RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Introduction to RPKI

Webinar

RIPE NCC Learning & Development

Agenda

Is BGP safe?

ROAs

Validation Tools

Validation

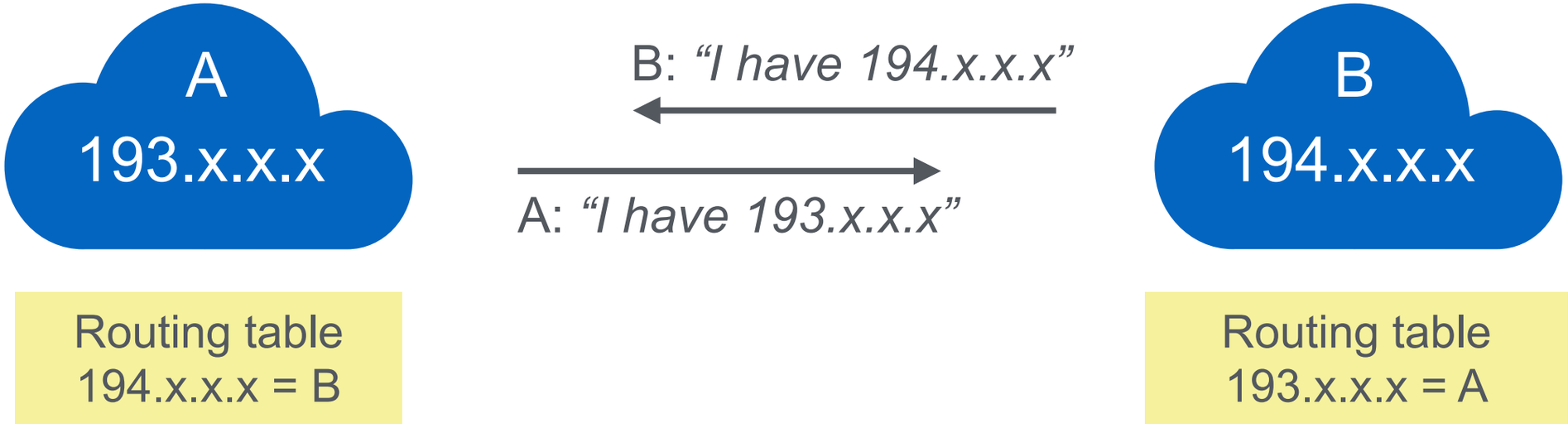
Is BGP safe?

Routing on the Internet

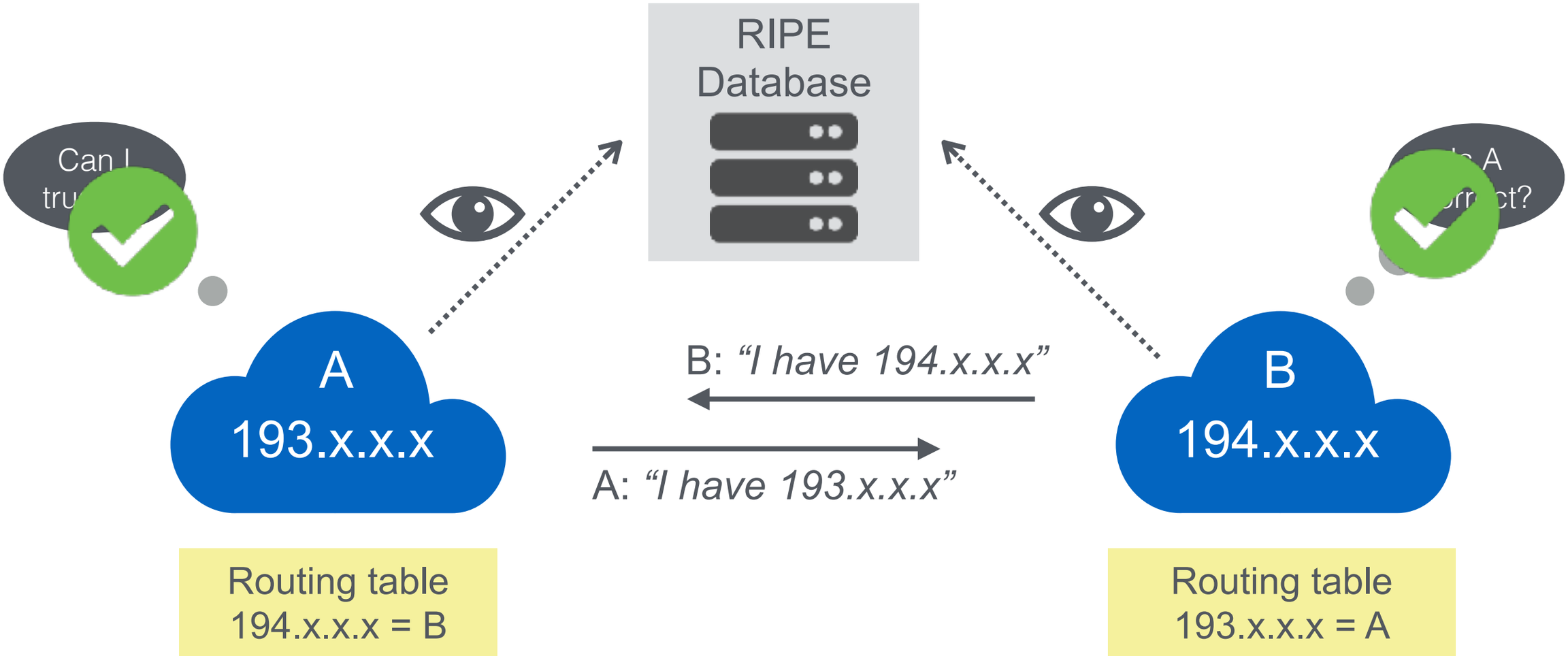
Can I trust B?

Is A correct?

"BGP protocol"



Routing on the Internet



Accidents Happen

- Fat Fingers
  - 2 and 3 are really close on our keyboards….
- Policy Violations (leaks)
  - Oops, we did not want this to go on the public Internet
  - Infamous incident with Pakistan Telecom and YouTube

Incidents Are Common

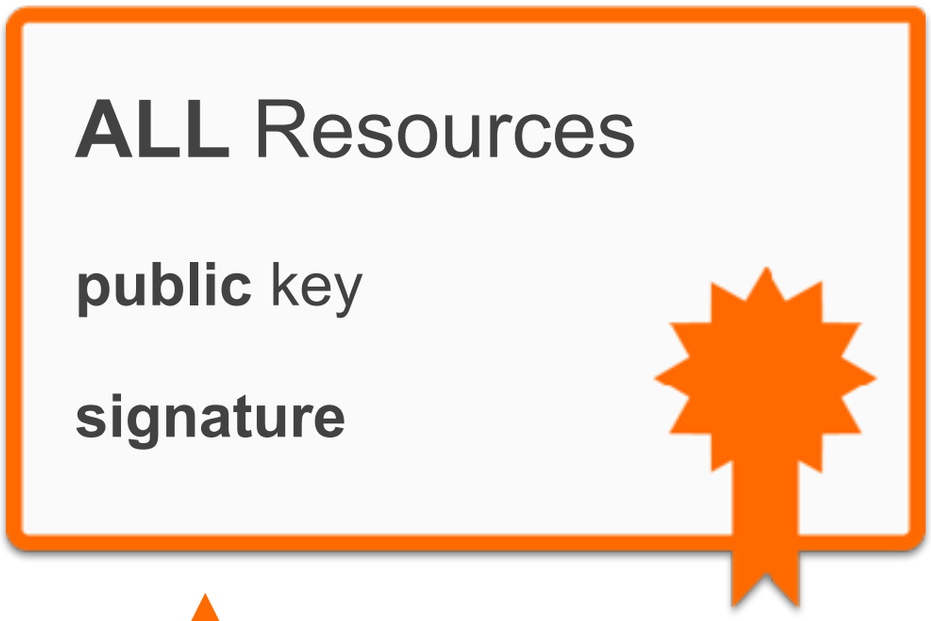
- 2019 Routing Security Review
  - 12,600 incidents
  - 4,4% of all ASNs affected
  - 3,000 ASNs are victims of at least one incident
  - 1,300 ASNs caused at least one incident

Source: https://bgpstream.com

Resource Public Key Infrastructure

- Ties IP addresses and ASNs to public keys
- Follows the hierarchy of the registries
- Authorised statements from resource holders
  - “ASN X is authorised to announce my Prefix Y”
  - Signed, holder of Y

RPKI Chain of Trust

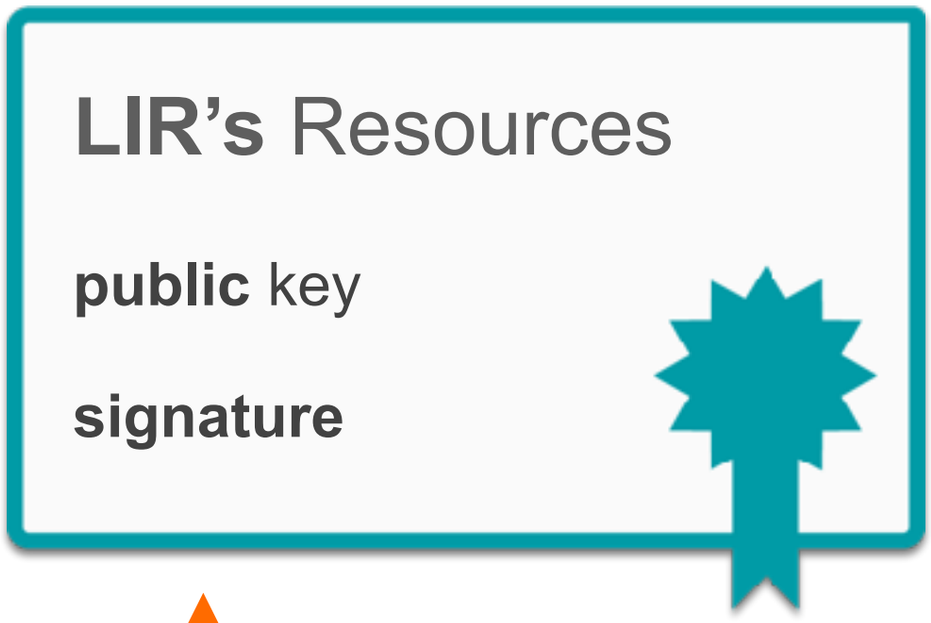


RIPE NCC Root Certificate

Self-signed

Root's **private** key

RPKI Chain of Trust



LIR Certificate

Signed by the Root private key

Root's **private** key

ROAs

ROA (Route Origin Authorisation)

- A ROA is…
- LIRs can create a ROA for each one of their resources (IP address ranges)
- Multiple ROAs can be created for an IP range
- ROAs can overlap

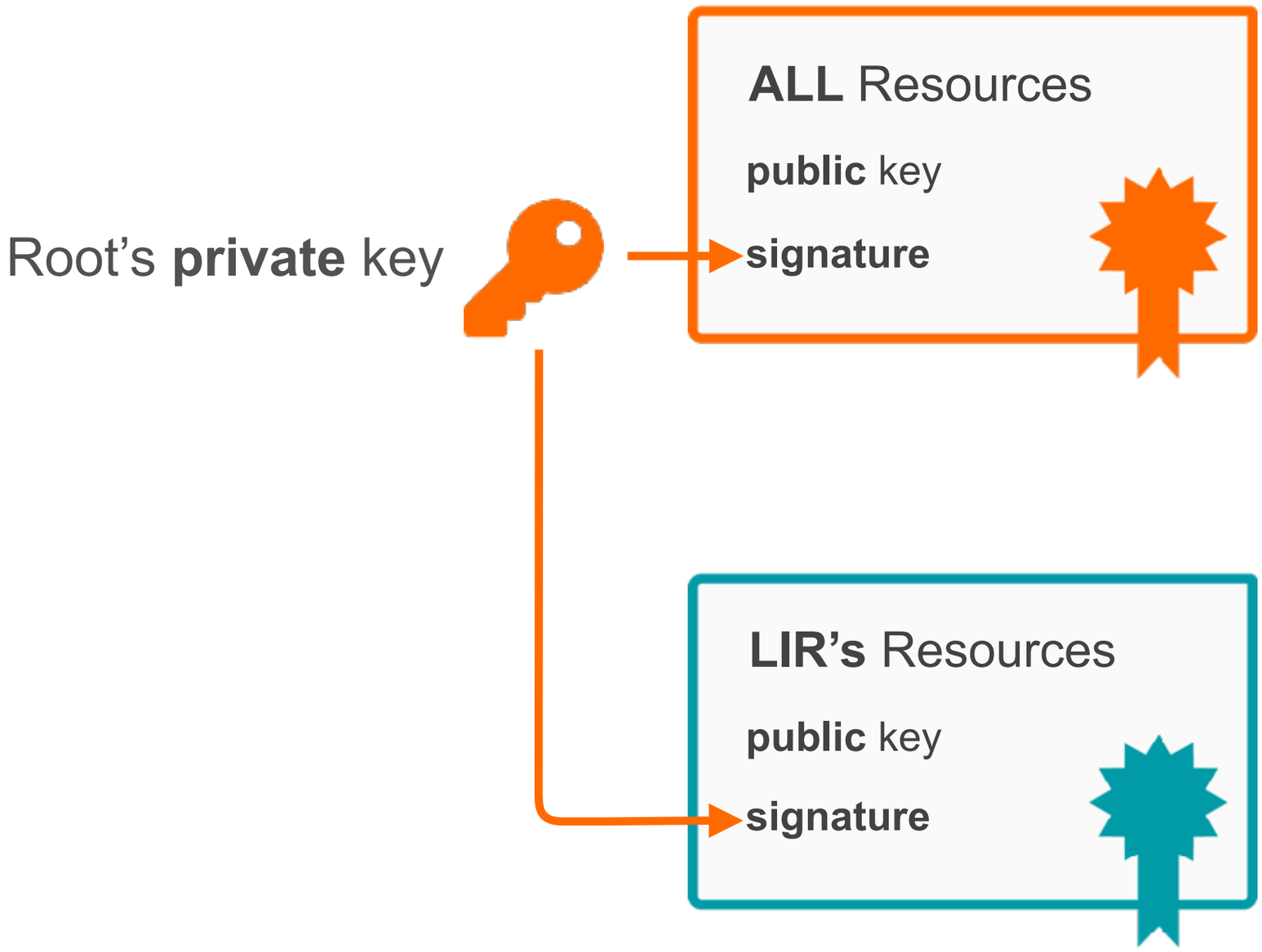
What is in a ROA ?

Prefix → The network for which you are creating the ROA

Origin ASN → The ASN that's supposed to be originating the BGP Announcement

Max Length → The Maximum prefix length accepted for this ROA

RPKI Chain of Trust



Route Origin Authorisation

ROA

signature

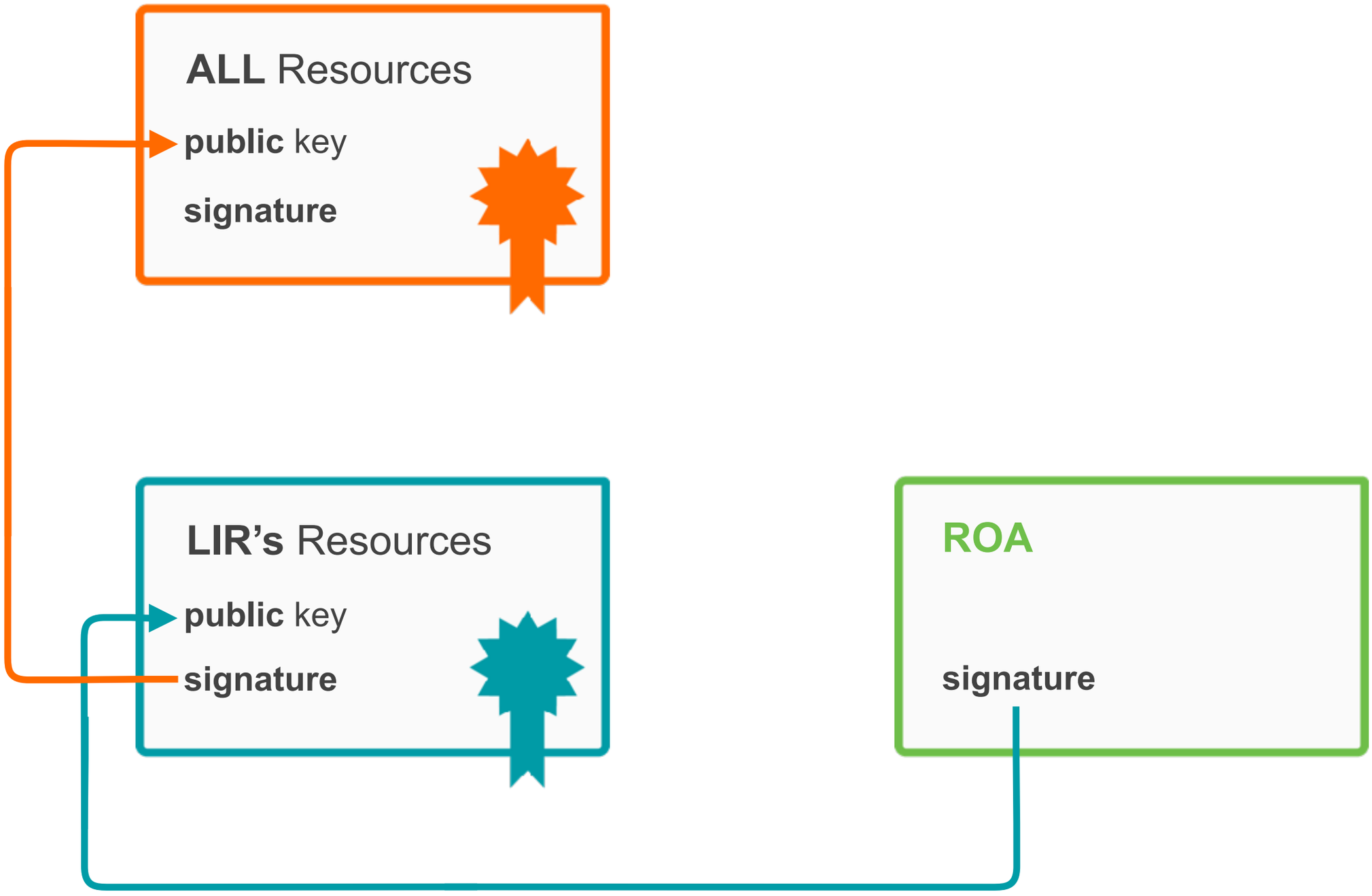
LIR's **private** key

Prefix

is authorised to be announced by

AS Number

RPKI Chain of Trust



Hosted RPKI

- Automatic signing and key roll overs
  - One click setup of resource certificate
  - User has a valid and published certificate for as long as they are the holder of the resources
  - All the complexity is handled by the hosted system
- Lets you focus on creating and publishing ROAs
  - Match your intended BGP configuration

Creating ROAs

RPKI Dashboard

9 CERTIFIED RESOURCES | NO ALERT EMAIL CONFIGURED

41 BGP Announcements

4 Valid | 1 Invalid | 36 Unknown

4 ROAs

3 OK | 1 Causing problems

BGP Announcements | Route Origin Authorisations (ROAs) | History

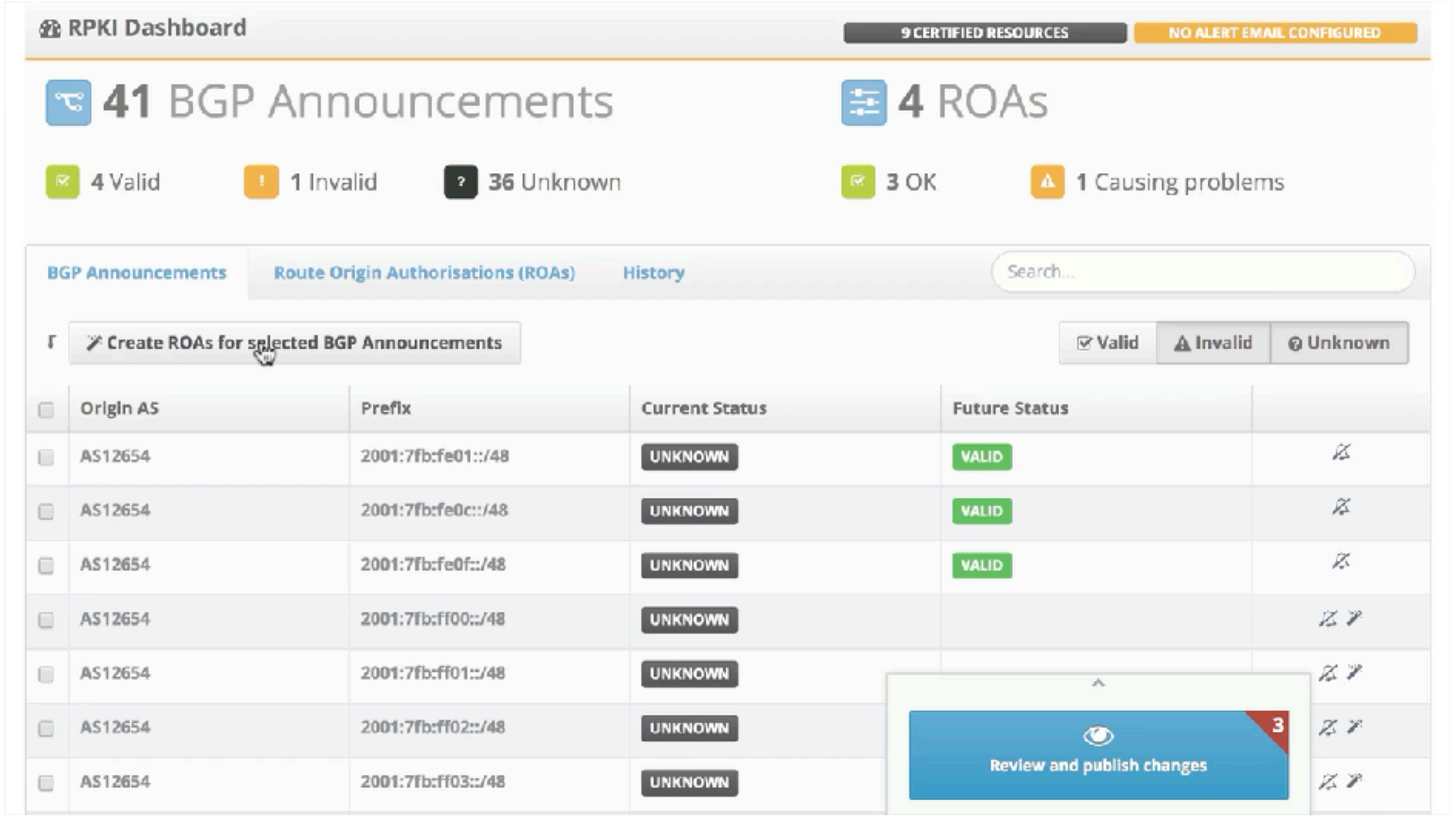
Search...

Create ROAs for selected BGP Announcements

Valid | Invalid | Unknown

Origin AS	Prefix	Current Status
AS12654	2001:7fb:fe01::/48	UNKNOWN
AS12654	2001:7fb:fe0c::/48	UNKNOWN
AS12654	2001:7fb:fe0f::/48	UNKNOWN
AS12654	2001:7fb:ff00::/48	UNKNOWN
AS12654	2001:7fb:ff01::/48	UNKNOWN
AS12654	2001:7fb:ff02::/48	UNKNOWN
AS12654	2001:7fb:ff03::/48	UNKNOWN

Reviewing changes



Checking the effects

RPKI Dashboard

9 CERTIFIED RESOURCES | NO ALERT EMAIL CONFIGURED

41 BGP Announcements

7 Valid | **1** Invalid | **33** Unknown

7 ROAs

6 OK | **1** Causing problems

BGP Announcements | Route Origin Authorisations (ROAs) | History

Search...

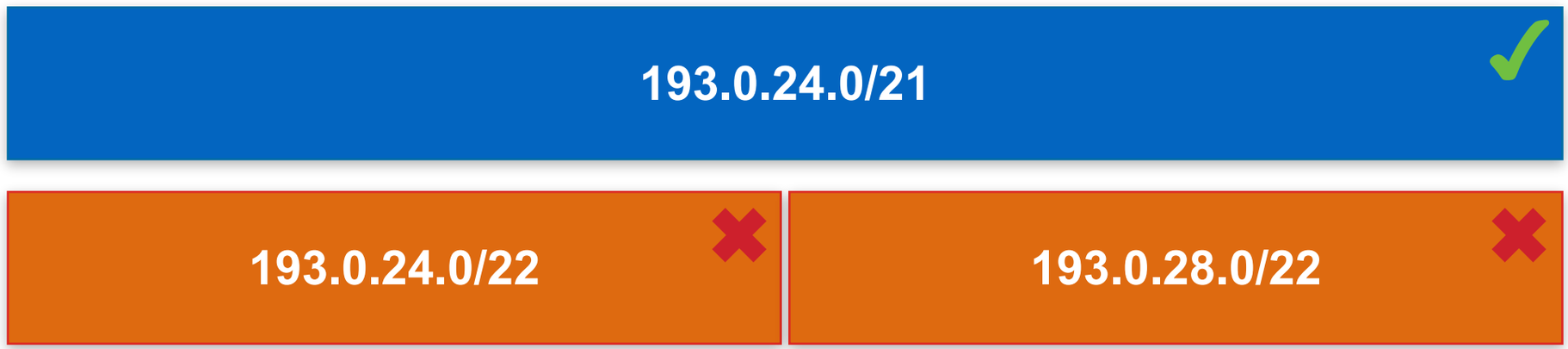
Create ROAs for selected BGP Announcements

Valid | Invalid | Unknown

Origin AS	Prefix	Current Status
AS12654	2001:7fb:ff00::/48	UNKNOWN
AS12654	2001:7fb:ff01::/48	UNKNOWN
AS12654	2001:7fb:ff02::/48	UNKNOWN
AS12654	2001:7fb:ff03::/48	UNKNOWN
AS12654	2001:7fb:ff04::/48	UNKNOWN
AS12654	2001:7fb:ff05::/48	UNKNOWN
AS12654	2001:7fb:ff07::/48	UNKNOWN

ROA

193.0.24.0/21
AS2121
Max Length: /21

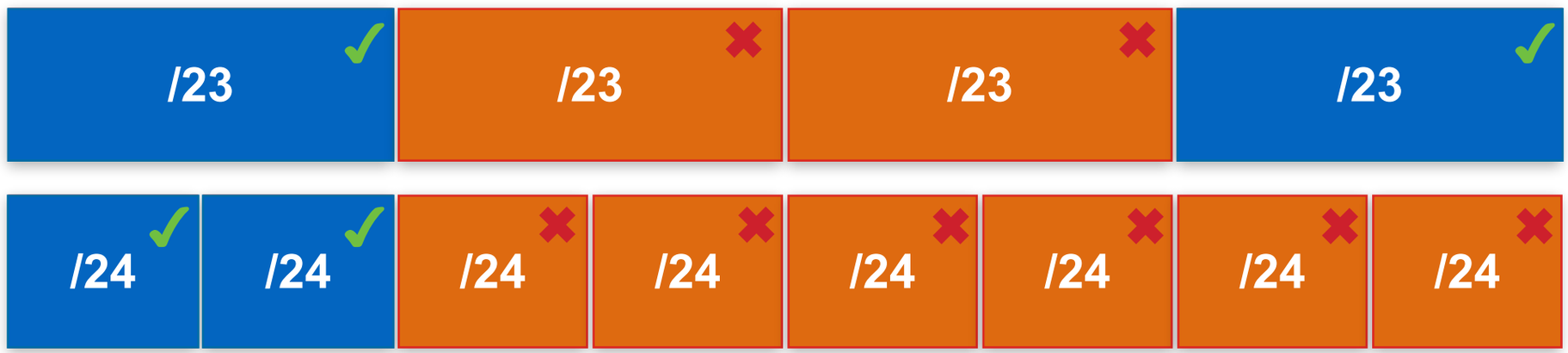


ROA

193.0.24.0/23
AS2121
Max Length: /24

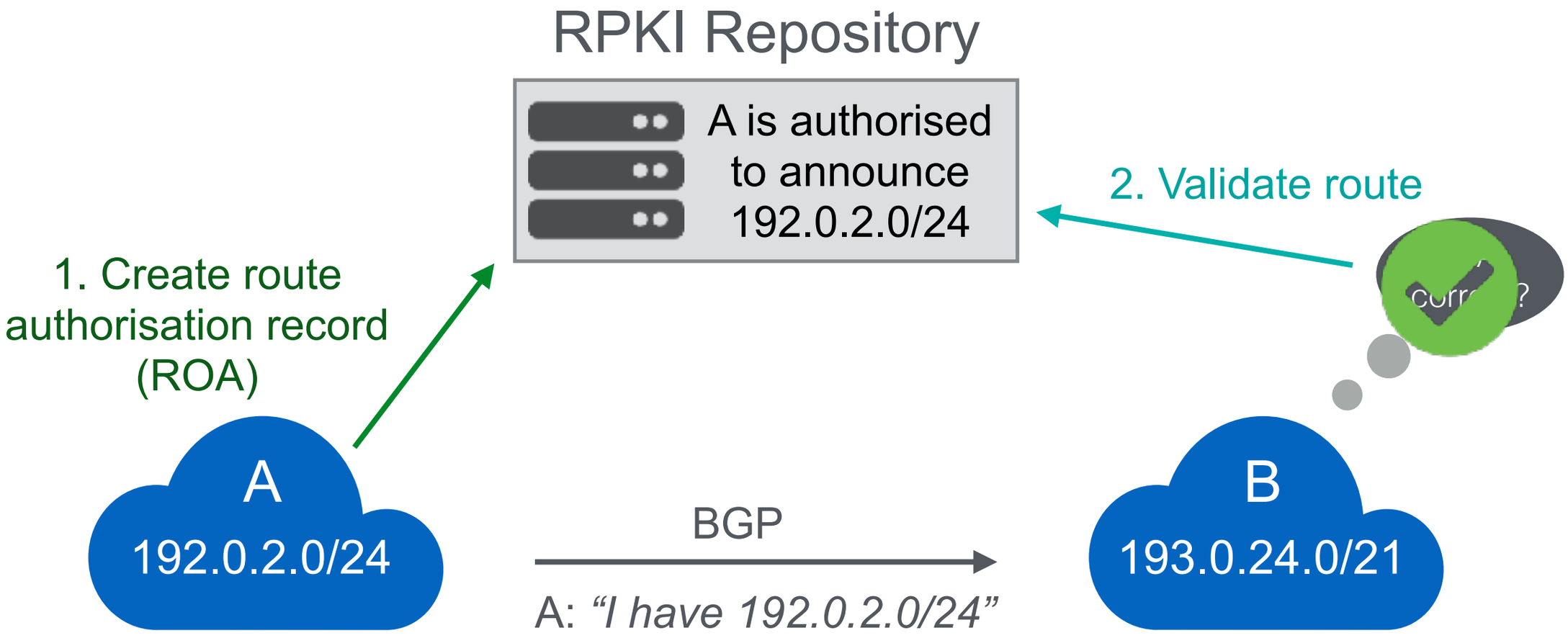
ROA

193.0.30.0/23
AS2121
Max Length: /23



Validation Tools

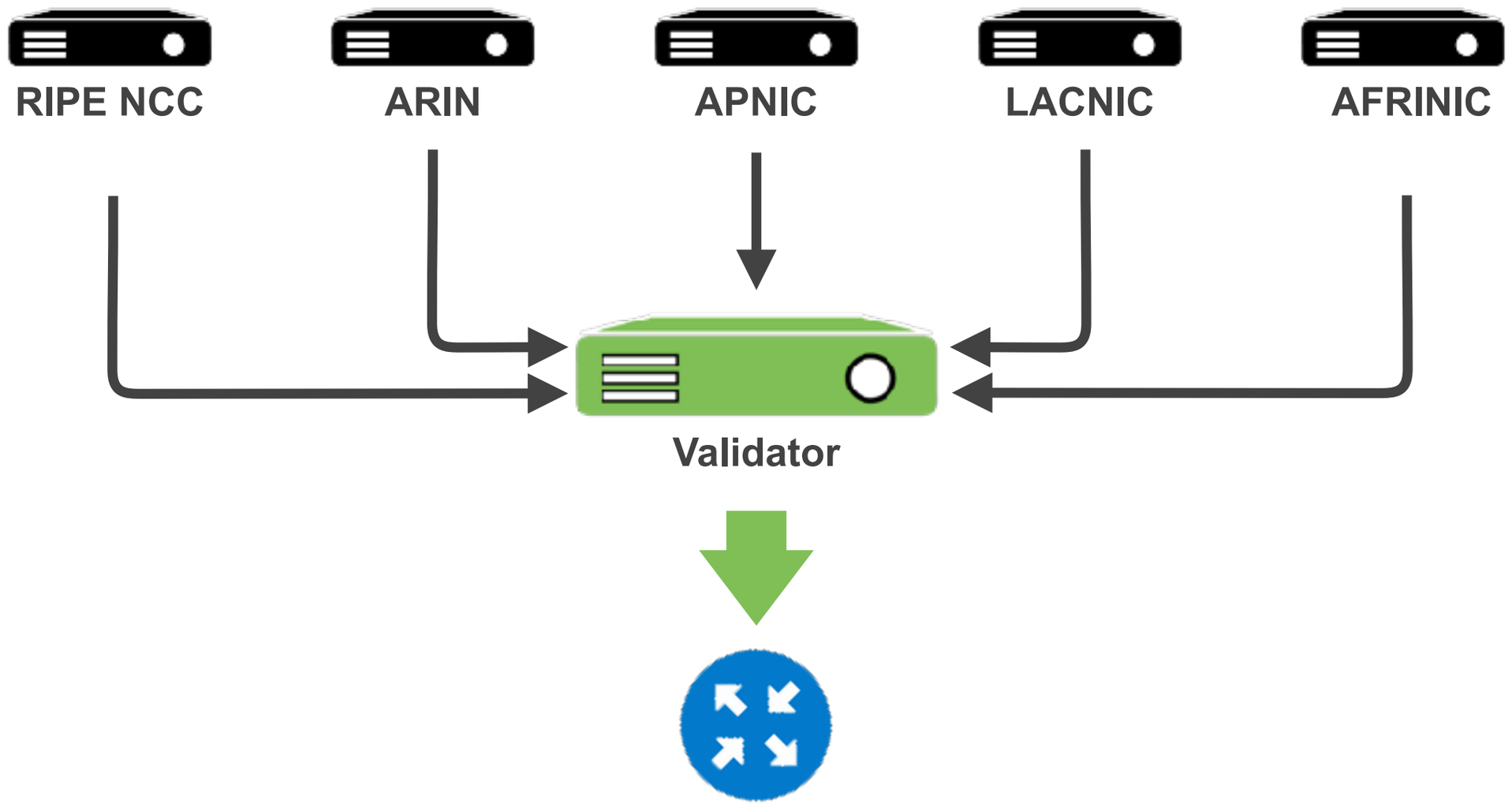
Routing on the Internet



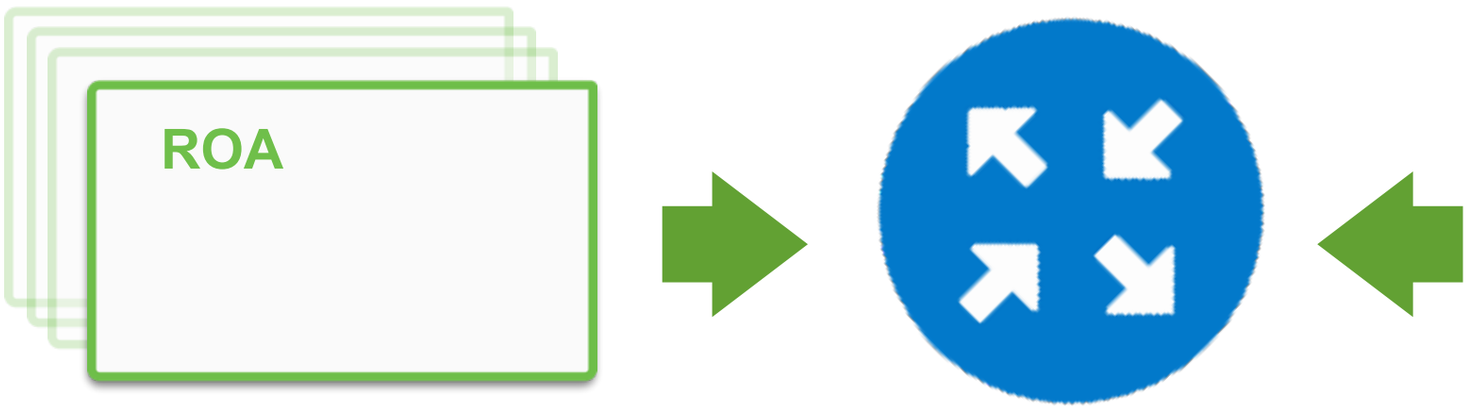
RPKI Validators

- Software that creates a local “validated cache” with all the valid ROAs
  - Downloads the RPKI repository from the RIRs
  - Validates the chain of trust of all the ROAs and associated CAs
  - Talks to your routers using the RPKI-RTR Protocol

Relying Party



Relying Party



BGP Announcements

AS111	10.0.7.30/22
AS222	10.0.6.10/24
AS333	10.4.17.5/20
AS111	10.0.7.30/22
AS111	10.0.7.30/22
AS111	10.0.7.30/22

BETTER ROUTING DECISIONS

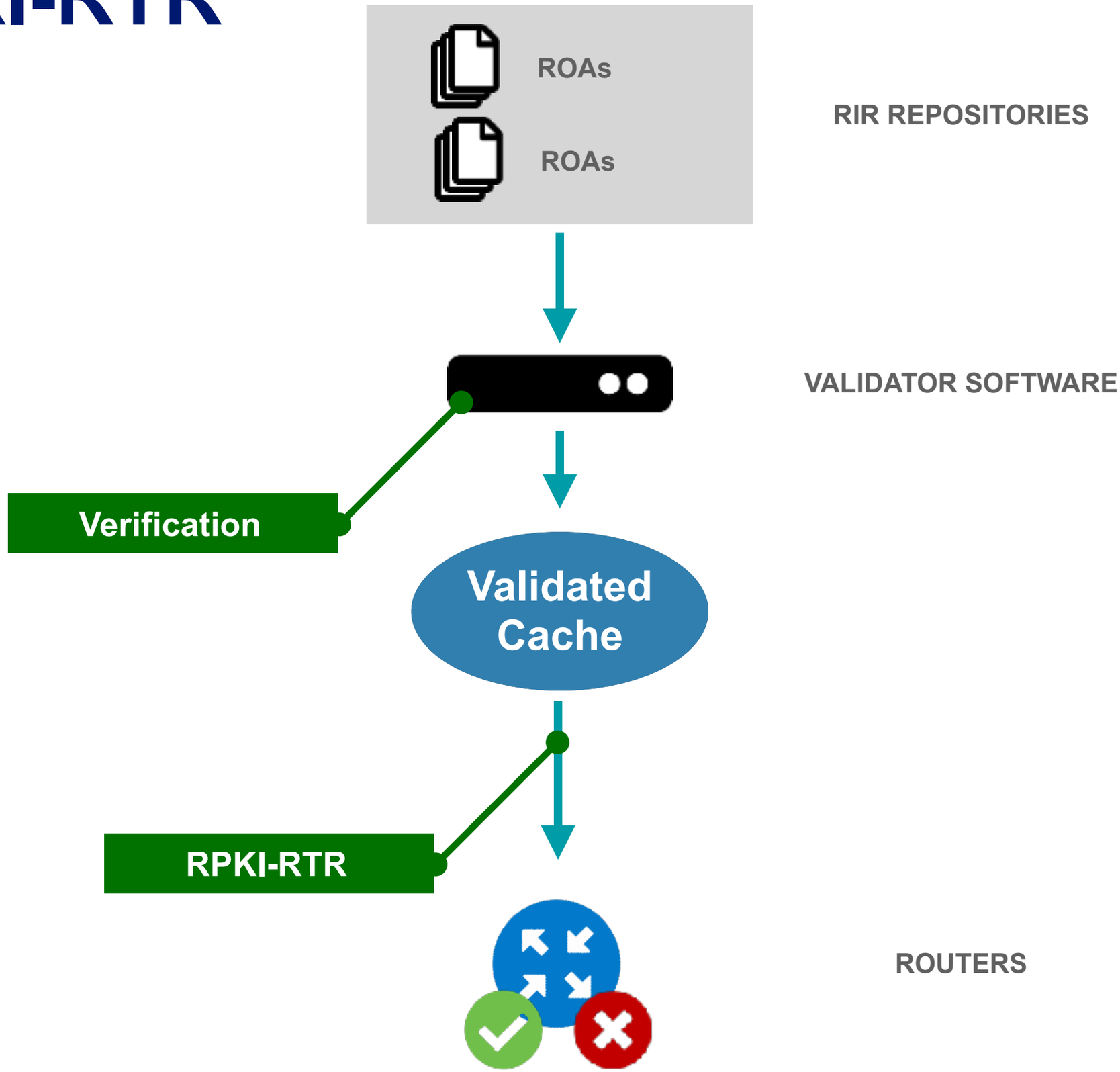
RPKI Validator Options

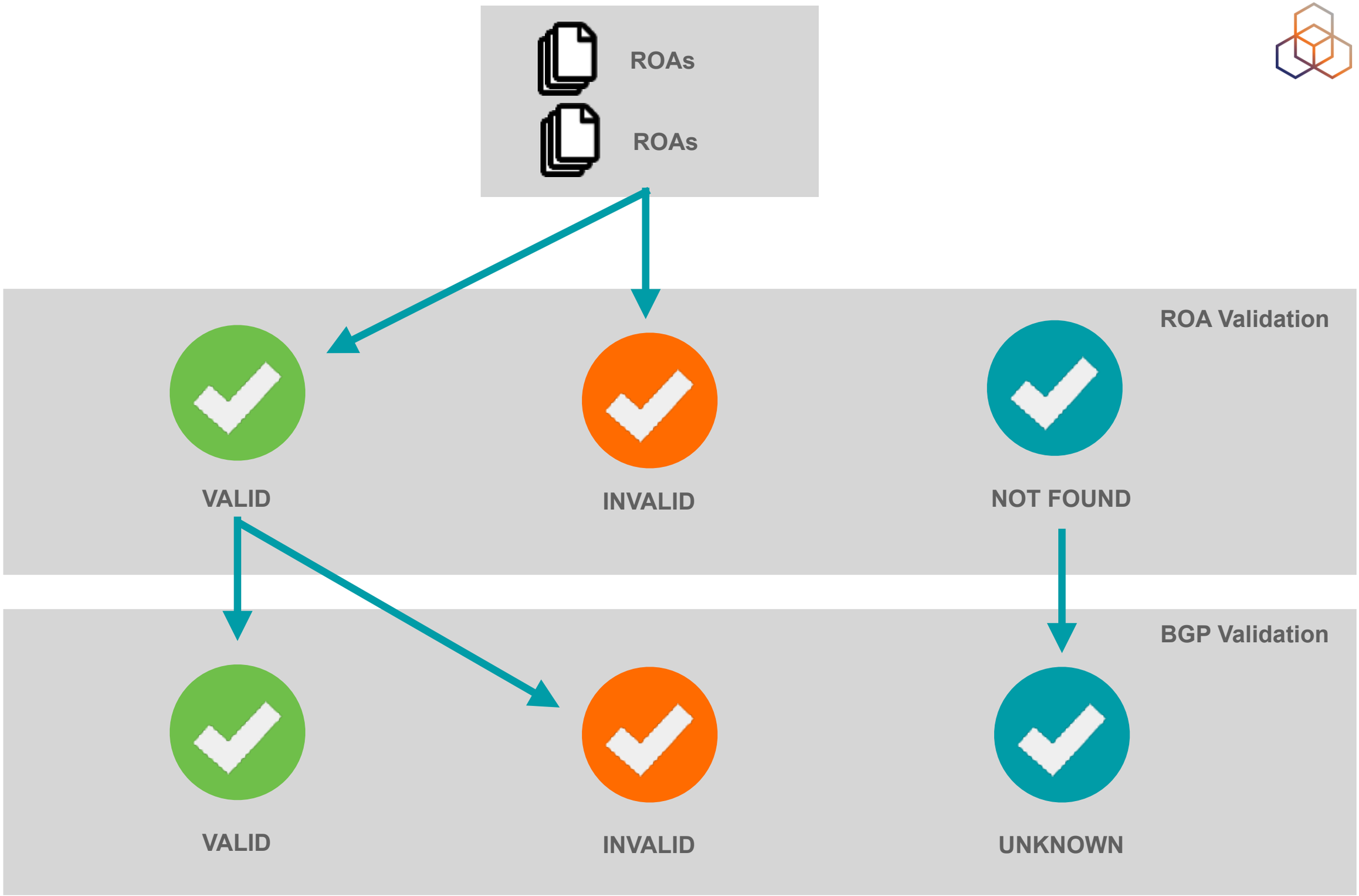
January 1, 2021 no new features!

July 1, 2021 end of support!

- **RIPE NCC Validator 3.2**
  - Java based
- **Routinator**
  - Built with Rust, built by NLNetlabs
- **OctoRPKI**
  - Cloudflare’s Relying Party software, written in the Go
- **Dragon Research Labs Validating Cache**
  - Written in Python

RPKI-RTR


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


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

Invalids

- Invalid ROA
  - The ROA in the repository cannot be validated by the client (ISP) so it is not included in the validated cache
- Invalid BGP announcement
  - There is a ROA in validated cache for that prefix but for a different AS.
  - Or the max length doesn’t match.
- If no ROA in the cache then announcement is “unknown”

Whitelisting

- If there is an invalid ROA for a network that's important for you or your customers, you can whitelist it
- This is done on your local validator software
  - It creates a "fake" ROA for the resources you want
- It allows you to contact the operator to fix their ROA
  - Think of e-mail, contact forms, etc…

Questions

training@ripe.net

rpki@ripe.net

The End!

Край

Y Diwedd

Fí

Finis

النهاية

Соңы

վերջ

Liðugt

Ende

Finvezh

Кінець

Konec

Kraj

Ënn

Fund

پایان

Kpaj

Lõpp

Beigas

Vége

Son

An Críoch

הסוף

Endir

Fine

Sfârşit

Fin

Τέλος

Einde

Конец

Slut

Slutt

დასასრული

Pabaiga

Tmiem

Koniec

Fim

Amaia

Loppu