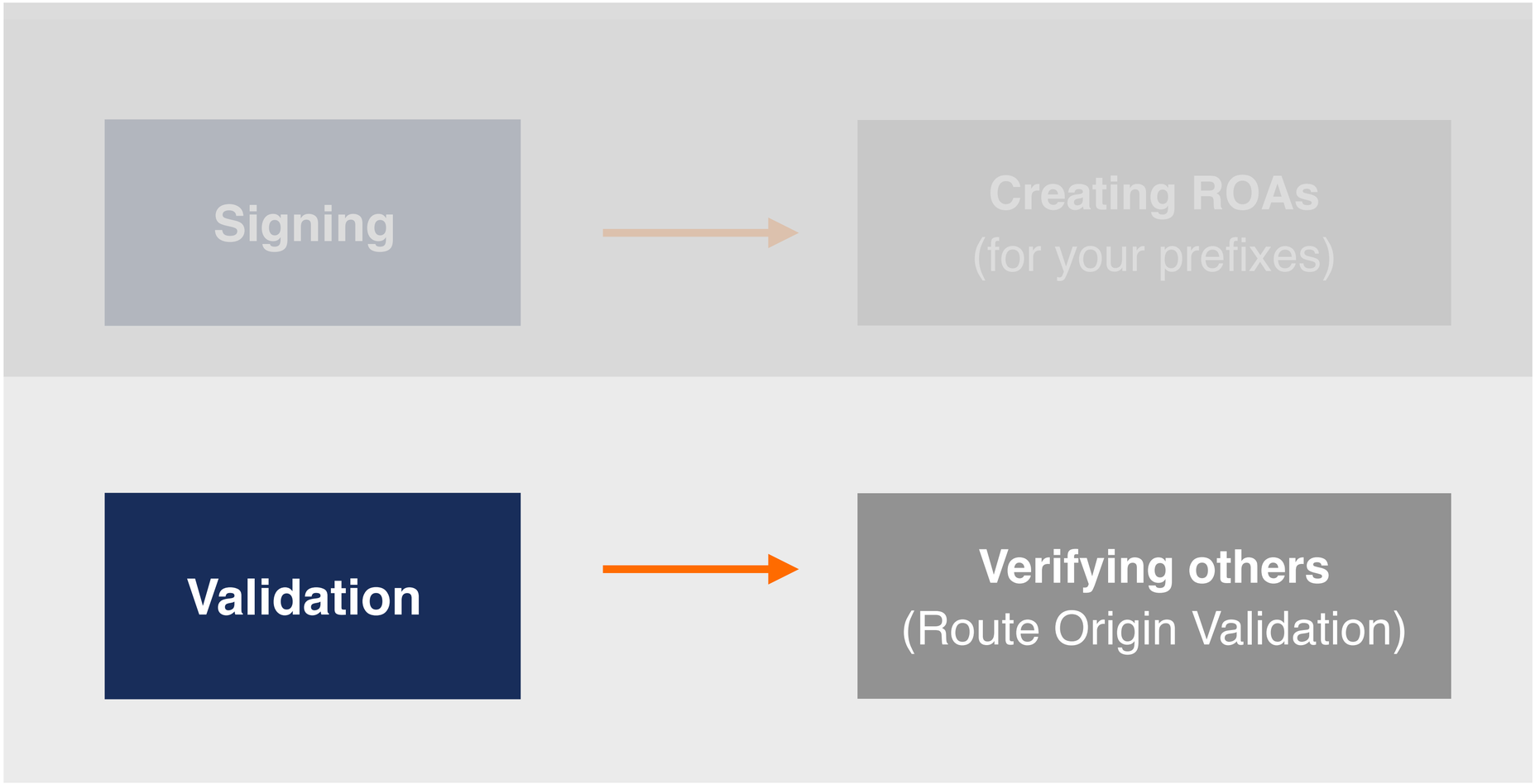

Let’s take a
5-minute
break!


WELCOME
WE ARE
OPEN
PLEASE COME IN

RPKI Validation

Deploying RPKI Validators

RPKI has two elements



RPKI Validation

- Verifying the information provided by others
- Goal is to validate the “origin of BGP announcements”
- Known as:
  - BGP Origin Validation (BGP OV) or
  - Route Origin Validation (ROV)

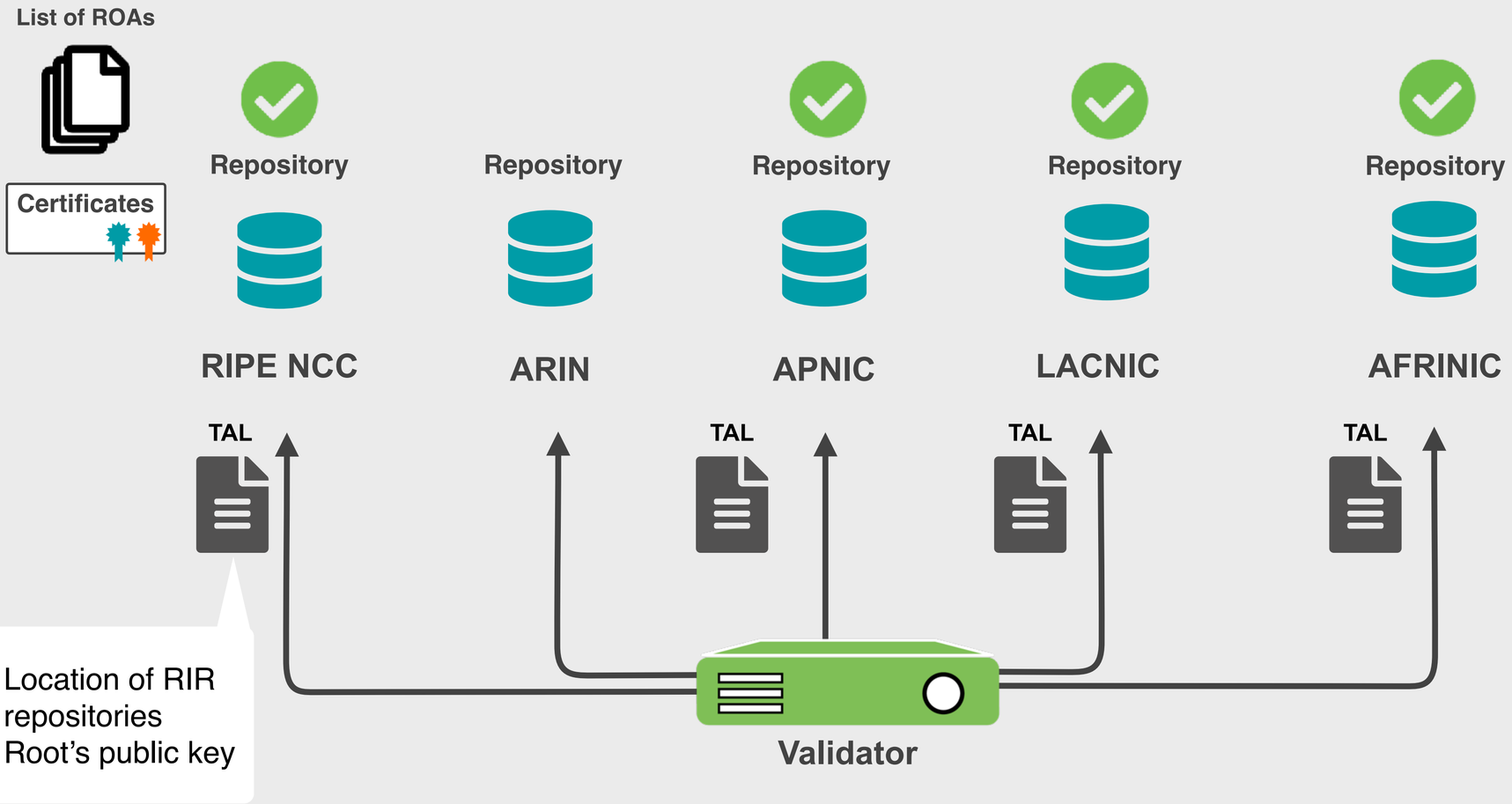
In order to validate BGP announcements…

- You need to:
  - Install a validator software locally in your network
  - Download all ROAs from RIR repositories
  - Validate ROAs by using a validator
  - Compare valid ROAs with BGP announcements
- Then you can make decisions based on the validation results

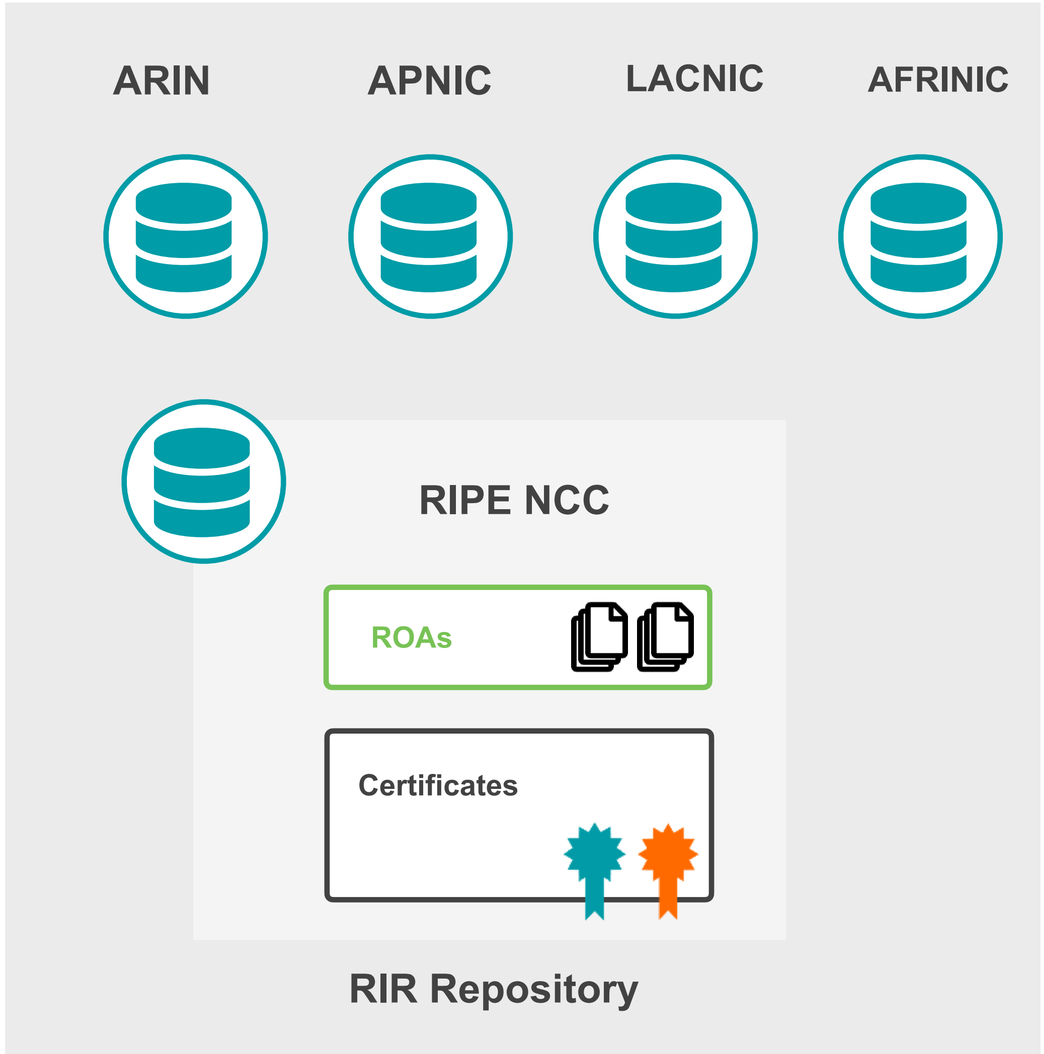
RPKI Validators

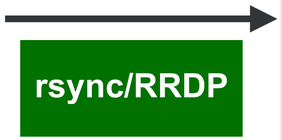
- Also known as Relying Party Software
- Download the RPKI repositories from RIRs
- Validate the chain of trust for all ROAs and associated CAs
- Create a local “validated cache” with all the valid ROAs
- Talk to routers using RPKI-RTR Protocol

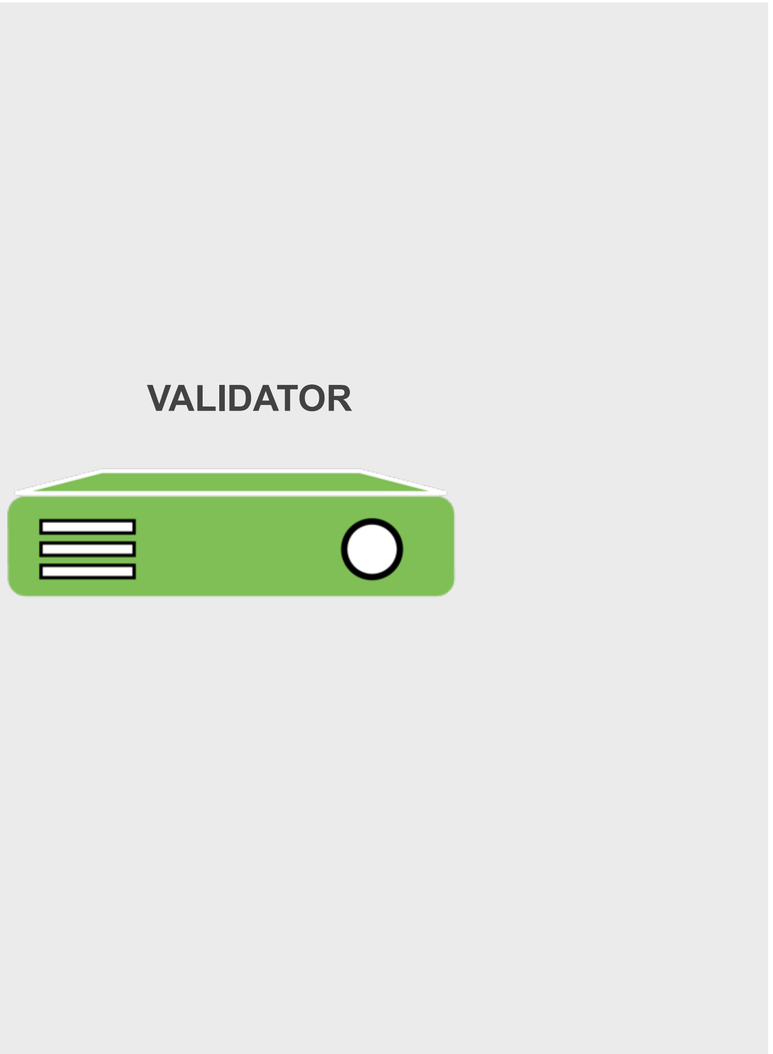
Trust Anchor Locator (TAL)



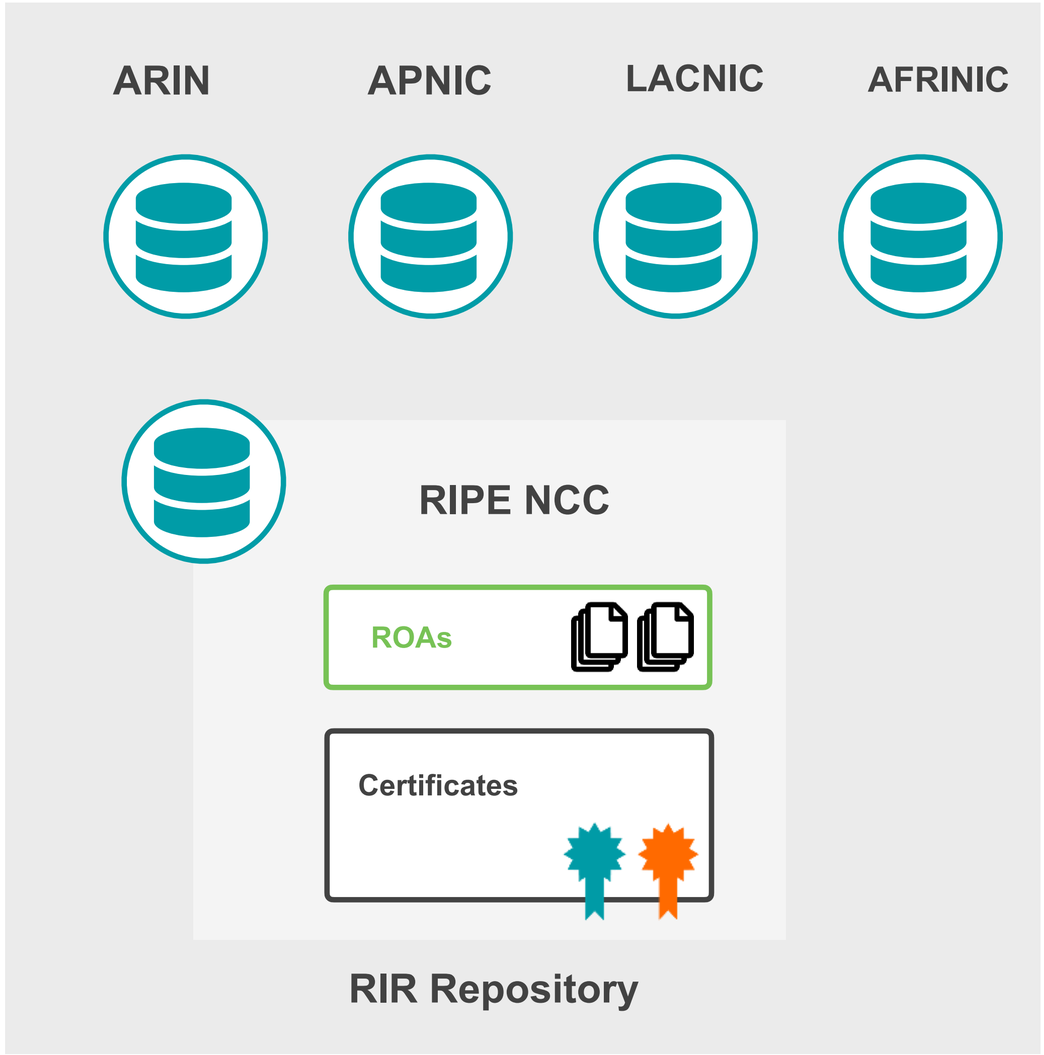
RPKI Validators

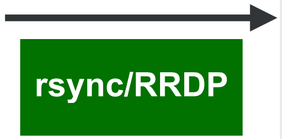


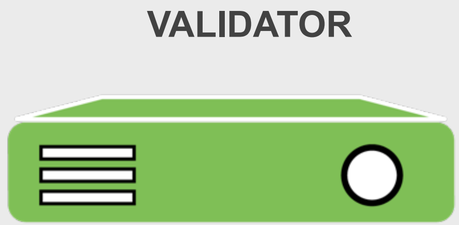




RPKI Validators





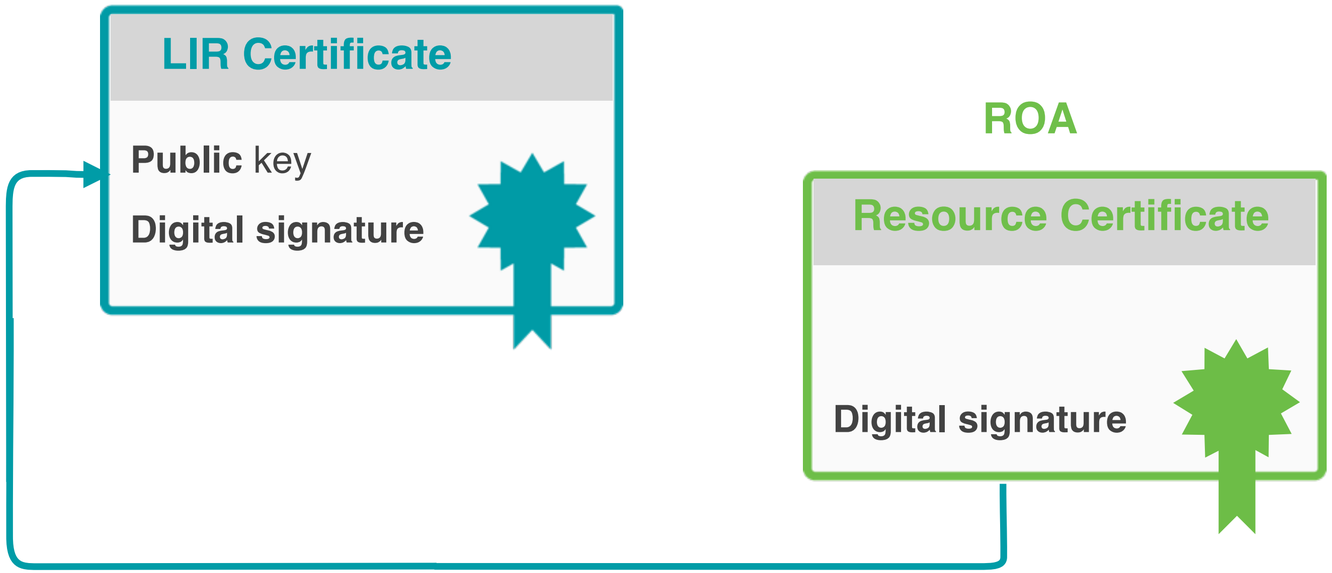


Validator, validates the chain of trust

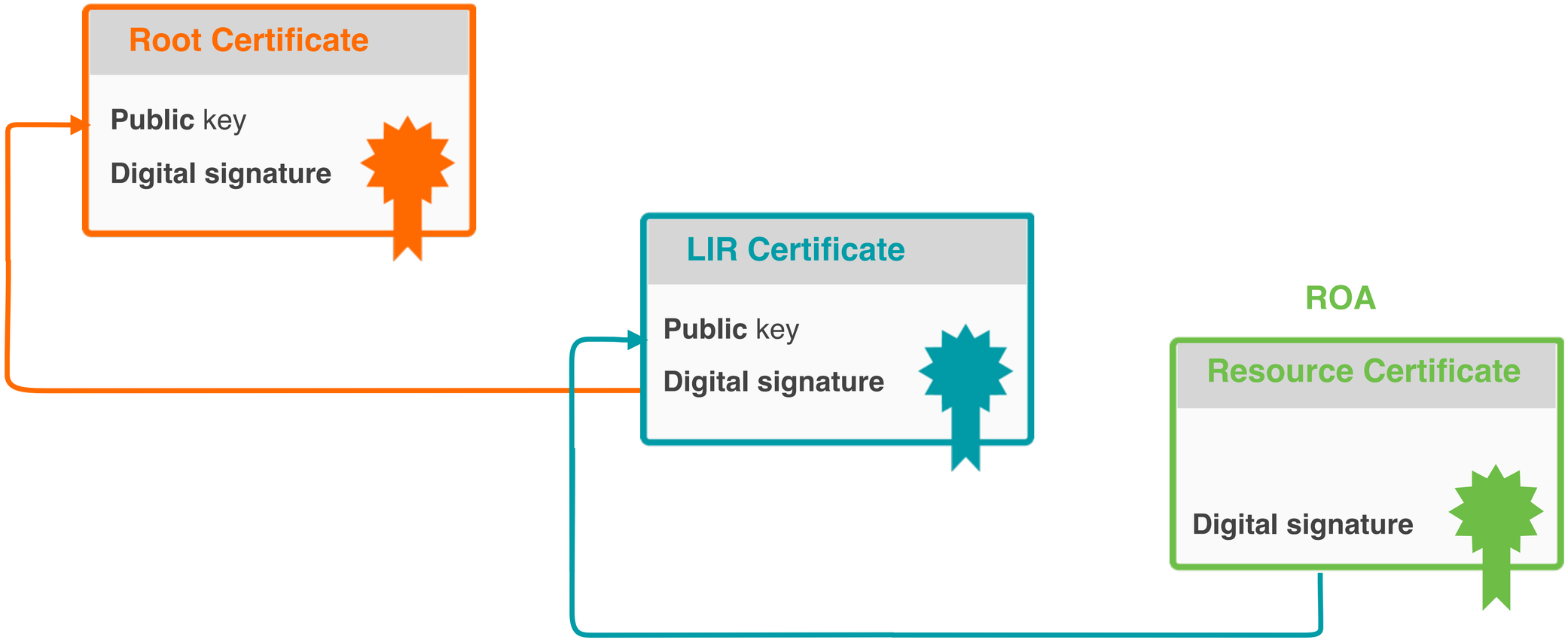
ROA Validation Process

ROA Validation Process

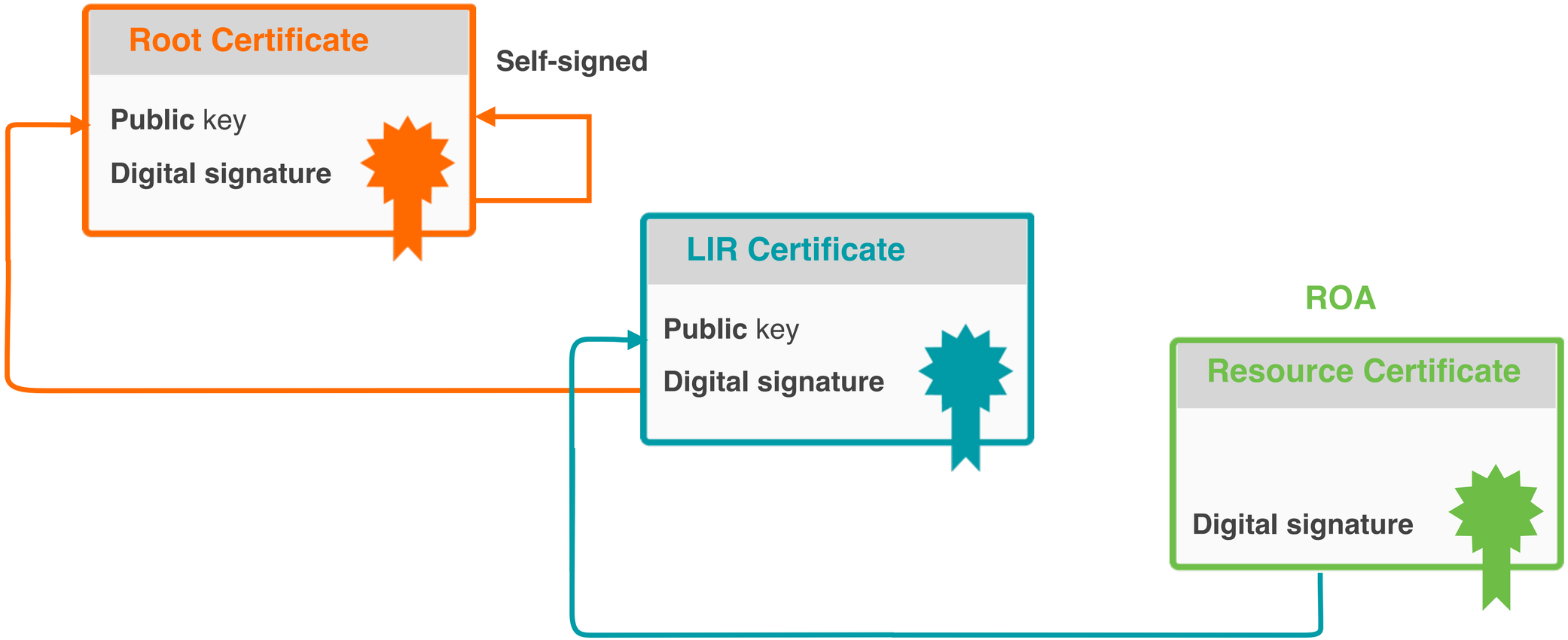
ROA Validation Process



ROA Validation Process

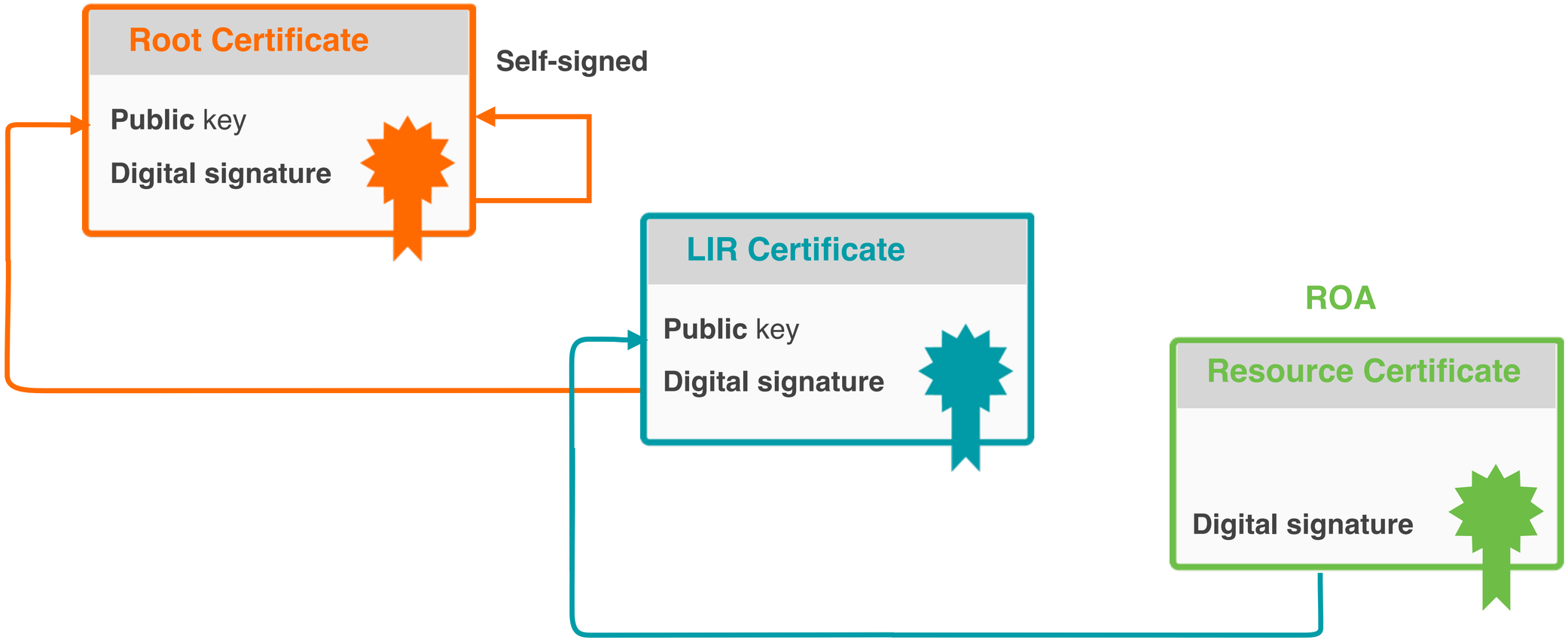


ROA Validation Process

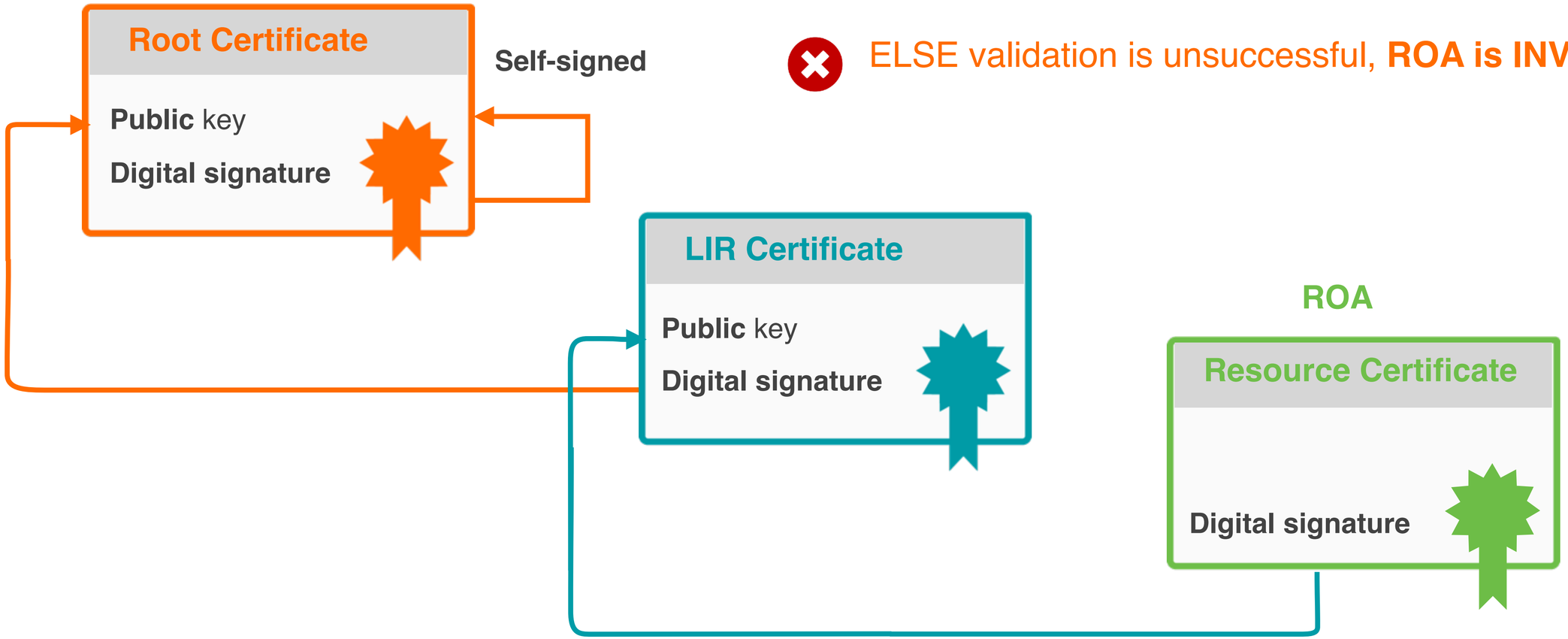


ROA Validation Process

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



ROA Validation Process



Only **valid ROAs** are sent to the router!

RPKI Validator Options

- **Routinator**
  - Built by NLNet Labs
- **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

Questions

Demo!

Running Validators

How to Run Validators

- Run at least two validators
- Configure the correct TALs
  - TALs are freely available with validator software
  - Only the ARIN TAL needs to be installed separately
- In the demo, the following validators will be used:
  - Routinator (0.8.2)
  - FORT (1.4.2)
- Validators are already installed and preconfigured

Start the Routinator

On the server:

```
routinator server --rtr 100.64.1.1:3323
```

The TAL directory is **missing!**

We need to initialise via the **init command!**

```
[root@server1 ~]# routinator server --rtr 100.64.1.1:3323
Missing TAL directory /root/.rpki-cache/tals.
You may have to initialize it via 'routinator init'.
```

```
[root@server1 ~]# routinator init
Before we can install the ARIN TAL, you must have read
and agree to the ARIN Relying Party Agreement (RPA).
It is available at

https://www.arin.net/resources/manage/rpki/rpa.pdf

If you agree to the RPA, please run the command
again with the --accept-arin-rpa option.
```

```
[root@server1 ~]# routinator init --accept-arin-rpa
Created local repository directory /root/.rpki-cache/repository
Installed 5 TALs in /root/.rpki-cache/tals
```

Start the Routinator

On the server:

```
routinator server --rtr 100.64.1.1:3323
```

Check if it’s running:

```
ps aux | grep routinator
```

```
[root@server1 ~]# routinator -v vrps | grep 193.0.24.0/21
rsyncing from rsync://localcert.ripe.net/ta/.
rsync://localcert.ripe.net/ta: successfully completed.
rsync://localcert.ripe.net/ta: The RIPE NCC Certification Repository is
subject to Terms and Conditions
rsync://localcert.ripe.net/ta: See http://www.ripe.net/lir-services/ncc/
legal/certification/repository-tc
*
*
*
*
AS2121,193.0.24.0/21,21,ripe-ncc-pilot
[root@server1 ~]#
```

Start FORT validator

On the server:

```
fort --init-tals -tal=/etc/fort/tal
```

```
[root@server1 ~]# fort --init-tals --tal=/etc/fort/tal
Please download and read ARIN Relying Party Agreement (RPA)
from https://www.arin.net/resources/manage/rpki/rpa.pdf. Once
you've read it and if you agree ARIN RPA, type 'yes' to
proceed with ARIN's TAL download:
yes
Successfully fetched '/etc/fort/tal/arin.tal'!
Successfully fetched '/etc/fort/tal/apnic.tal'!
Successfully fetched '/etc/fort/tal/afrinic.tal'!
Successfully fetched '/etc/fort/tal/ripe.tal'!
Successfully fetched '/etc/fort/tal/lacnic.tal'!
```

Start FORT validator

On the server:

```
systemctl start fort
```

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

```
Systemctl status fort

journalctl –u fort
```

Verify FORT is listening

- 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@server1 ~]# ss -tlnp | grep fort
LISTEN     0      128    100.64.1.1:323                 *:*
users:(("fort",pid=1009,fd=4))
```

```
root@server1 ~]# journalctl -u fort -f
-- Logs begin at Mon 2021-02-08 11:51:24 CET. --
Feb 08 14:34:46 server1 fort[1009]: INF: - Real execution time: 132
secs.
Feb 08 14:35:46 server1 fort[1009]: INF: Starting validation.
Feb 08 14:35:46 server1 fort[1009]: INF: - Current serial number is.
0.
Feb 08 14:37:58 server1 fort[1009]: INF: Checking if there are new or
modified SLURM files
Feb 08 14:37:58 server1 fort[1009]: INF: Applying configured SLURM
Feb 08 14:37:58 server1 fort[1009]: INF: Validation finished:
Feb 08 14:37:58 server1 fort[1009]: INF: - Valid Prefixes: 4740
Feb 08 14:37:58 server1 fort[1009]: INF: - Valid Router Keys: 0
Feb 08 14:37:58 server1 fort[1009]: INF: - Current serial number is 0.
Feb 08 14:37:58 server1 fort[1009]: INF: - Real execution time:132 secs.
```

```
[root@server1 ~]#  cat  /var/lib/fort/roas.csv | grep 193.0.24.0/21
AS2121,193.0.24.0/21,21
```

Questions

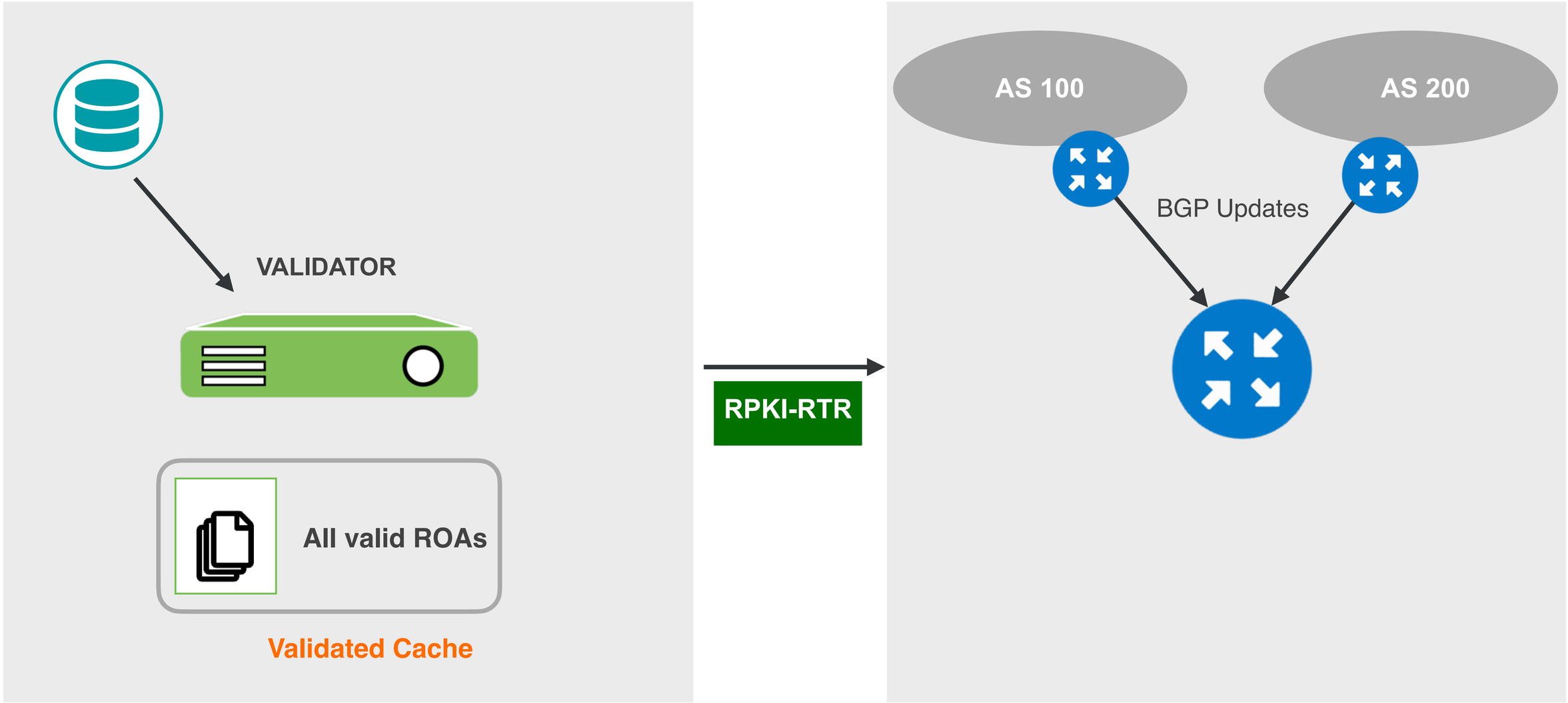
RPKI Validation

Validating BGP Announcements

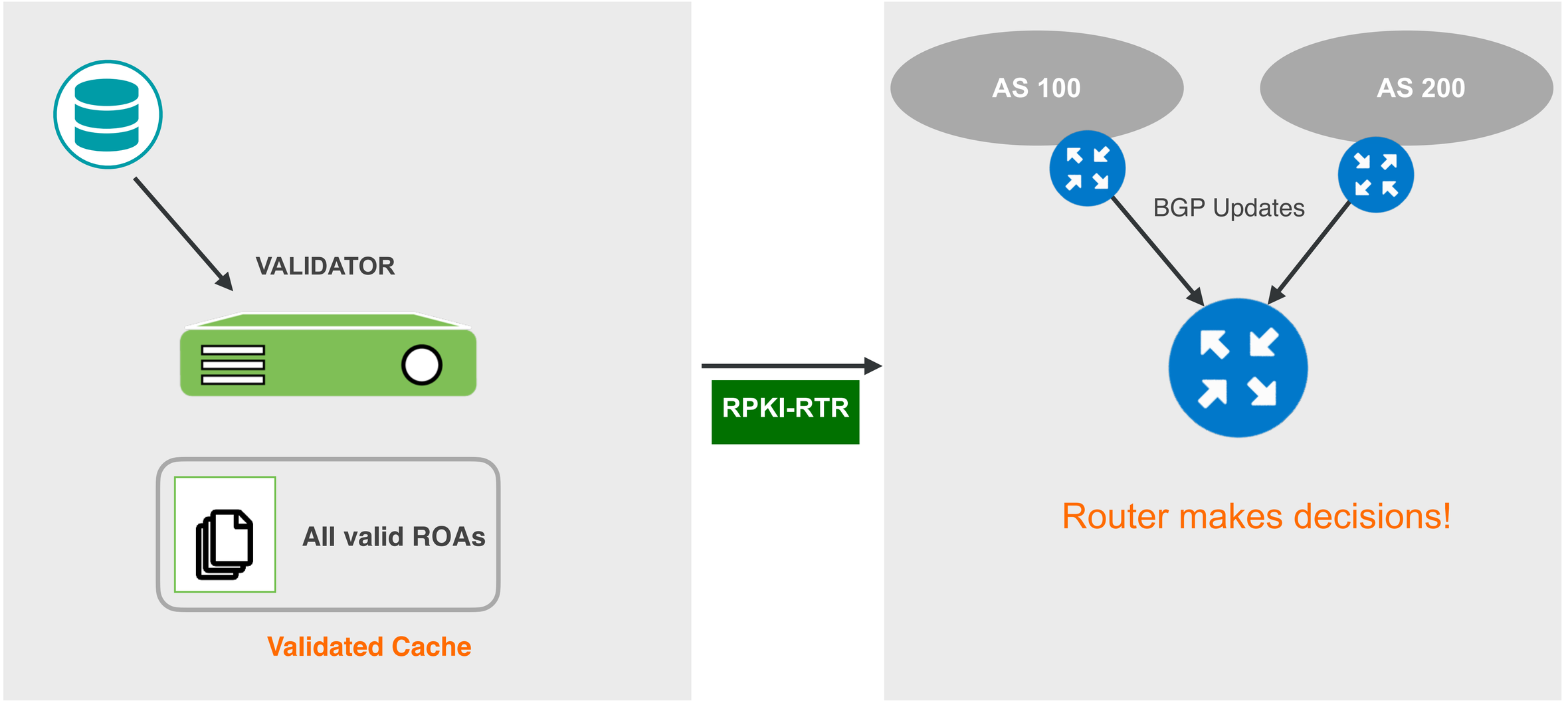
BGP Origin Validation (BGP OV)

- RFC#6811
- BGP filtering with ROAs
- Validating BGP announcements by using RPKI infrastructure

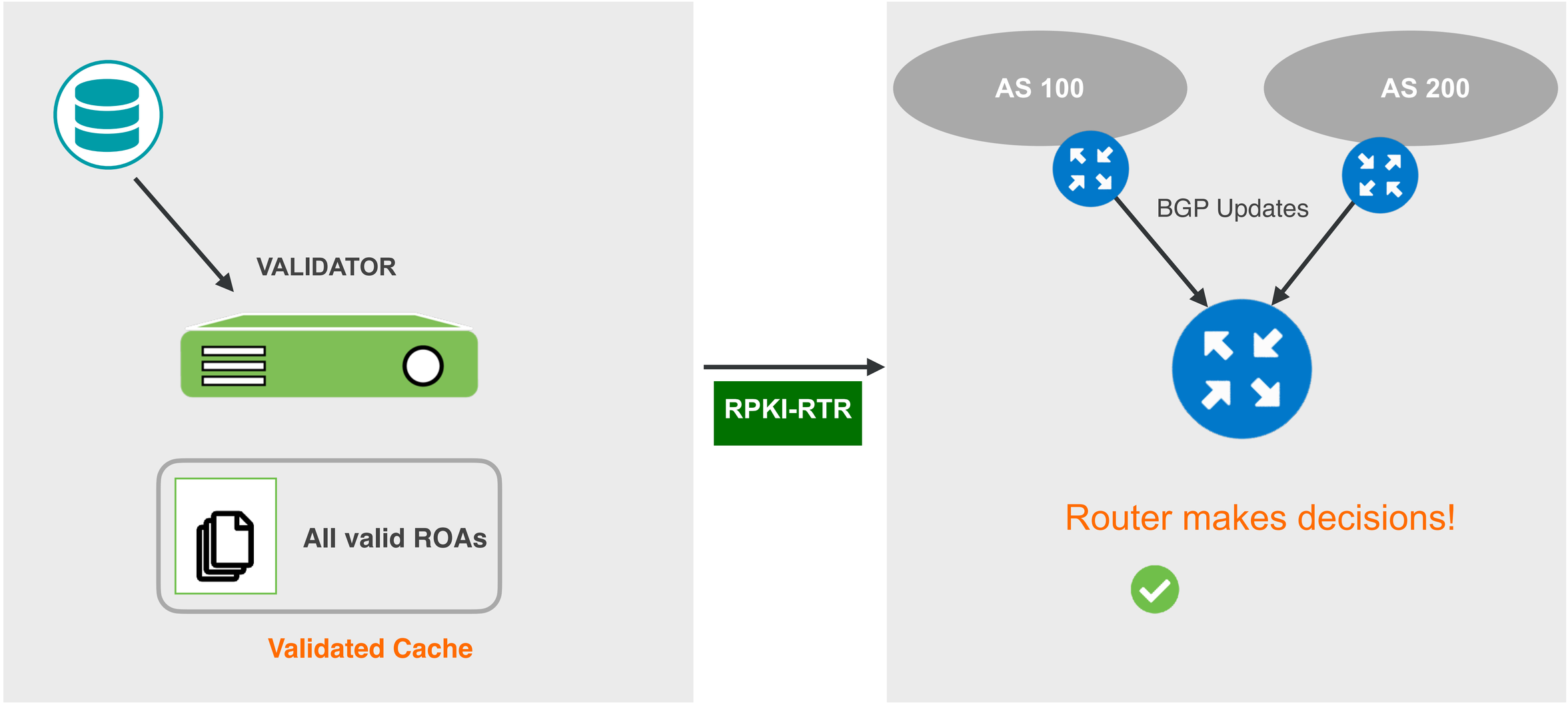
BGP Origin Validation



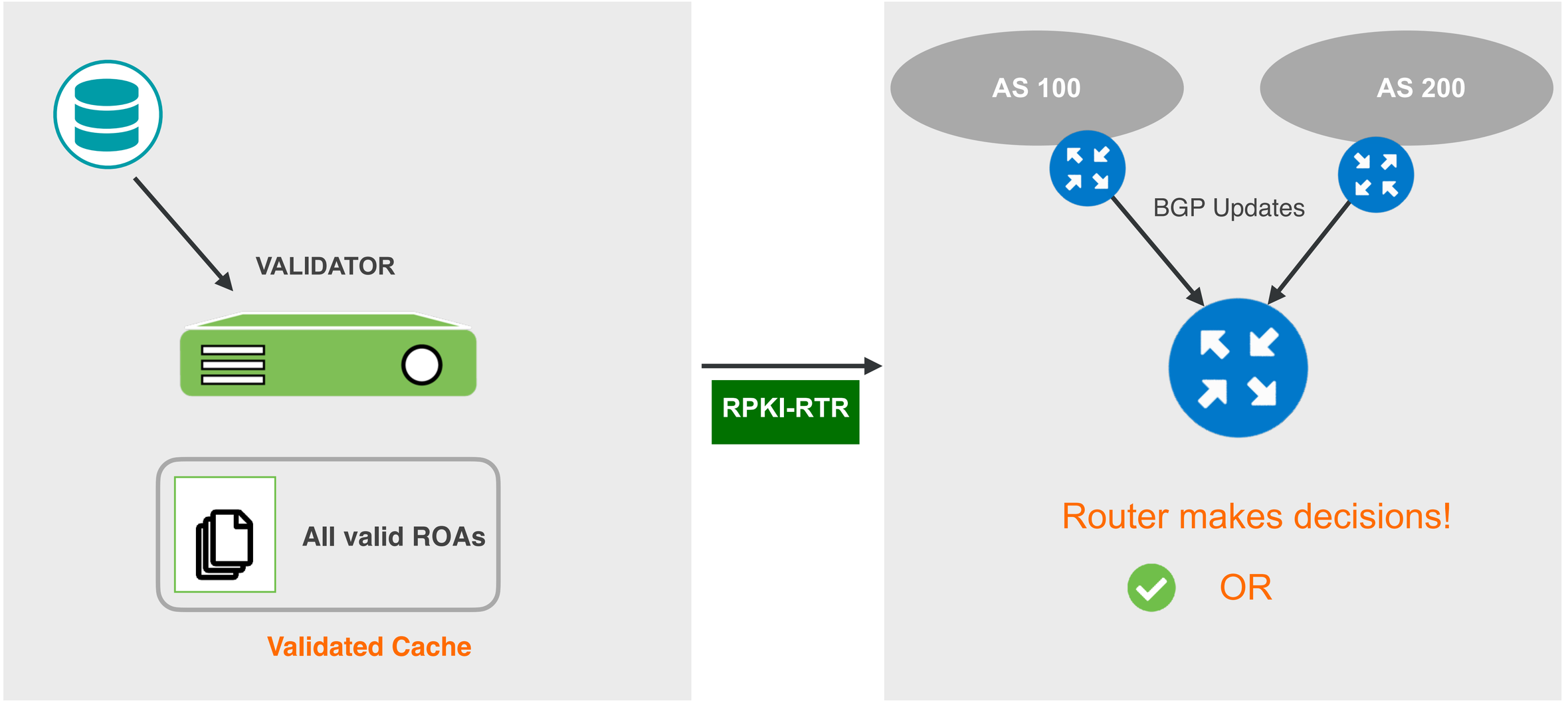
BGP Origin Validation



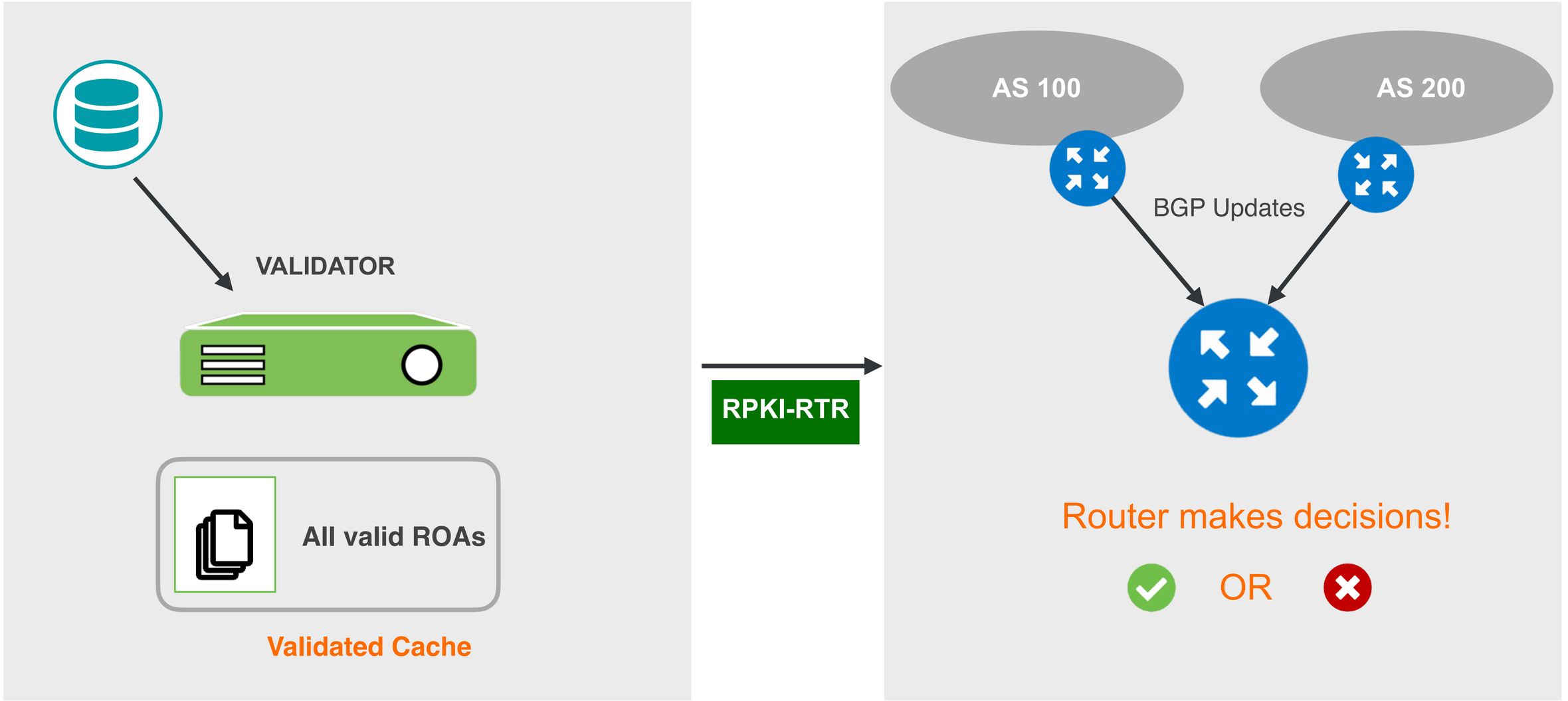
BGP Origin Validation



BGP Origin Validation

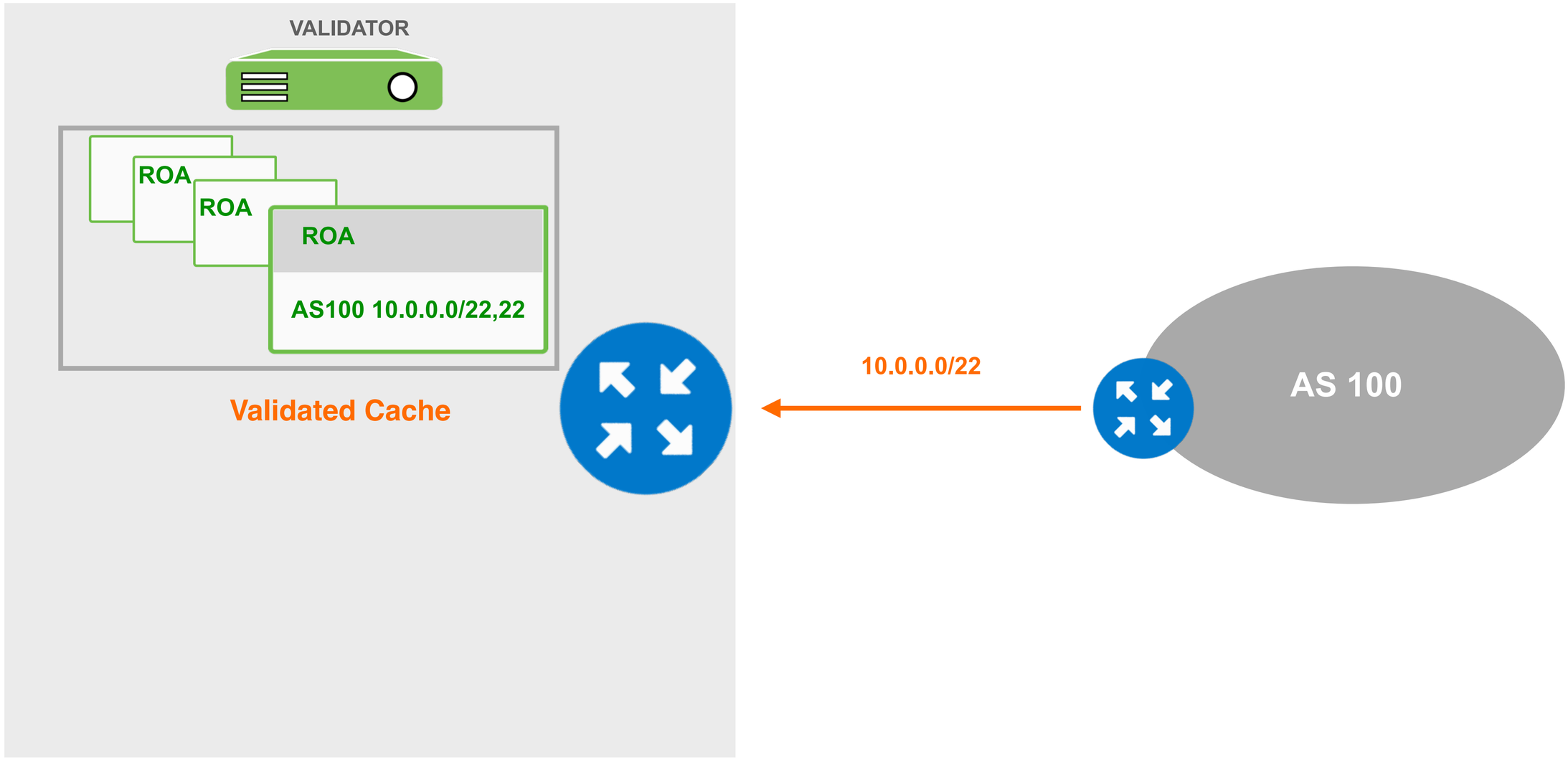


BGP Origin Validation

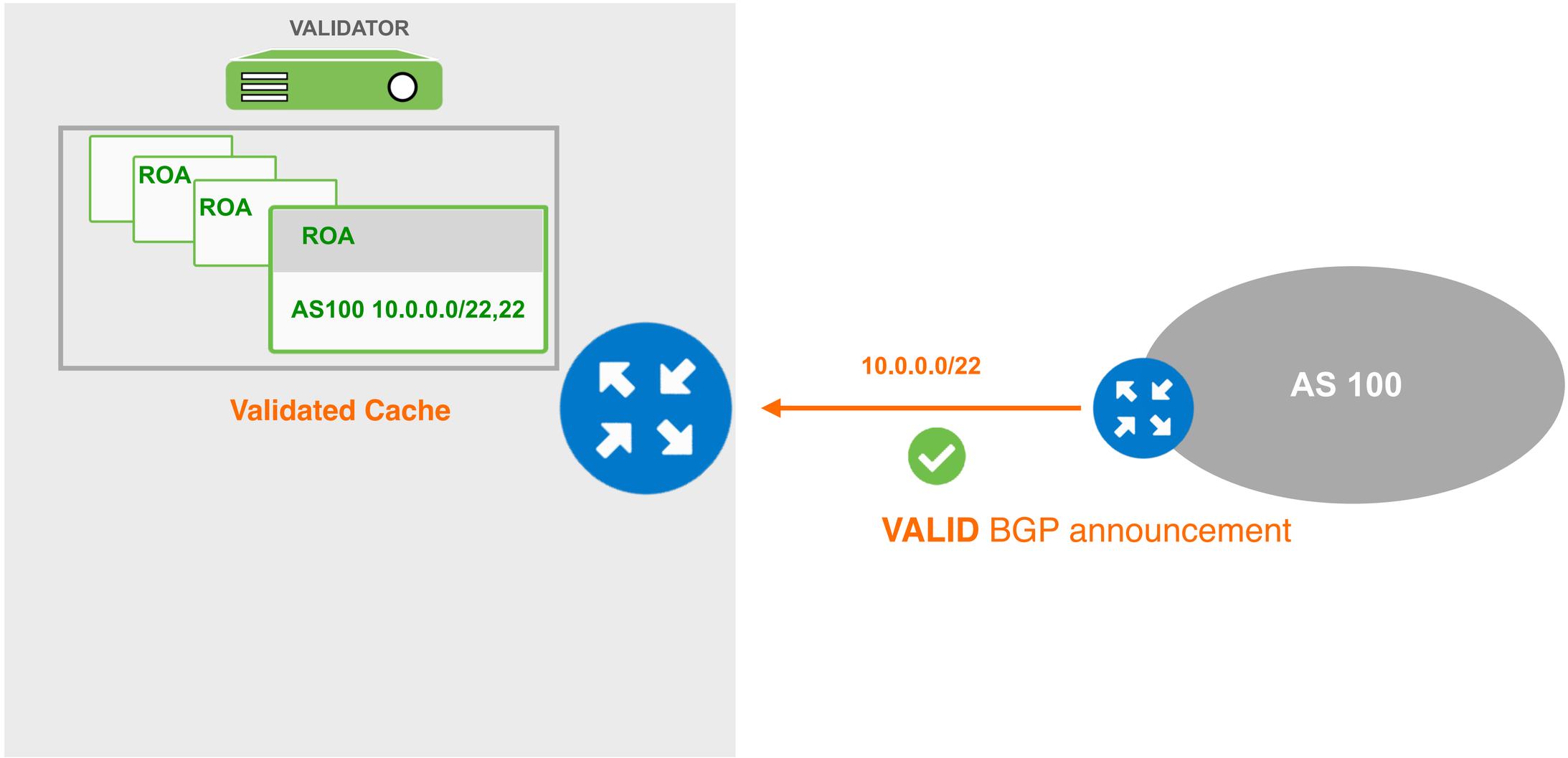


Let’s explain it with examples…

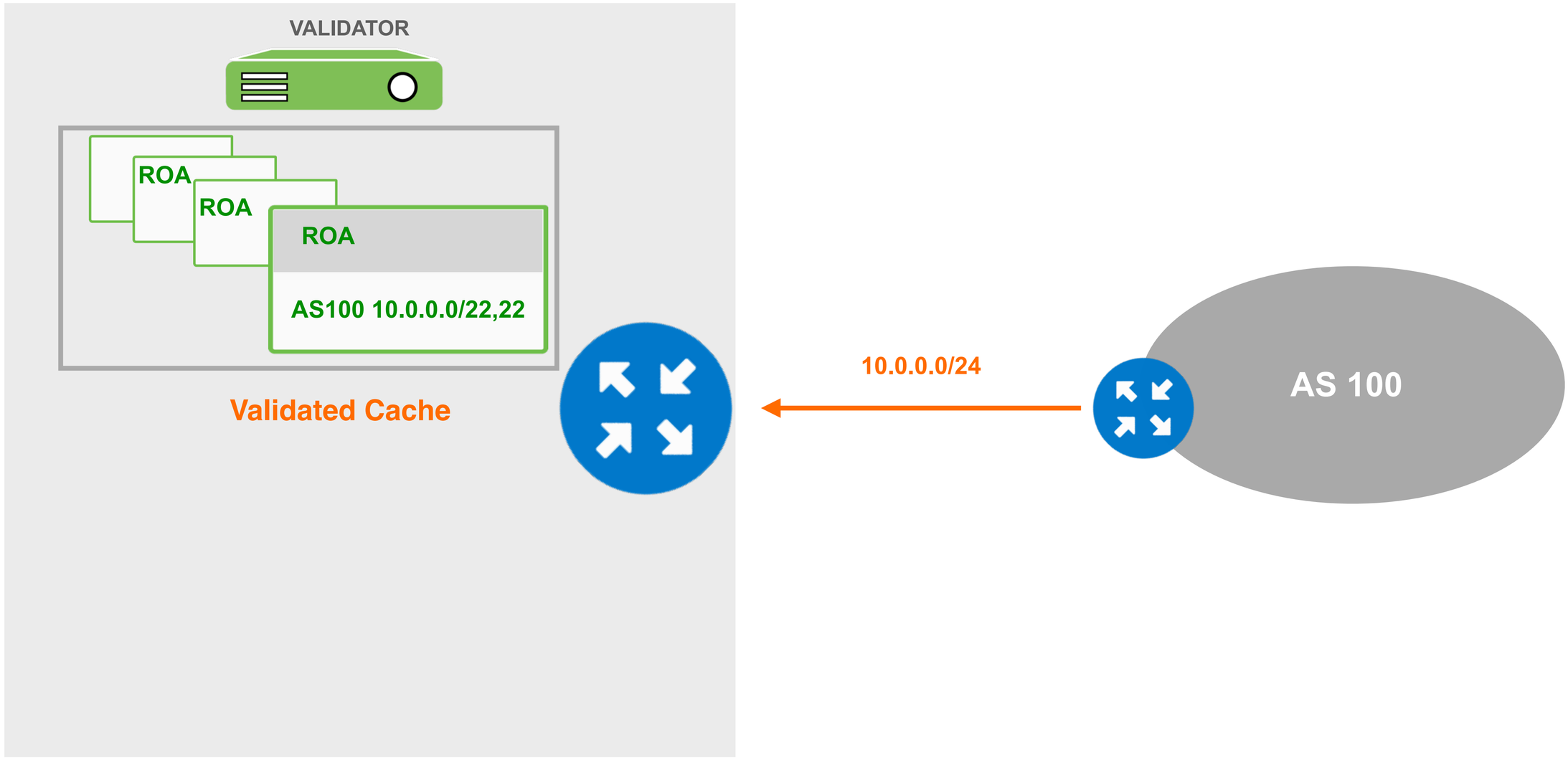
BGP Valid


VALIDATOR
ROA
ROA
ROA
AS100 10.0.0.0/22,22
Validated Cache
10.0.0.0/22
AS 100

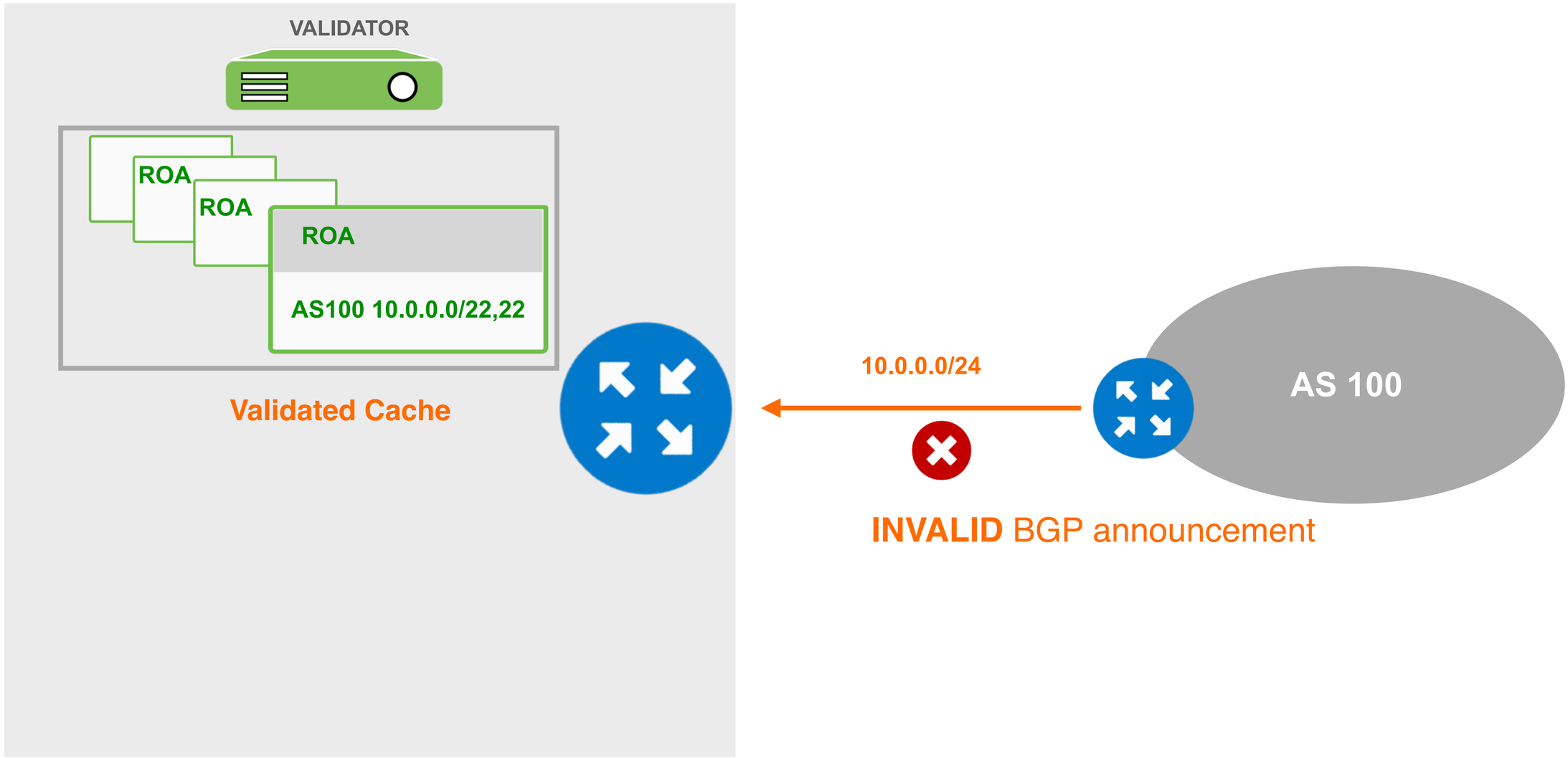
BGP Valid


VALIDATOR
ROA
ROA
ROA
AS100 10.0.0.0/22,22
Validated Cache
10.0.0.0/22
AS 100
VALID BGP announcement

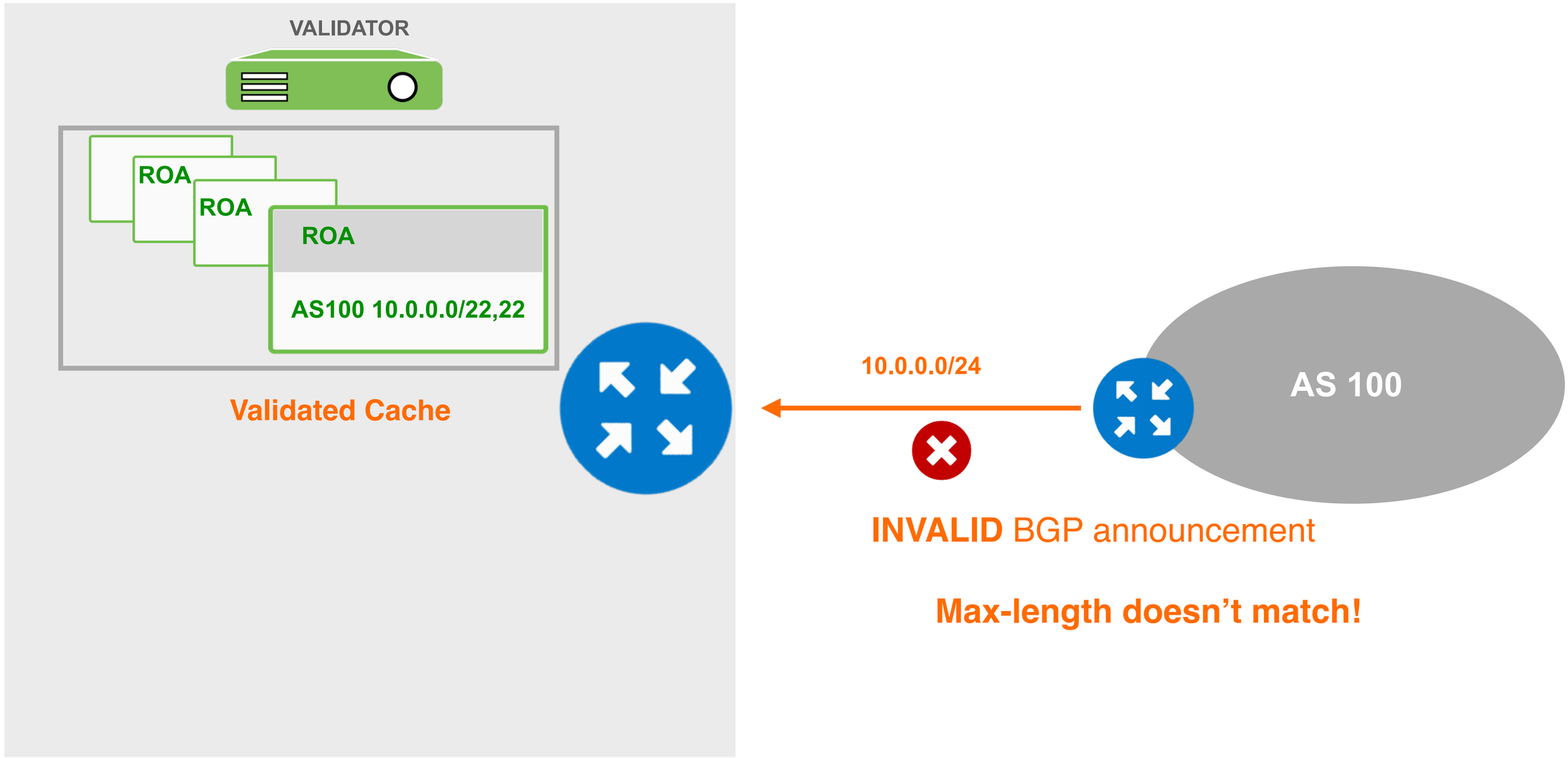
BGP Invalid


VALIDATOR
ROA
ROA
ROA
AS100 10.0.0.0/22,22
Validated Cache
10.0.0.0/24
AS 100

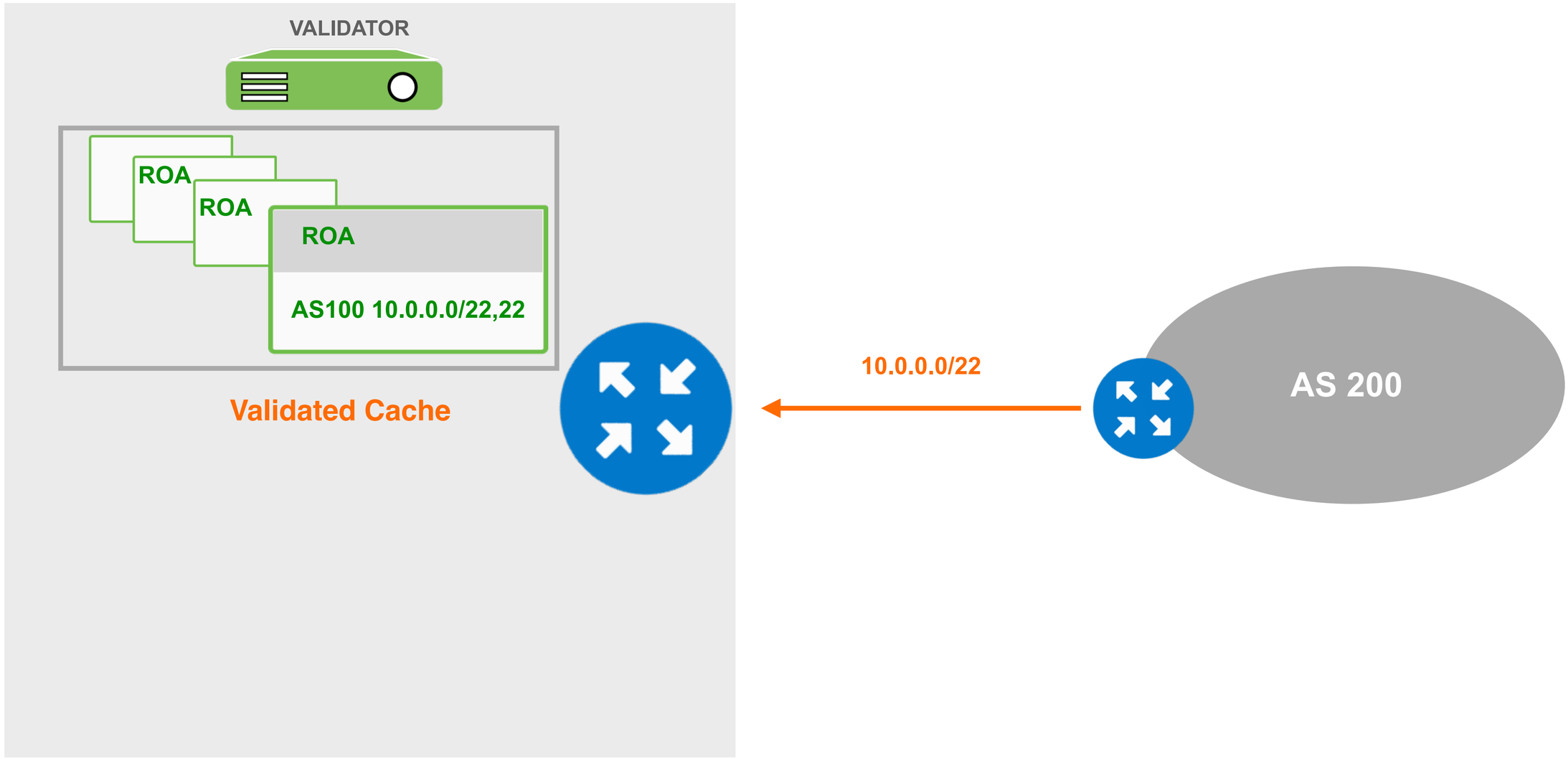
BGP Invalid


VALIDATOR
ROA
ROA
ROA
AS100 10.0.0.0/22,22
Validated Cache
10.0.0.0/24
AS 100
INVALID BGP announcement

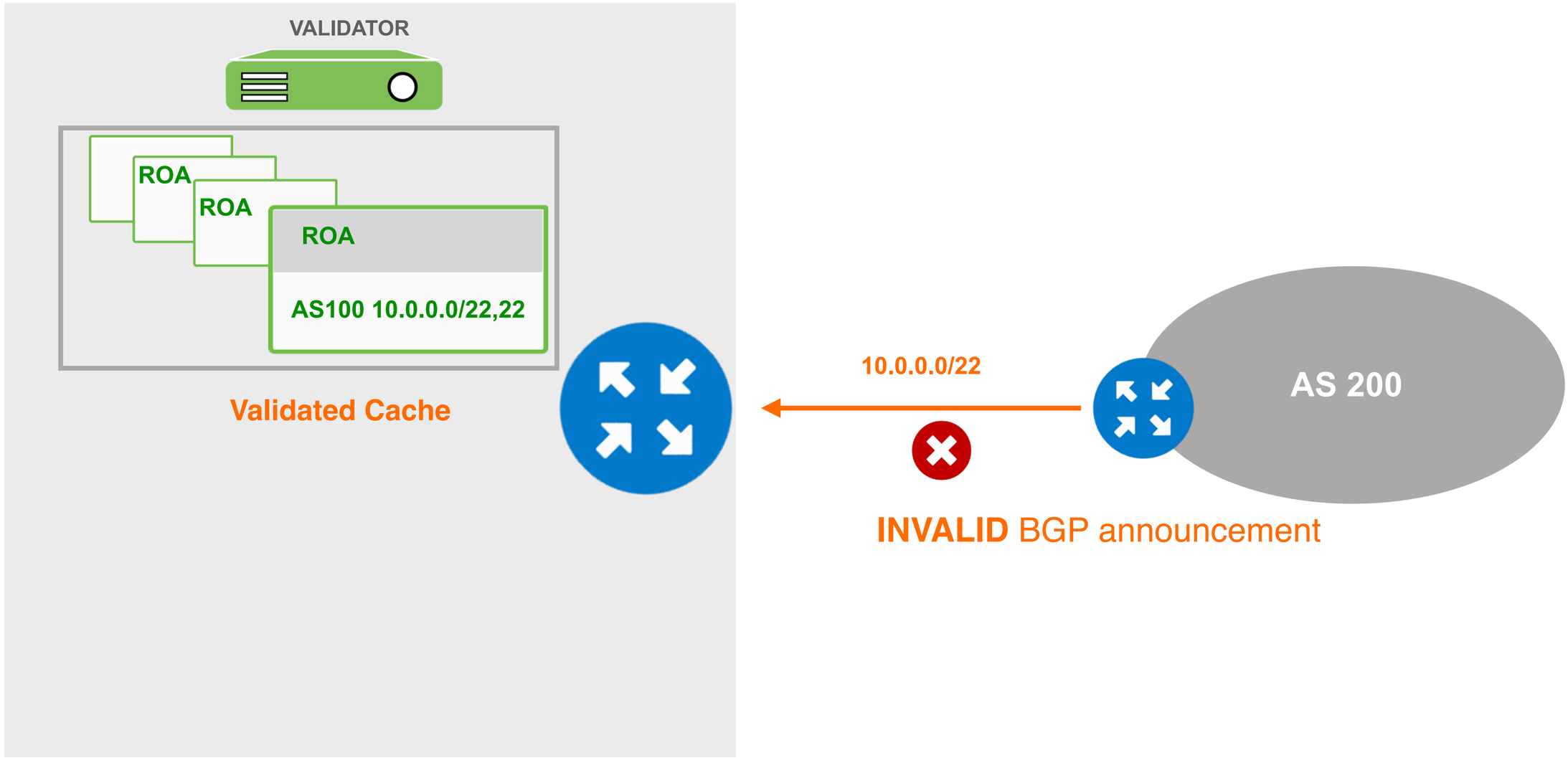
BGP Invalid


VALIDATOR
ROA
ROA
ROA
AS100 10.0.0.0/22,22
Validated Cache
10.0.0.0/24
AS 100
INVALID BGP announcement
Max-length doesn't match!

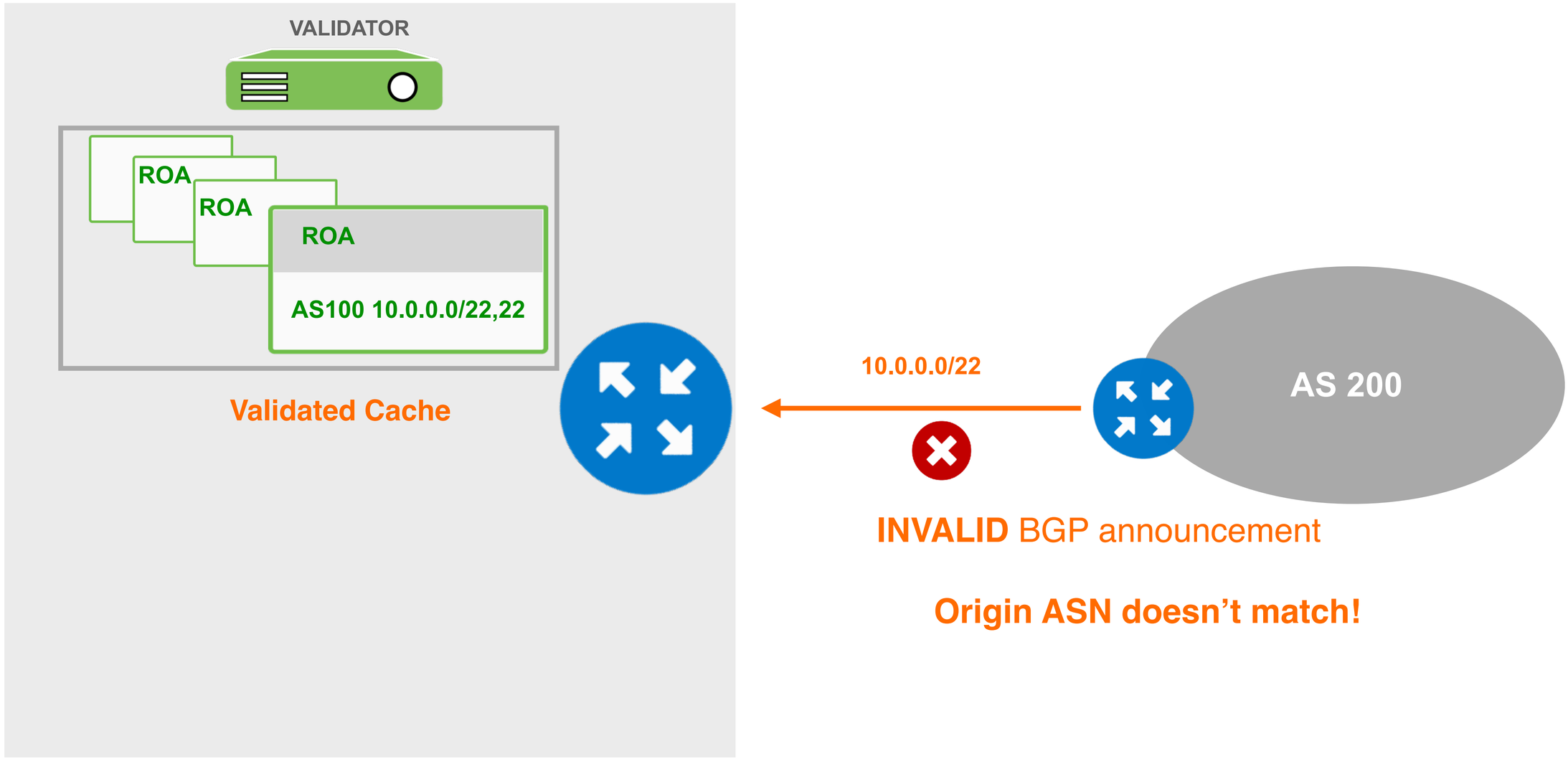
BGP Invalid


VALIDATOR
ROA
ROA
ROA
AS100 10.0.0.0/22,22
Validated Cache
10.0.0.0/22
AS 200

BGP Invalid


VALIDATOR
ROA
ROA
ROA
AS100 10.0.0.0/22,22
Validated Cache
10.0.0.0/22
AS 200
INVALID BGP announcement

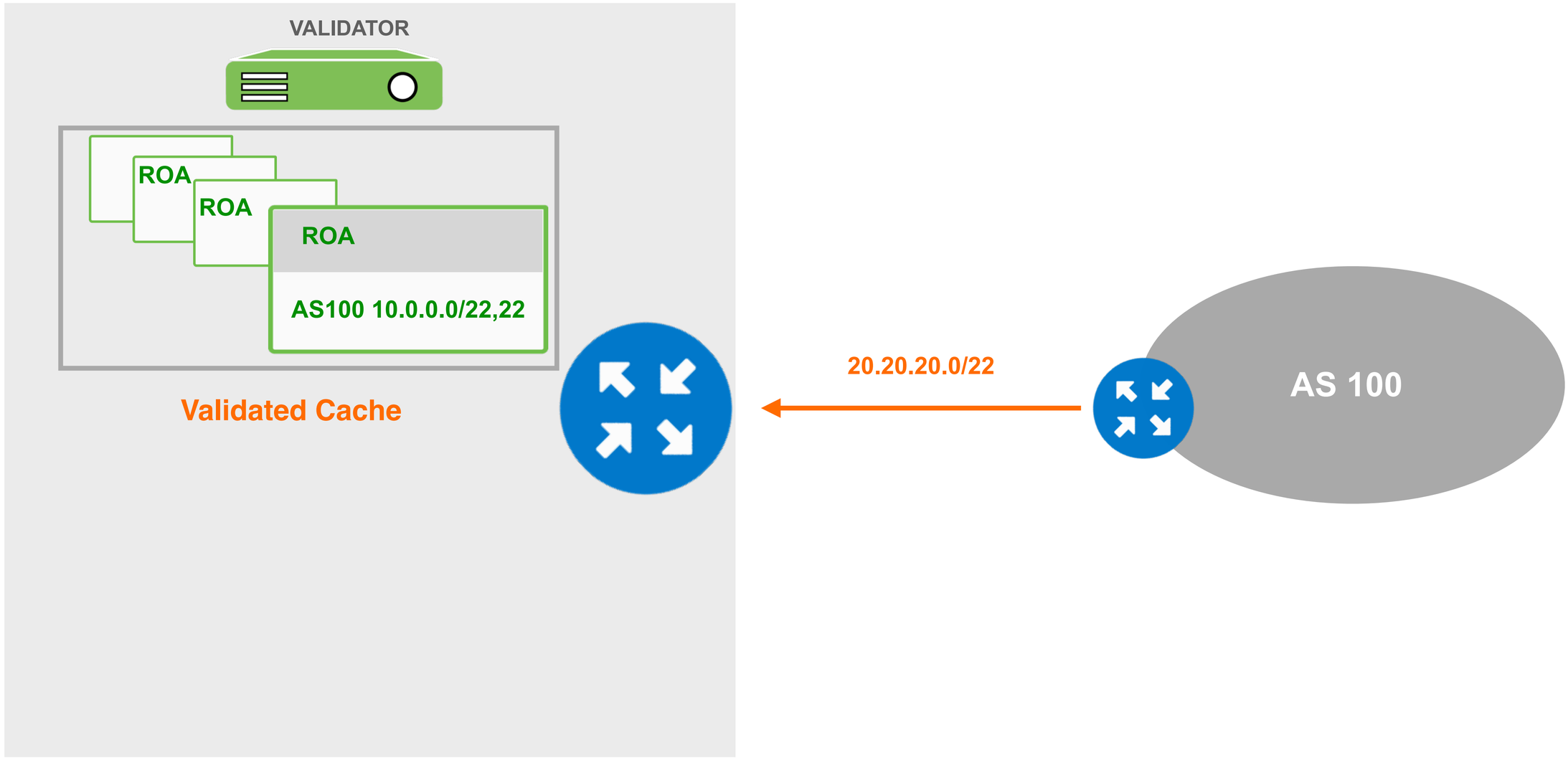
BGP Invalid


VALIDATOR
ROA
ROA
ROA
AS100 10.0.0.0/22,22
Validated Cache
10.0.0.0/22
AS 200
INVALID BGP announcement
Origin ASN doesn't match!

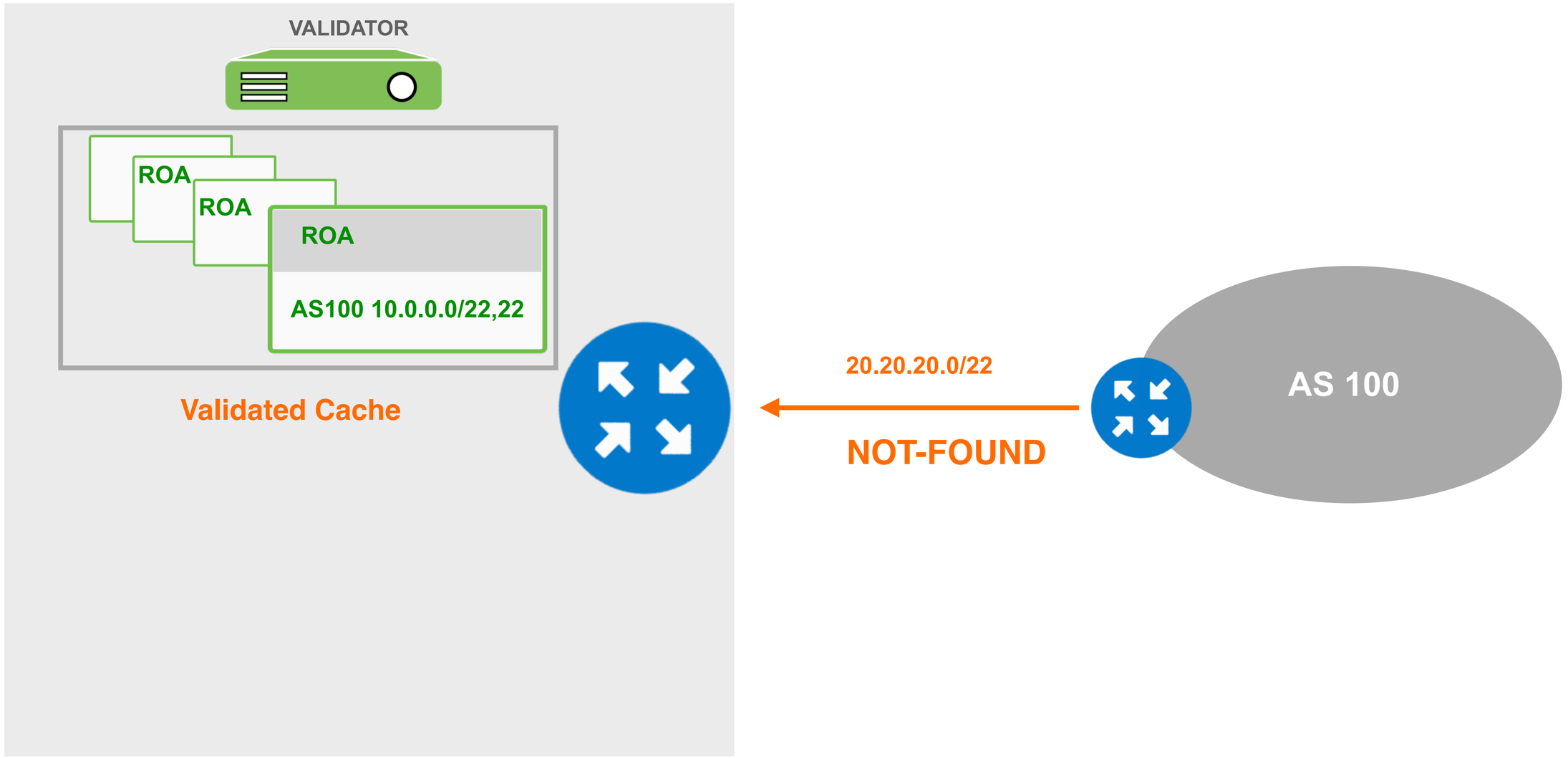
So, RPKI does two checks to validate BGP announcements:

Max-length and **Origin ASN**

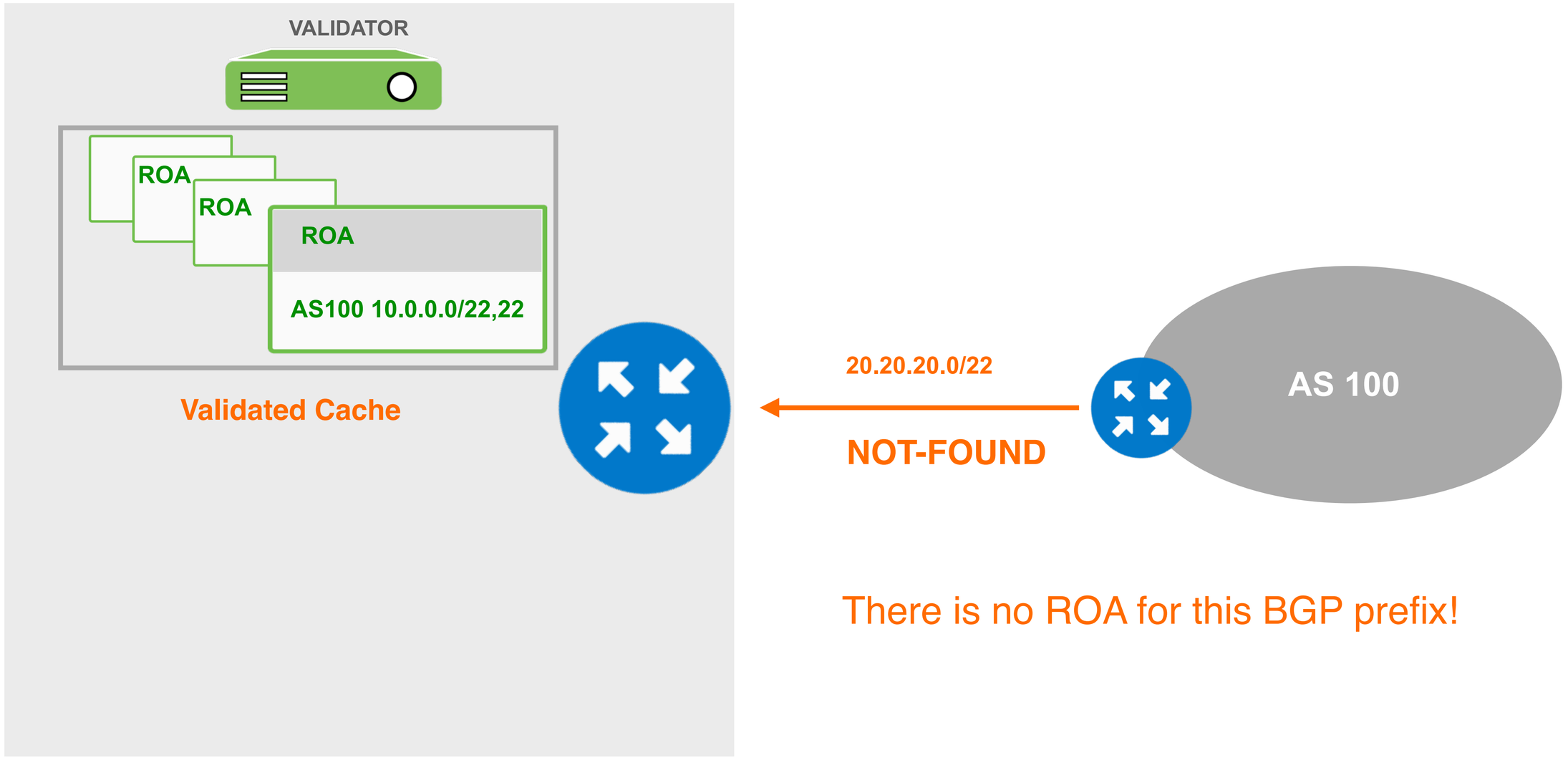
BGP Not-Found



BGP Not-Found

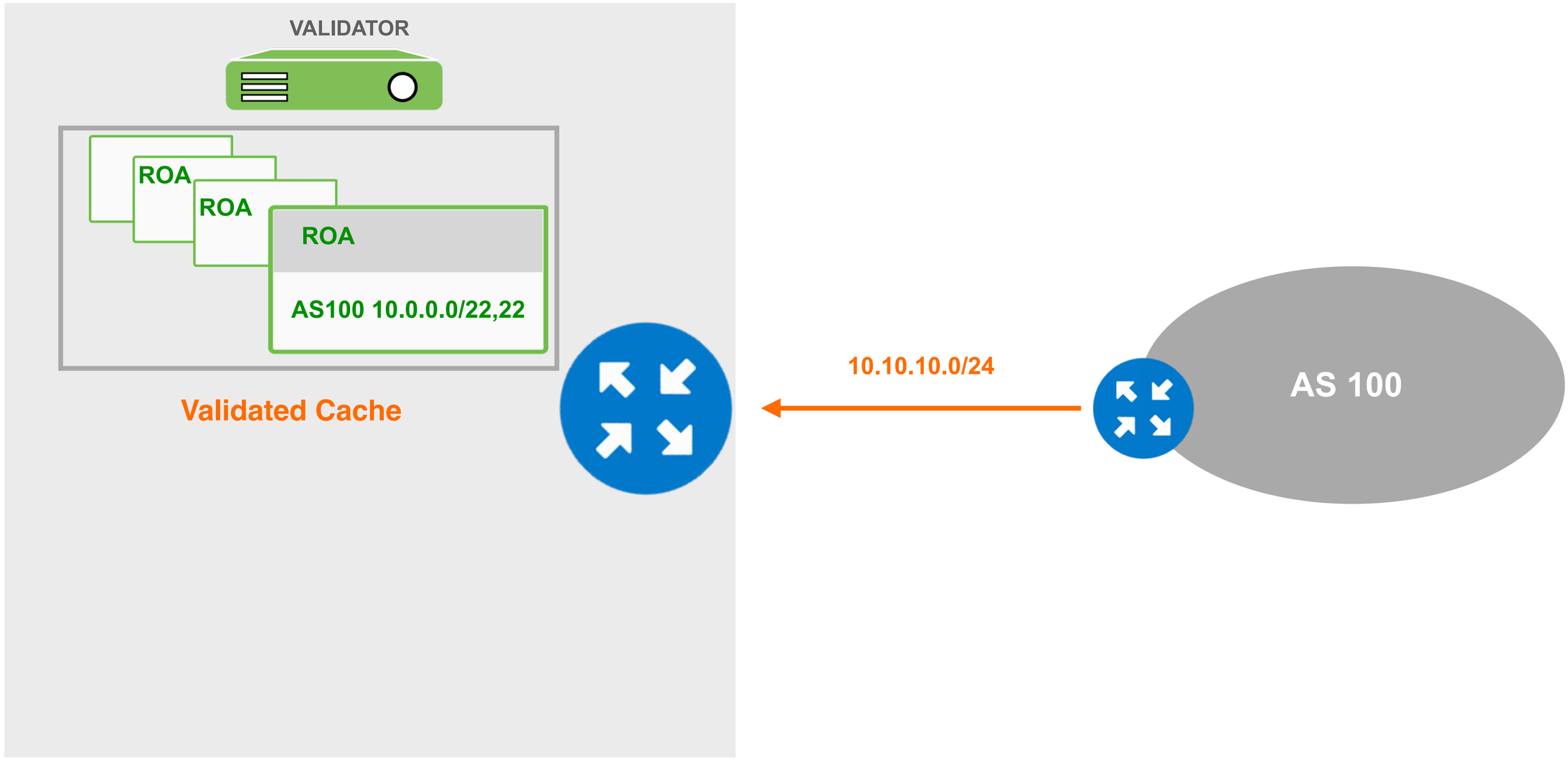


BGP Not-Found

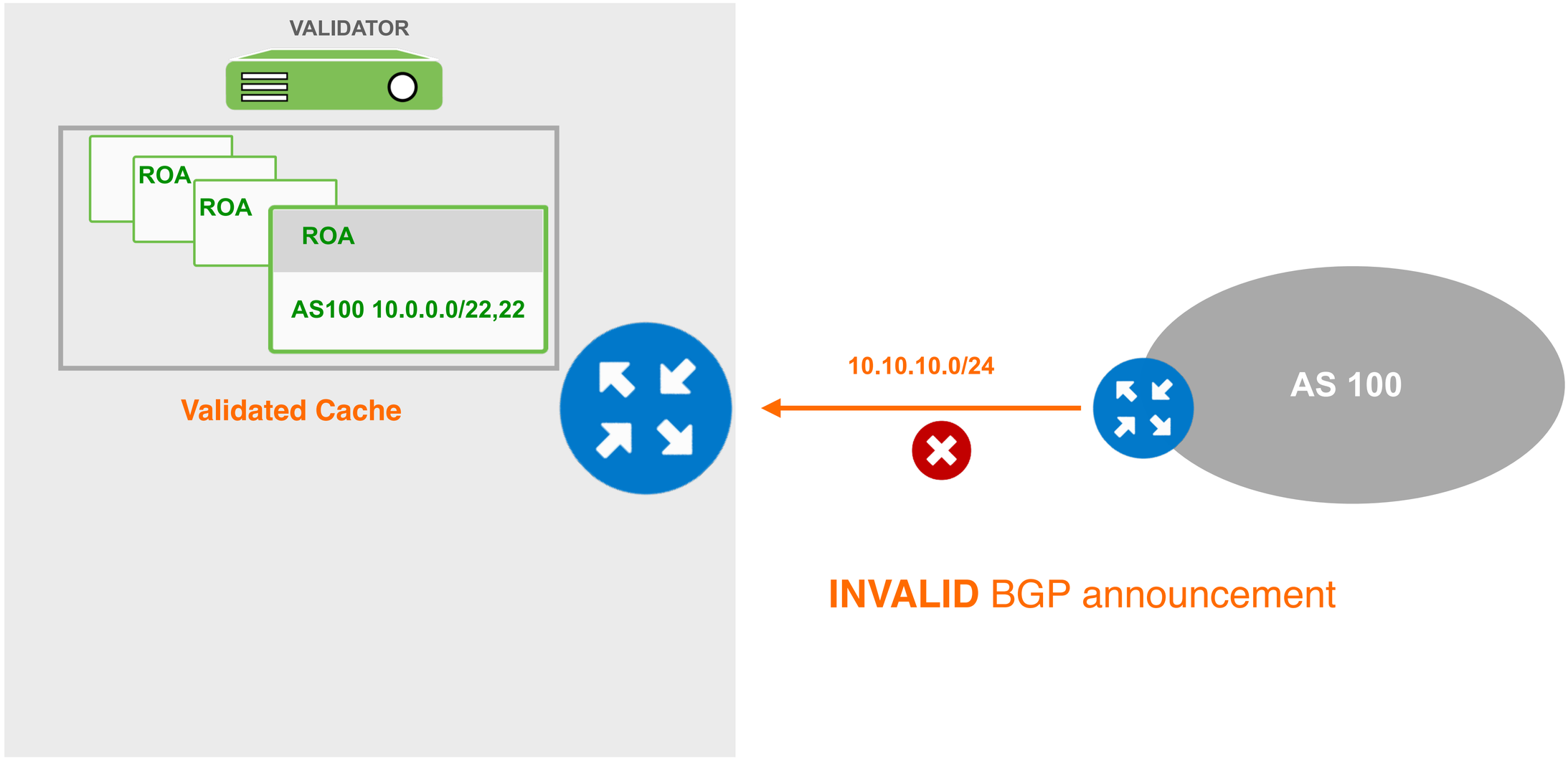


There is no ROA for this BGP prefix!

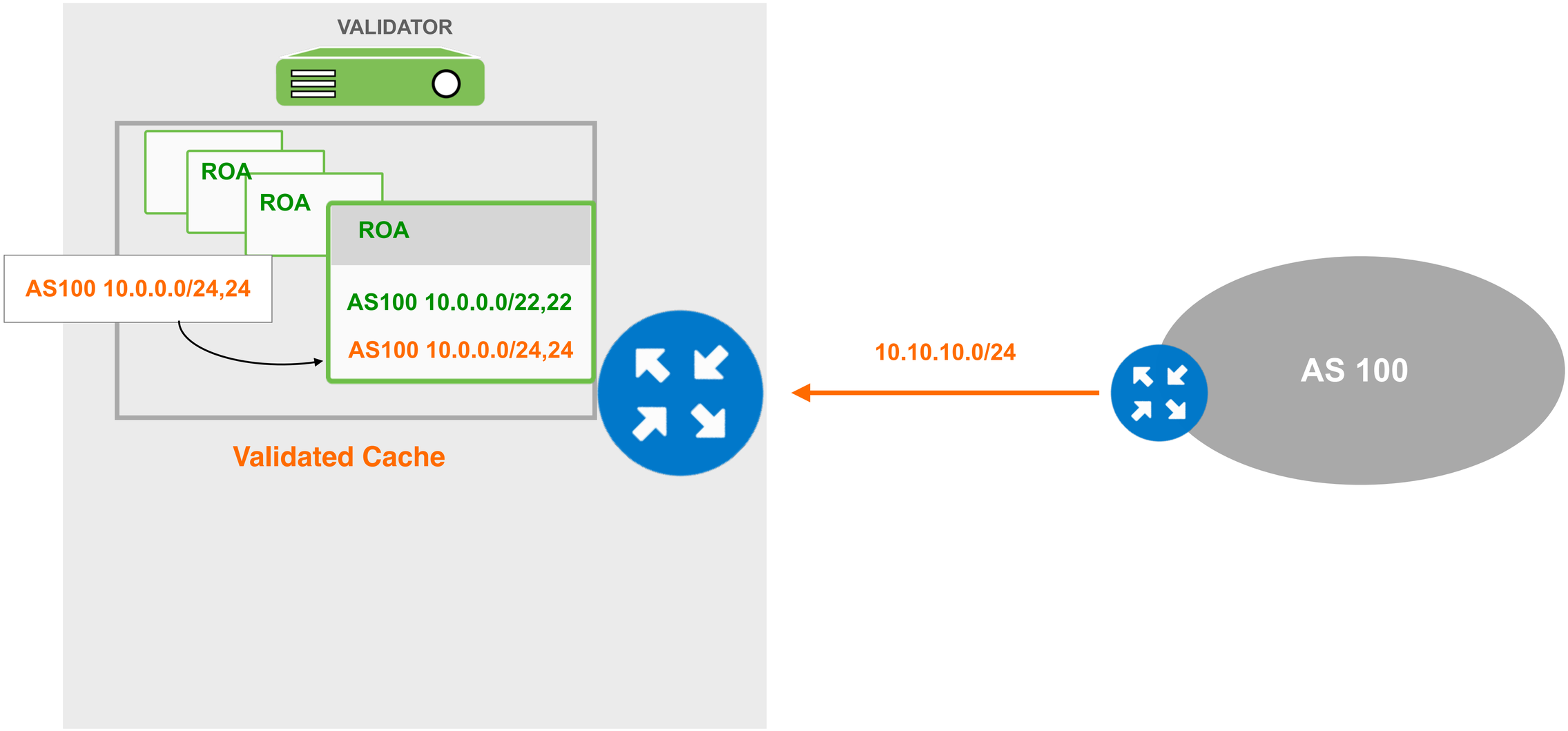
Whitelisting



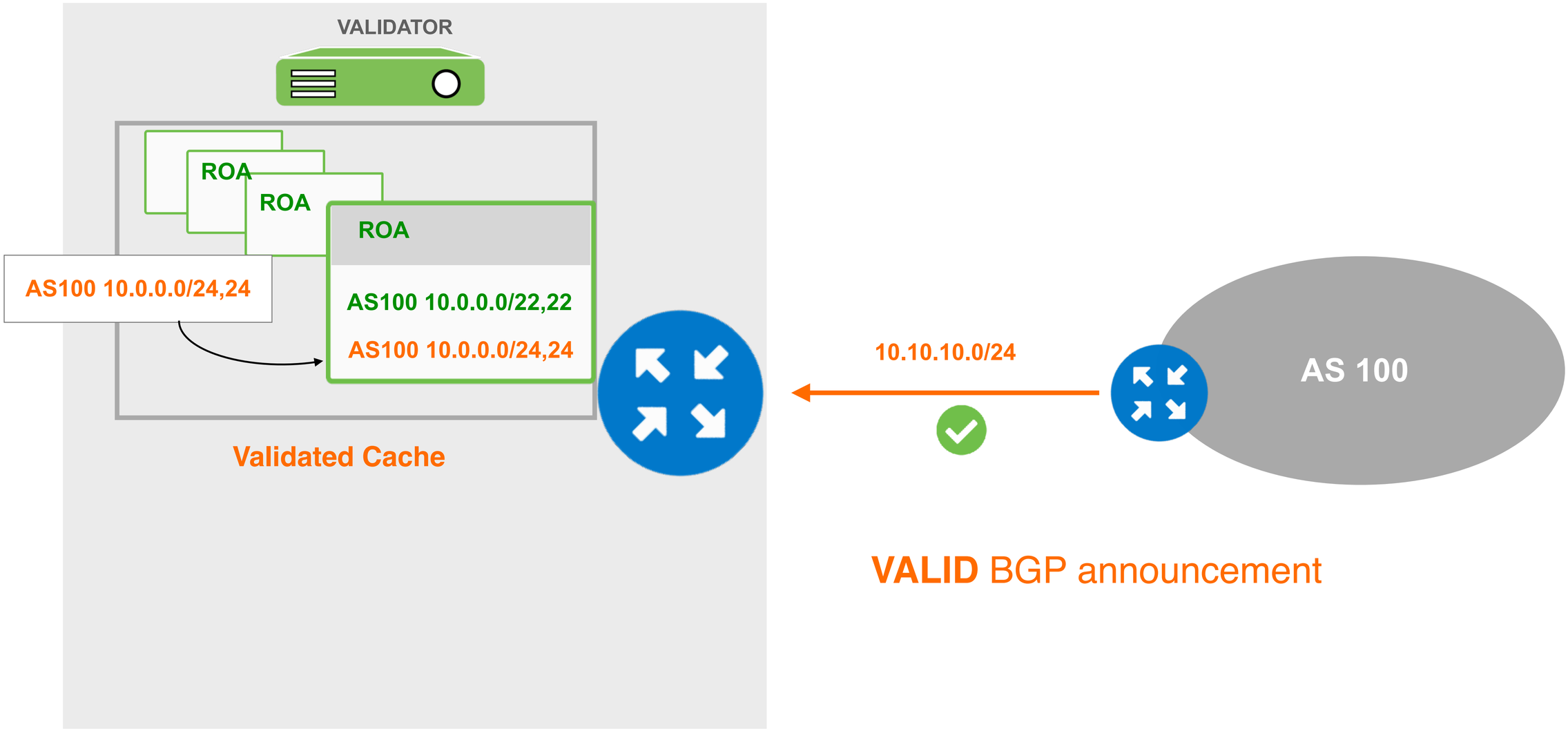
Whitelisting



Whitelisting



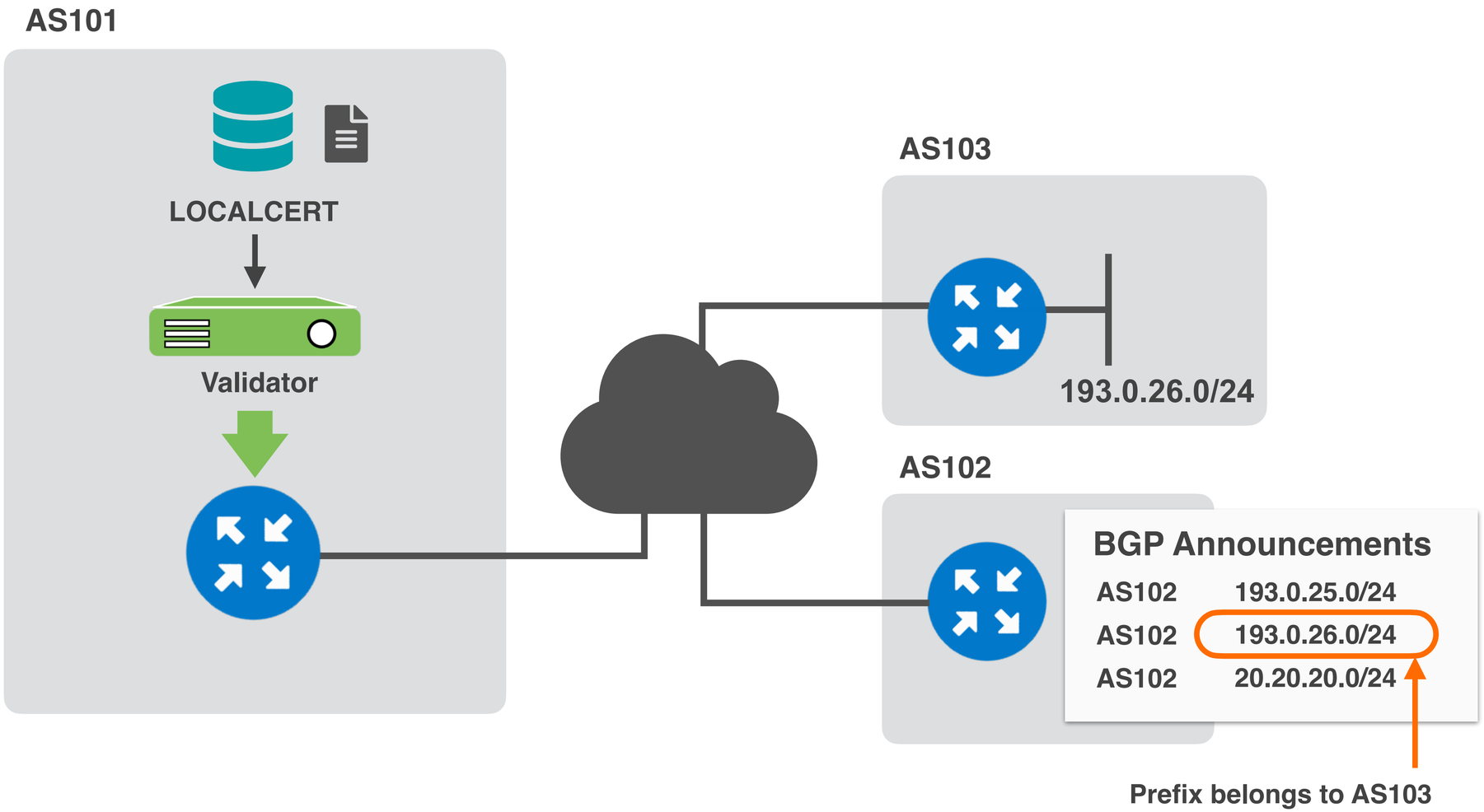
Whitelisting



Demo!

Setting up BGP Origin Validation

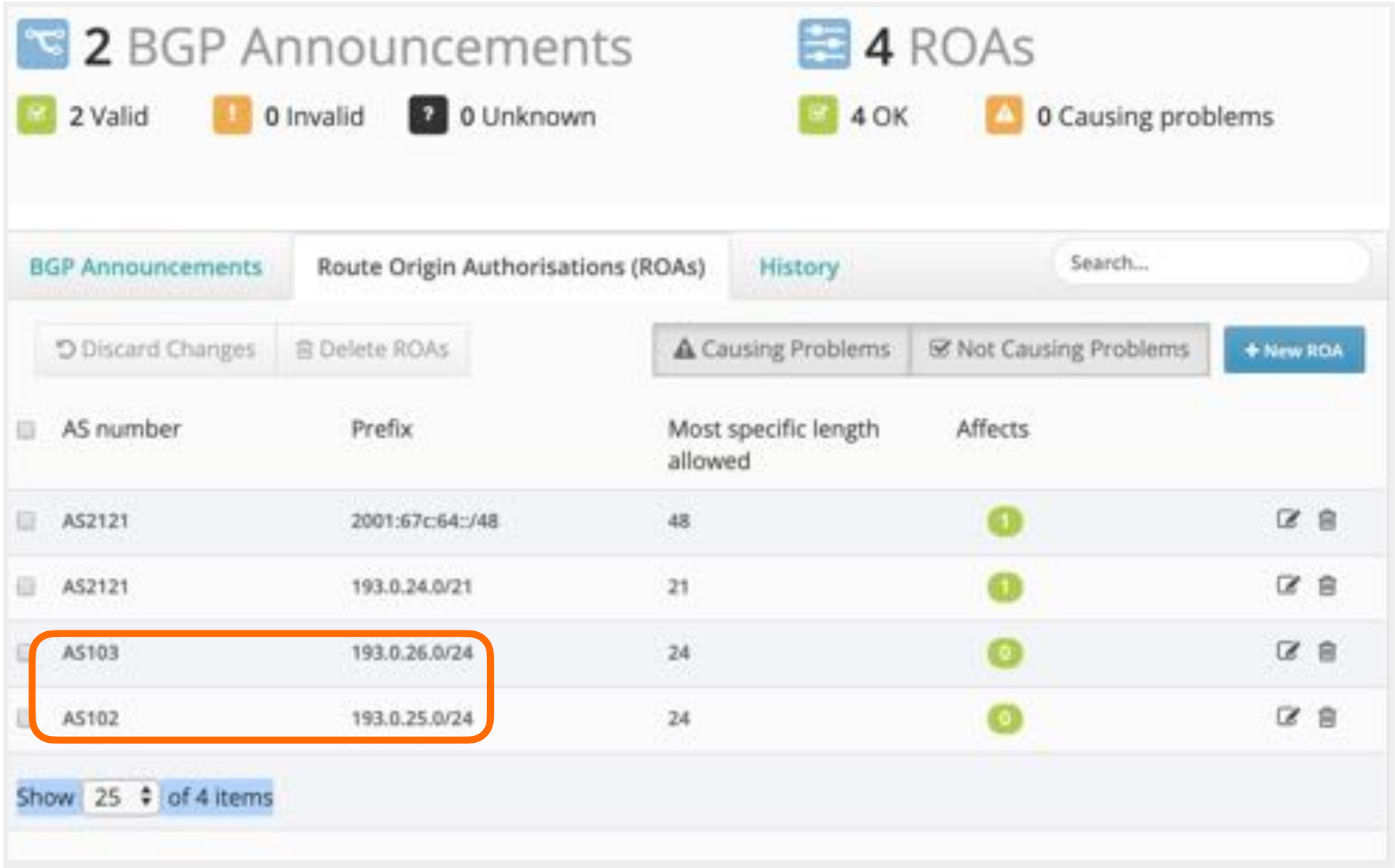
Demo Setup


AS101
LOCALCERT
Validator
AS103
193.0.26.0/24
AS102
BGP Announcements
AS102 193.0.25.0/24
AS102 193.0.26.0/24
AS102 20.20.20.0/24
Prefix belongs to AS103

Set up Origin Validation in AS101

- We are using the 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 the First Demo



Configure Validator Connection

On AS101 router:

```
(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
```

FORT

Routinator

And check it:

```
# 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

Let’s Check How We’re Doing…

```
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
```

```
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!
- Check origin validation 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

RPKI Validation

Discarding BGP Invalids

What to do with INVALIDs?

- For BGP origin validation to achieve its goal:
  - Invalids should be dropped!
- As a first step:
  - You can set lower local preference (not a long term solution)
  - Tag the invalids with a BGP community
- After analysing the effect, you can start dropping INVALIDs

Demo!

Discarding BGP Invalids

Configure Route Maps

Configure route-map on the router of **AS101** and apply to neighbour

```
(config-router)# route-map rpki-accept permit 10
(route-map)# match rpki valid
(route-map)# set local-preference 110
(route-map)# route-map rpki-accept permit 20
(route-map)# match rpki not-found
(route-map)# set local-preference 80
```

```
(config)# router bgp 101
(config)# address-family ipv4
(config)# neighbor 192.168.1.254 route-map rpki-accept in
```

Check Your Work

Clear your BGP session and check BGP table

```
# clear bgp ipv4 unicast 192.168.1.254
# show ip bgp XXX
```

RPKI Valid

```
U1_Router#show  ip bgp 193.0.25.0/24
BGP routing table entry for 193.0.25.0/24, version 2205270
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 3
  99 102
    192.168.1.2 from 192.168.1.254 (99.0.0.1)
      Origin IGP, metric 0, localpref 110, valid, external, best
      path 7FD962379360 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
% Network not in table
```

Network is not in BGP table!

RPKI Invalid

Prefix belongs to AS103!

```
U1_Router#show  ip bgp 193.0.26.0/24
% Network not in table
```

Network is not in BGP table!

Because RPKI status is Invalid!

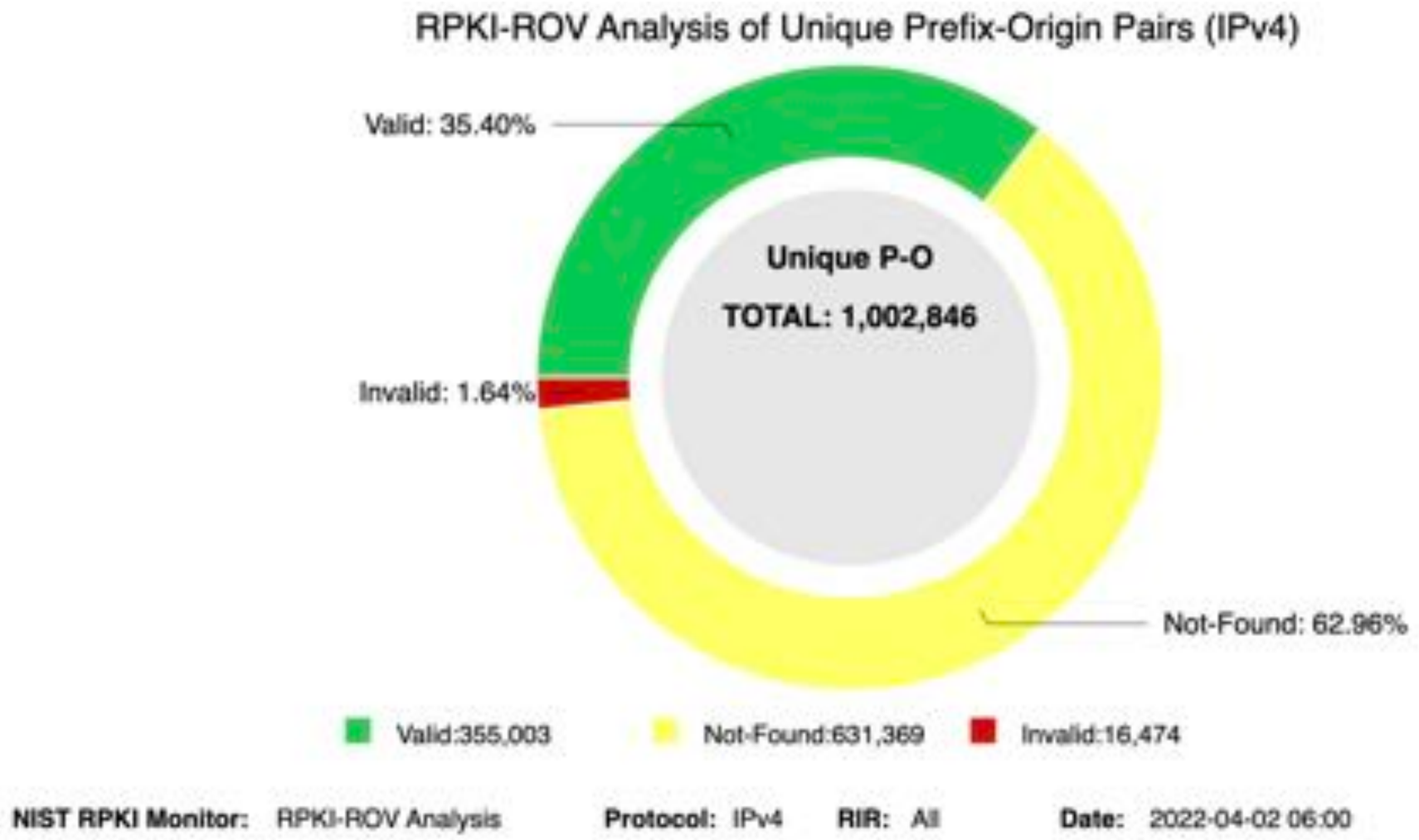
Prefix without a ROA

```
U1_Router#show  ip bgp 20.20.20.0/24
BGP routing table entry for 20.20.20.0/24, version 2240082
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 3
  99 102
    192.168.1.2 from 192.168.1.254 (99.0.0.1)
      Origin IGP, metric 0, localpref 80, valid, external, best
      path 7FD95FF03740 RPKI State not found
      rx pathid: 0, tx pathid: 0x0
```

Questions

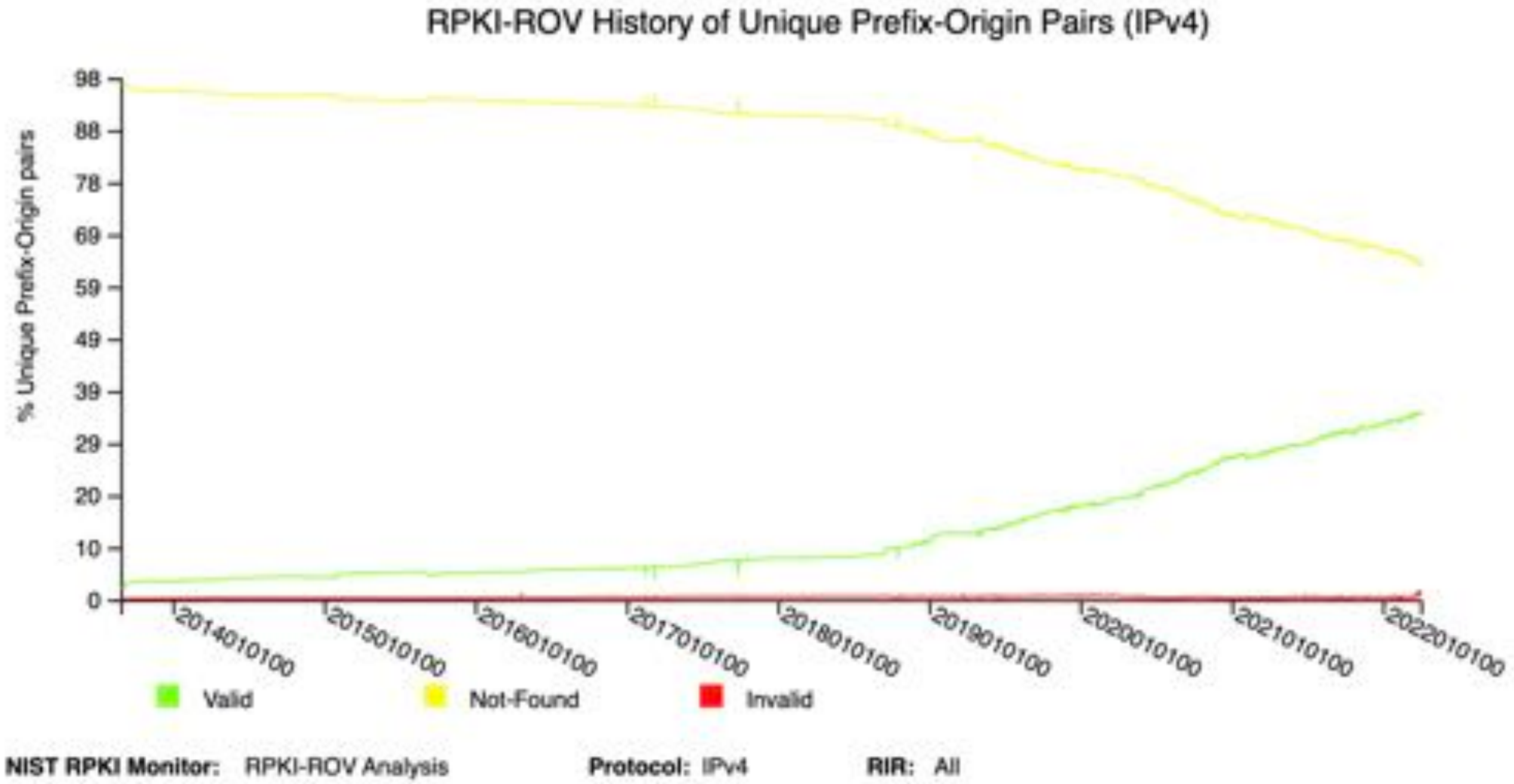
RPKI Statistics for Ukraine

Global RPKI Statistics



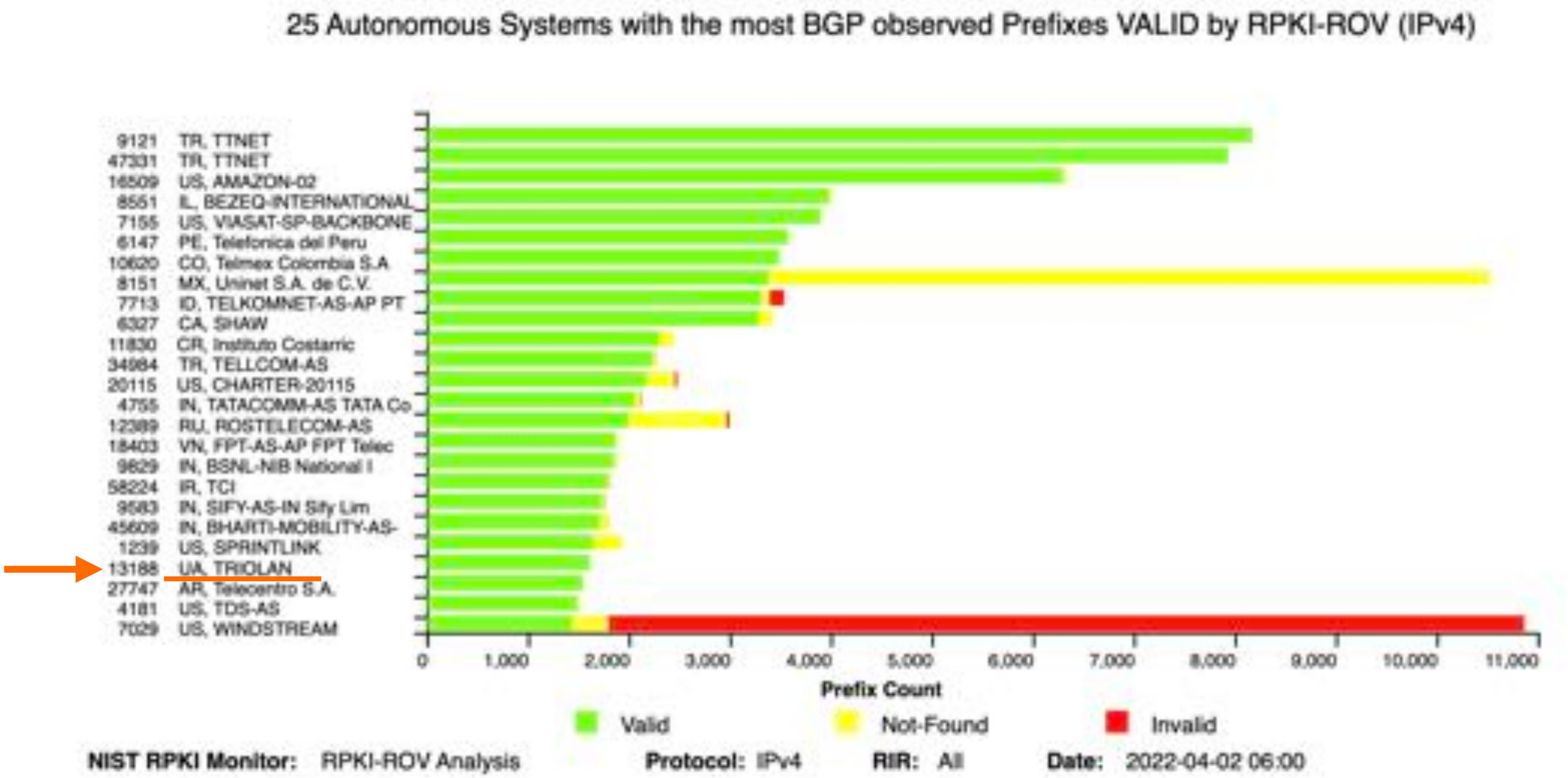
https://rpki-monitor.antd.nist.gov/

Global RPKI Statistics



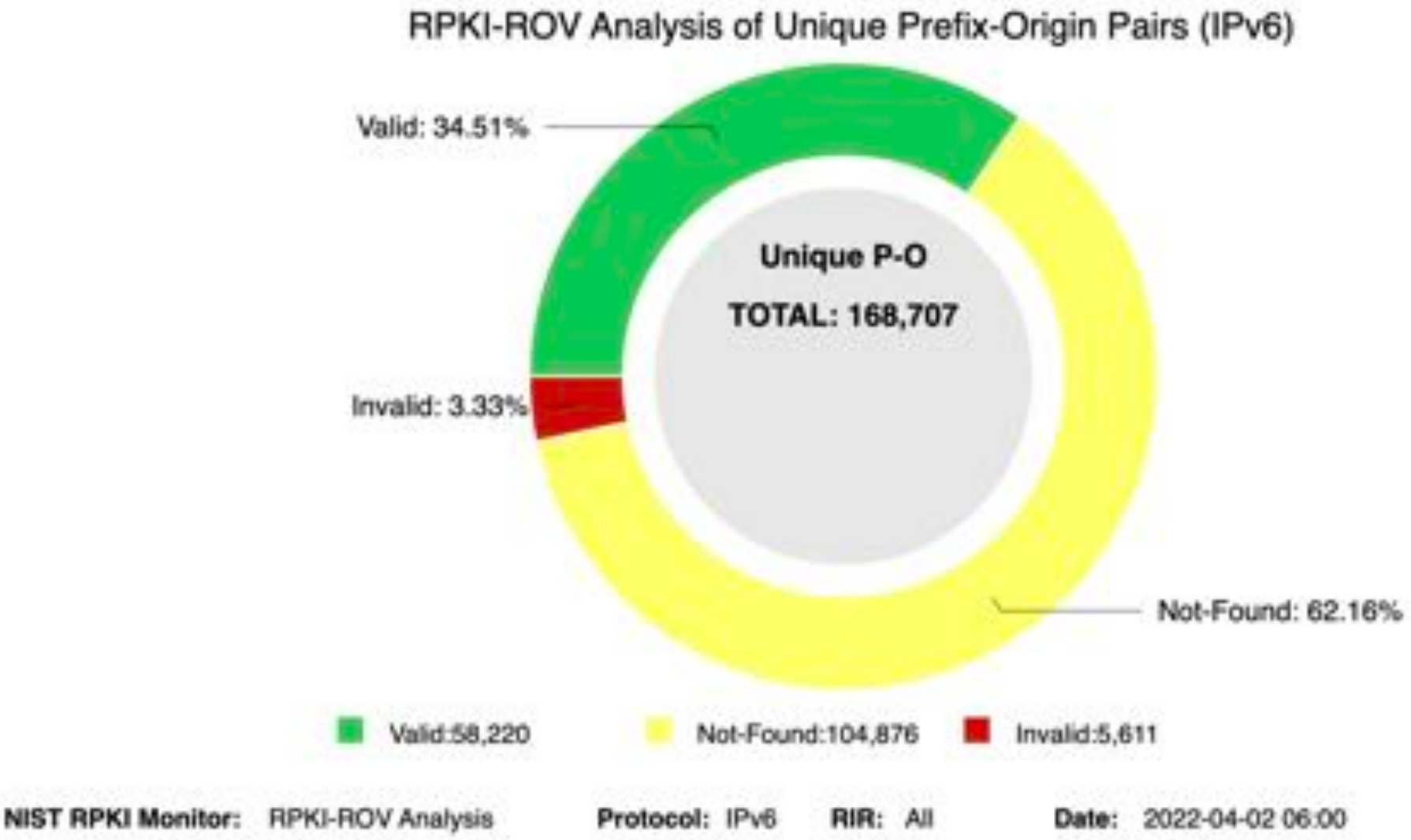
https://rpki-monitor.antd.nist.gov/

Global RPKI Statistics



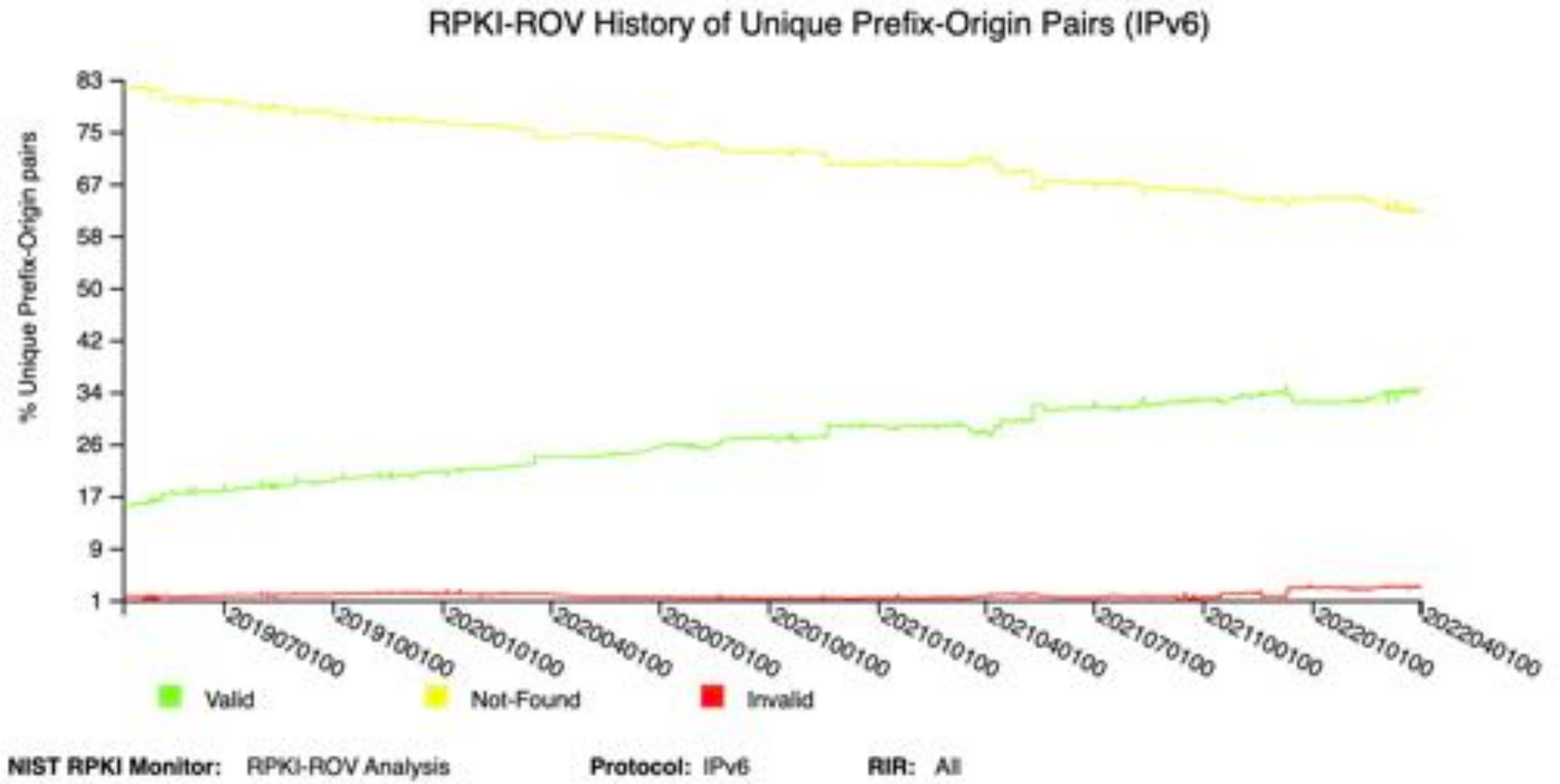
https://rpki-monitor.antd.nist.gov/

Global RPKI Statistics



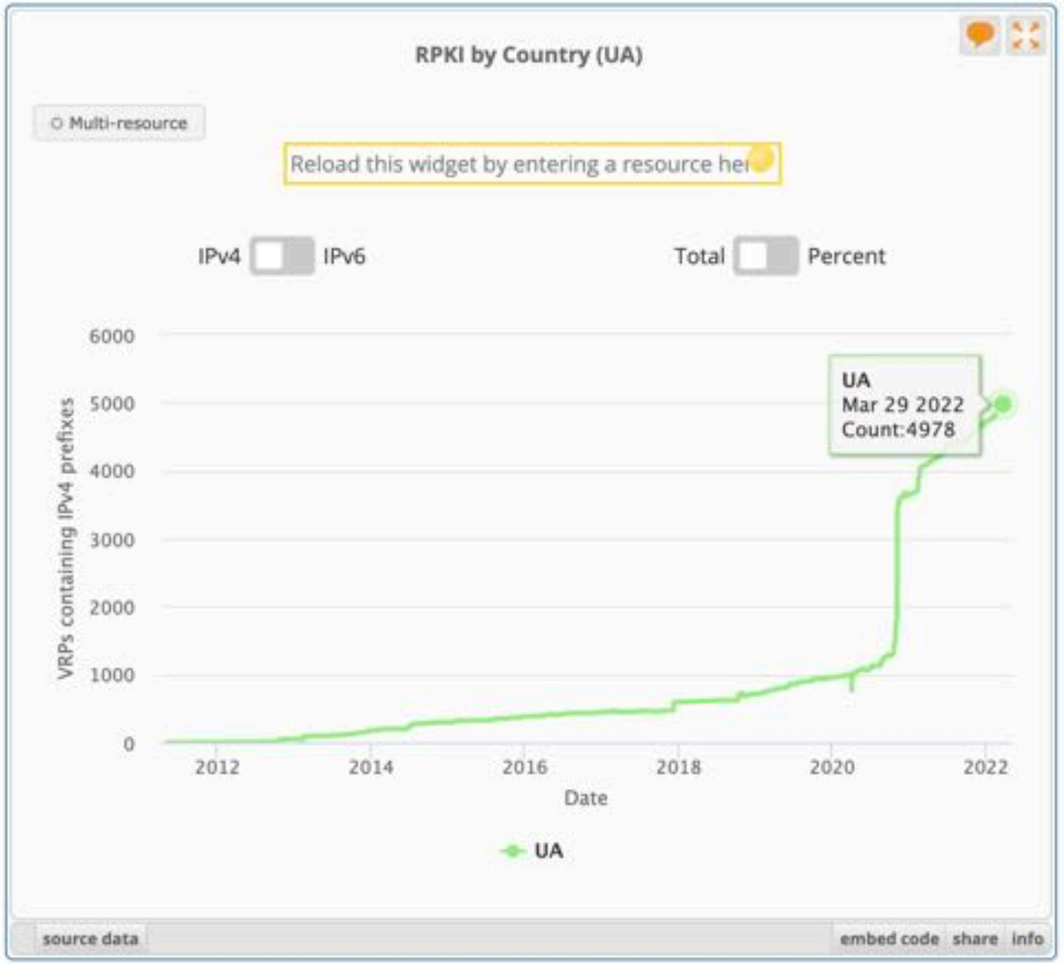
https://rpki-monitor.antd.nist.gov/

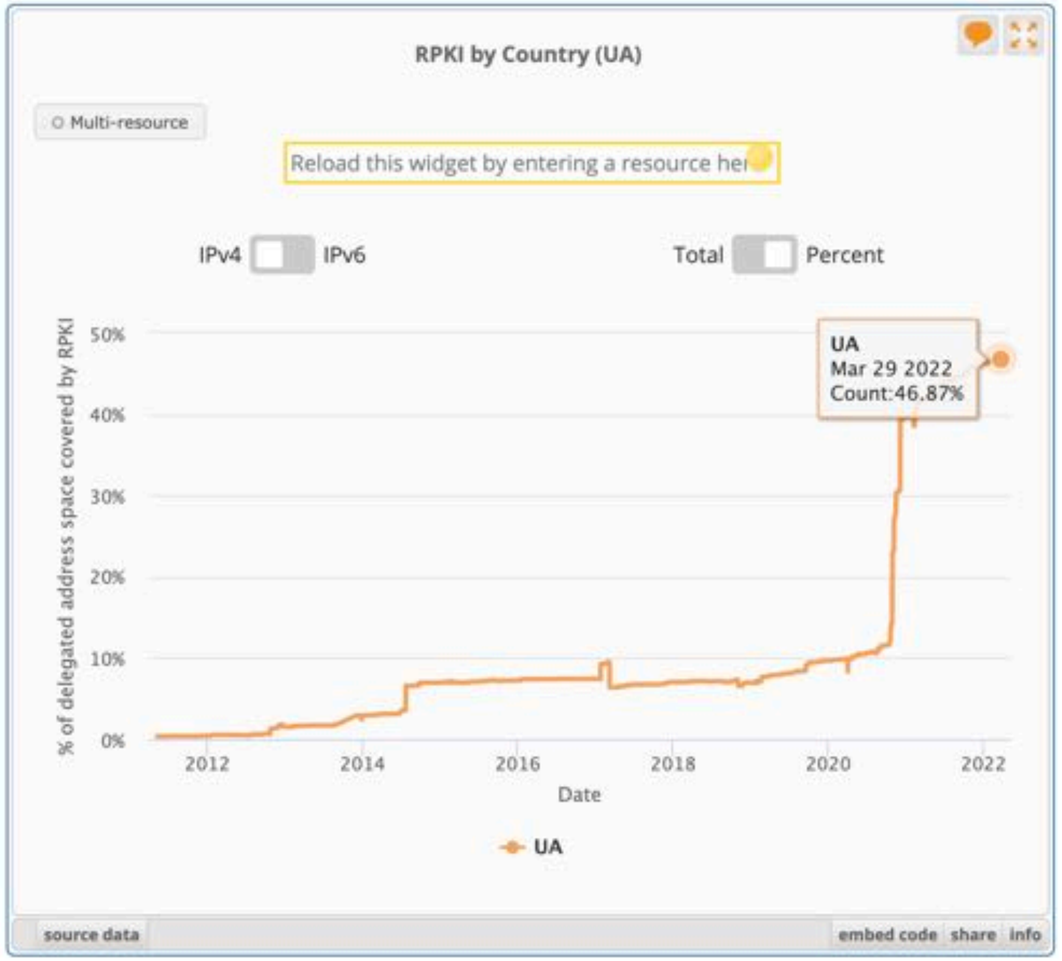
Global RPKI Statistics



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

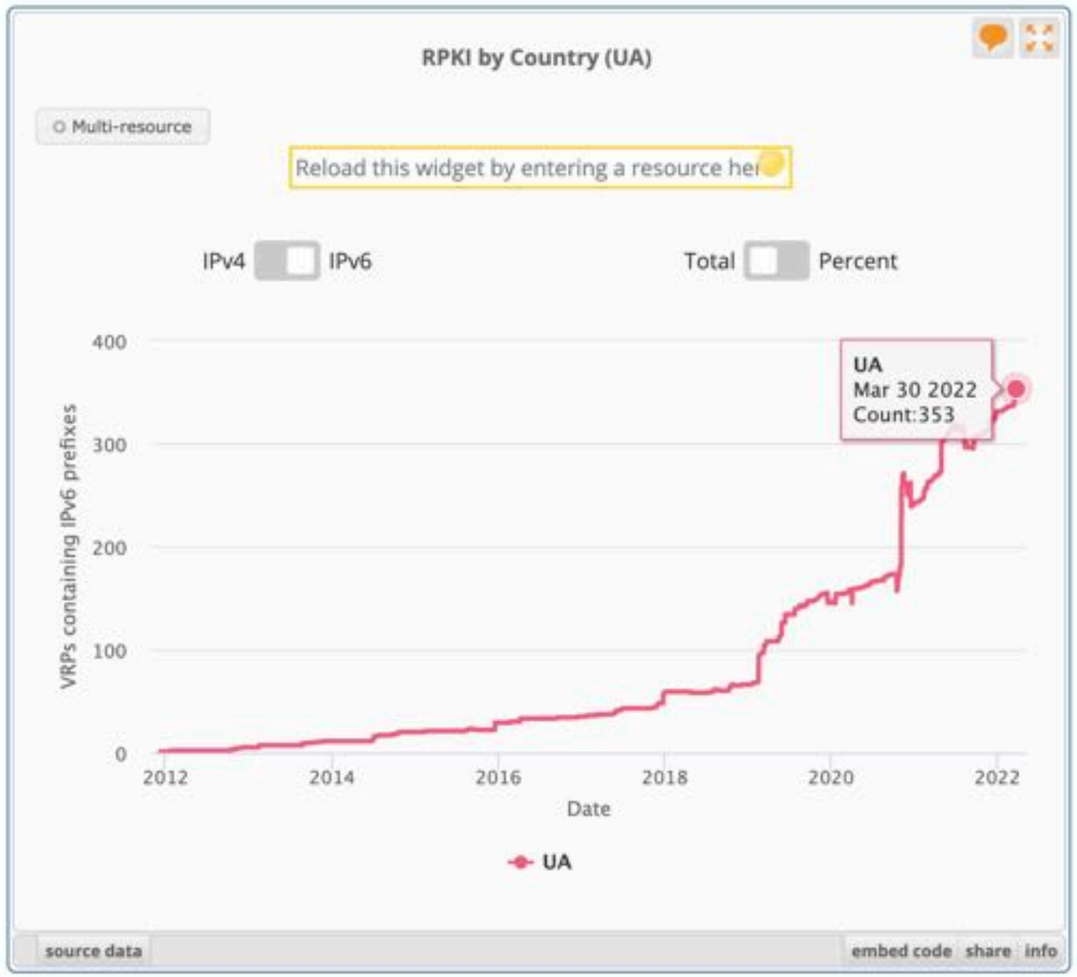
IPv4 Valid ROAs

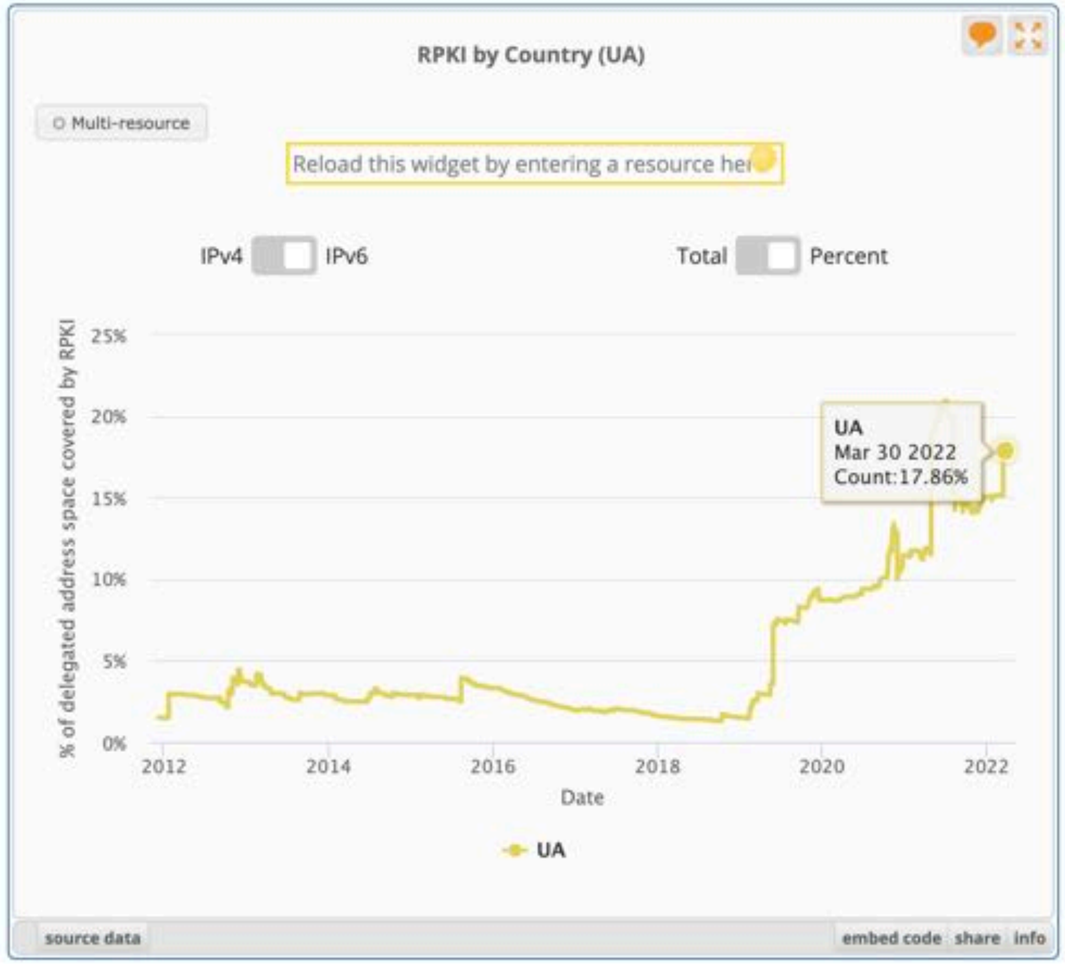




https://stat.ripe.net/widget/rpki-by-country

IPv6 Valid ROAs





https://stat.ripe.net/widget/rpki-by-country

Questions

We want your feedback!

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

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

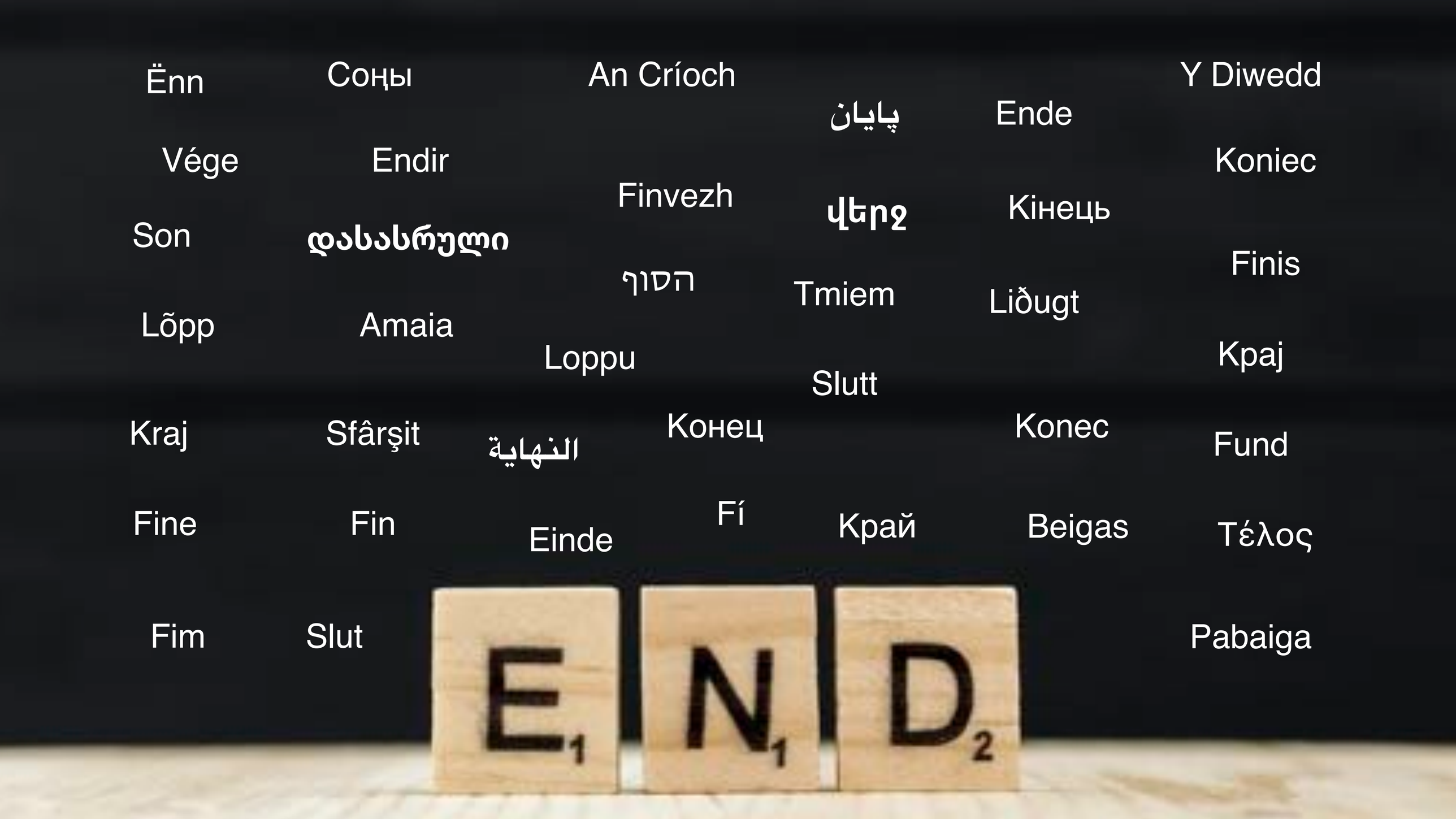
RIPE NCC
Academy

Learn something new today!

academy.ripe.net

RIPE NCC Certified Professionals

https://www.ripe.net/certifiedprofessionals


Ënn
Соңы
An Críoch
پایان
Ende
Y Diwedd
Vége
Endir
Finvezh
վերջ
Koniec
Son
დასასრული
Кінець
Finis
הסוף
Tmiem
Liðugt
Lõpp
Amaia
Kpaj
Loppu
Slutt
Kraj
Sfârşit
Конец
Konec
Fund
النهاية
Fí
Fine
Fin
Край
Beigas
Τέλος
Einde
Fim
Slut
Pabaiga
E1 N1 D2