RPKI

What is it, and what it can do for you

Ralph Smit | 20 April 2023 | HRNOG

What is the problem again?

BGP announcements

- The Internet works with the Border Gateway Protocol (BGP)

- Routers use BGP to pass messages ("announcements")

- These announcements explain:

  - which network "owns" (originate) a particular prefix

  - which path to follow to reach that particular network/prefix

Untrusted BGP announcements

- The Internet is bigger than ever

- Lot of people are working on it, and can make a mistake

- There are also bad people

BGP4

- RFC1654 from 1994

- Can we update it?

- Can we add something "out of band"?
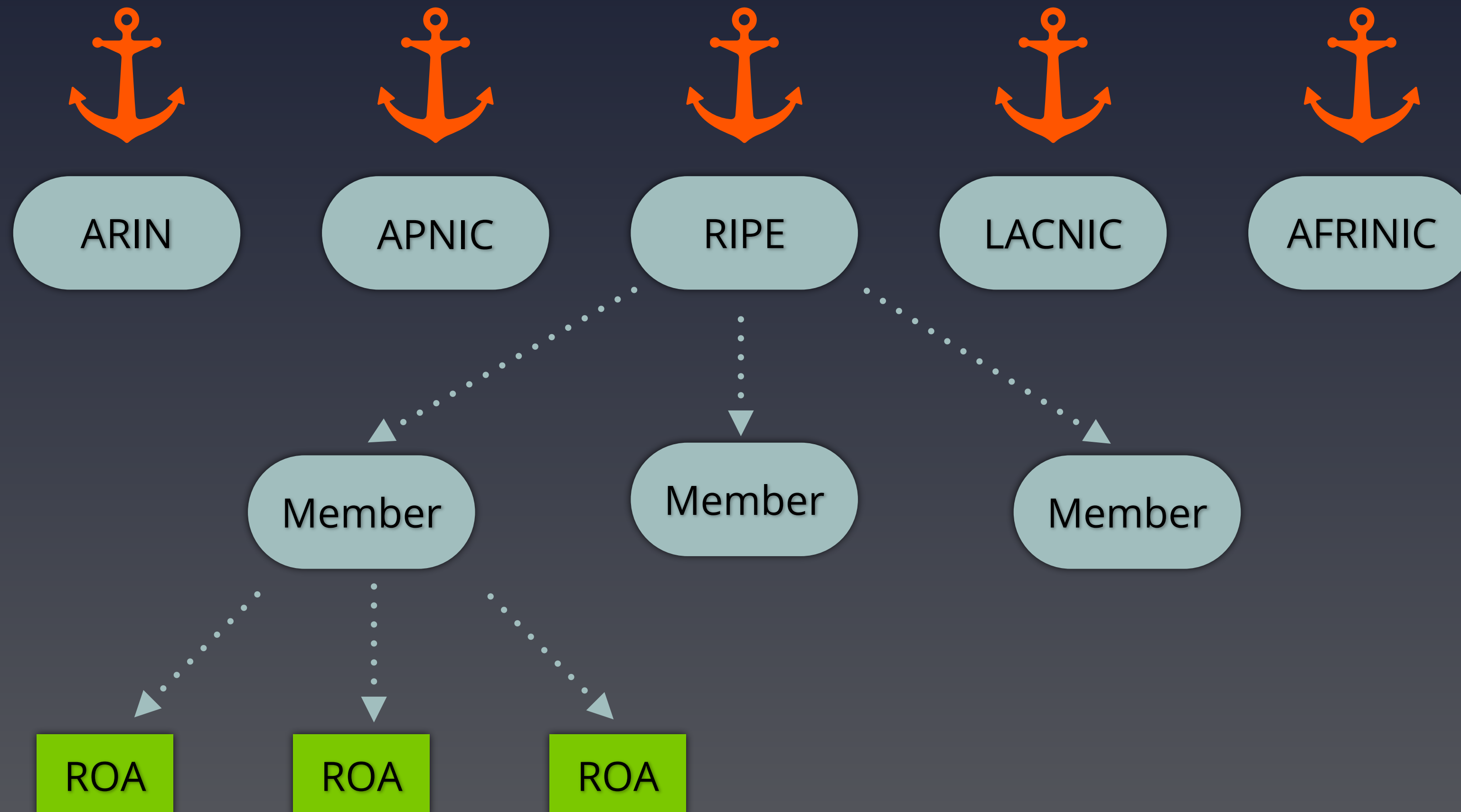
Something like?

- Prefix lists

- Internet Routing Registries (IRRs)

- Resource Public Key Infrastructure (RPKI)
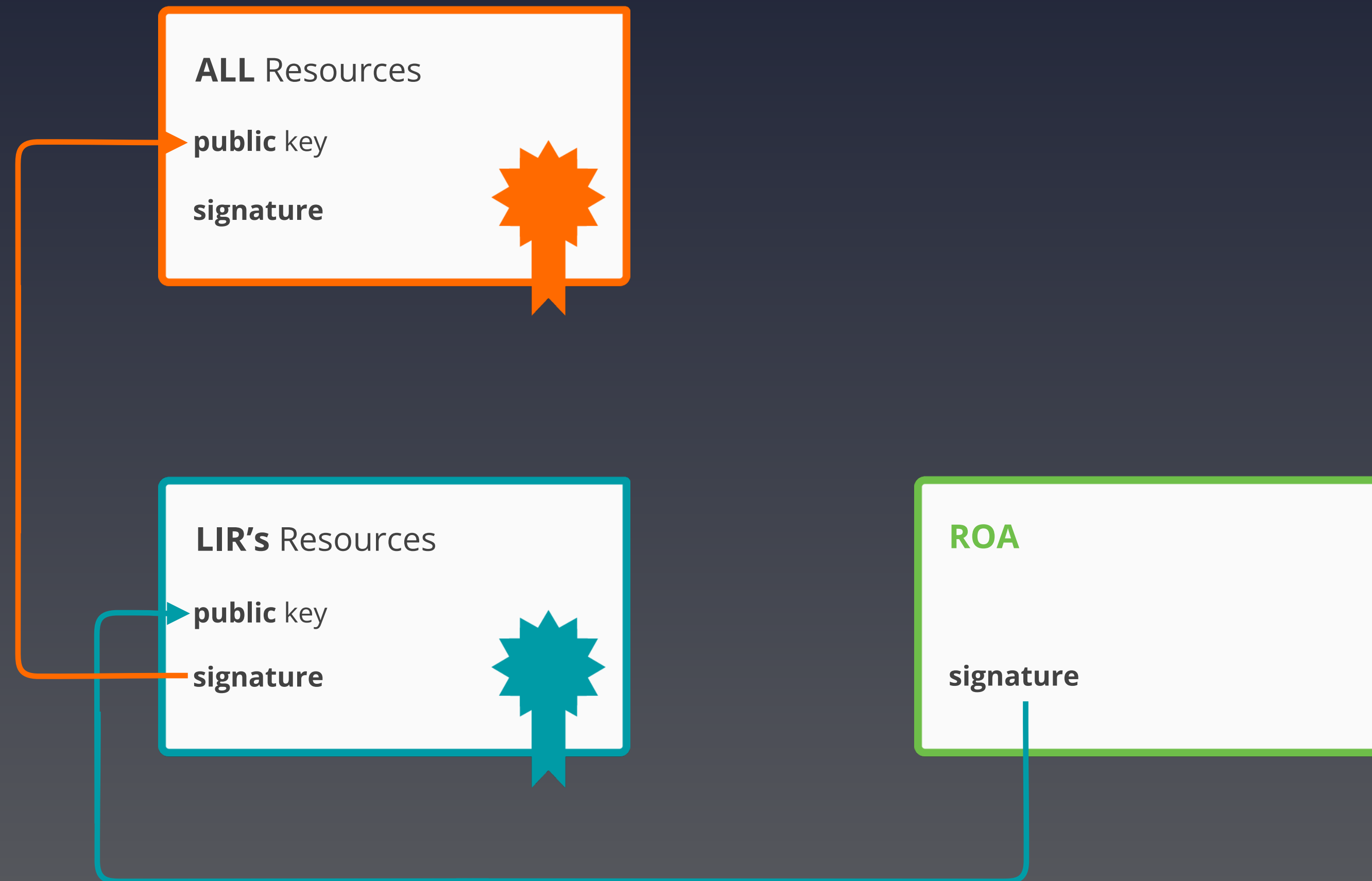
Resource Public Key Infrastructure

- Ties IP addresses and AS numbers to public keys

- Follows the hierarchy of the IP address registries

- Allows for authorised statements from IP address holders

  - AS X is authorised to announce my prefix Y
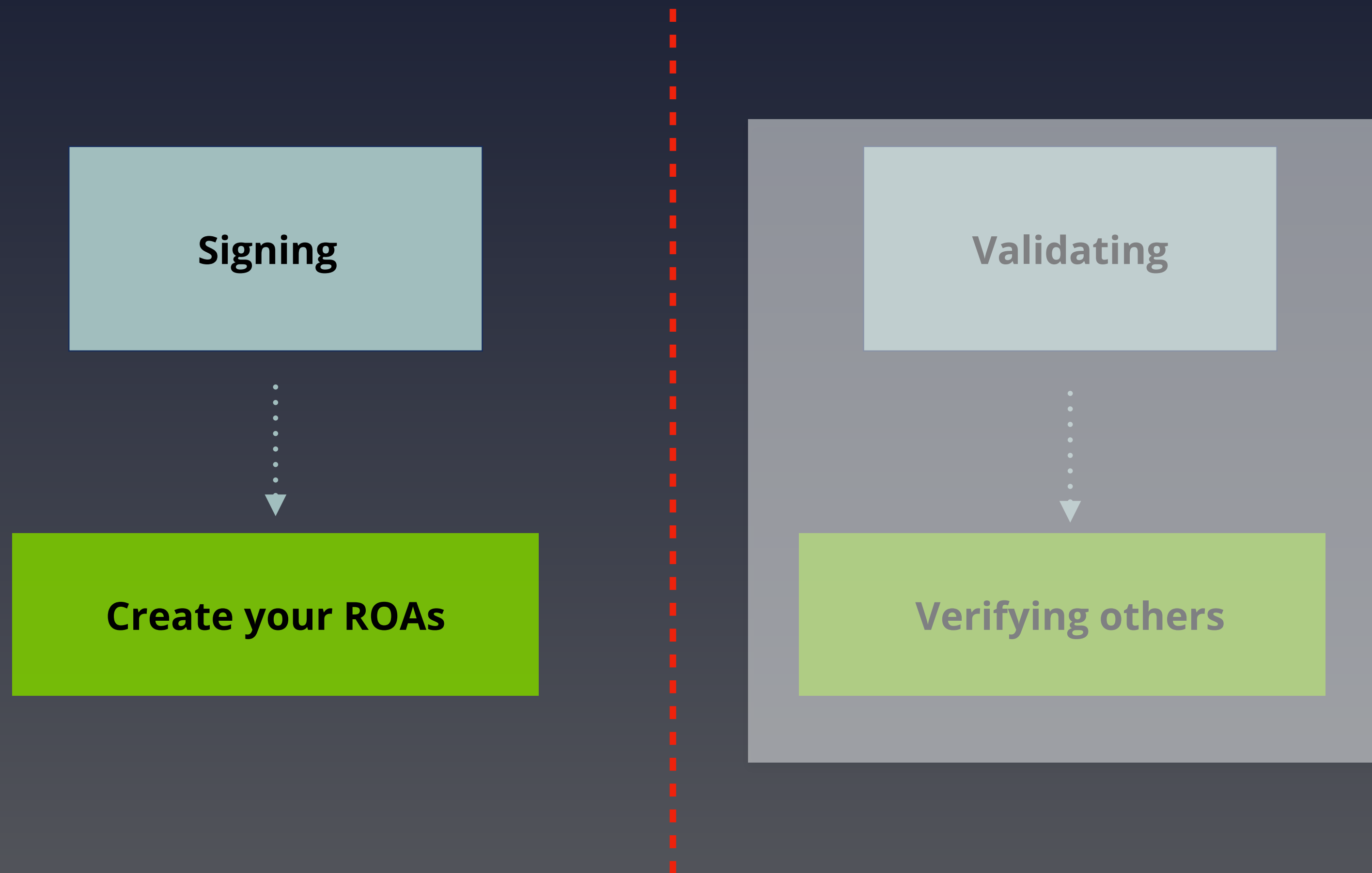
  - Signed, holder of Y

RPKI Certificate Structure

RPKI Chain of Trust

ALL Resources

public key

signature

LIR's Resources

public key

signature

ROA

signature

Two elements of RPKI

Signing
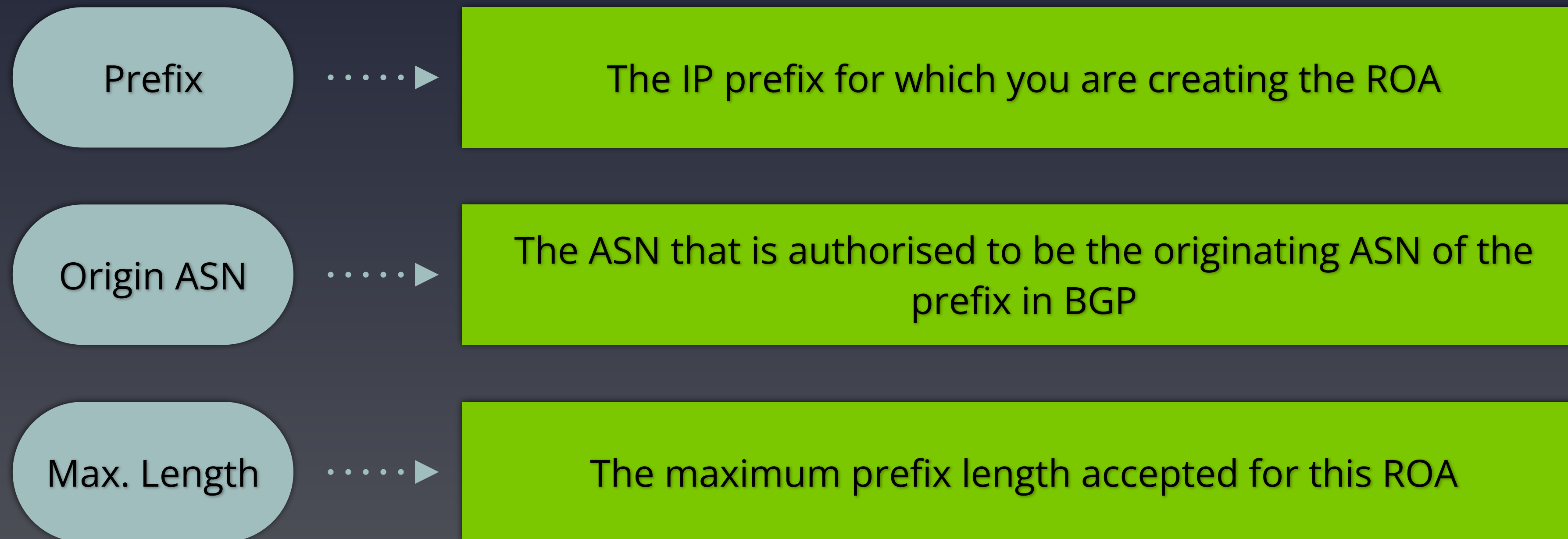
Create your ROAs

Validating

Verifying others

Signing ROAs

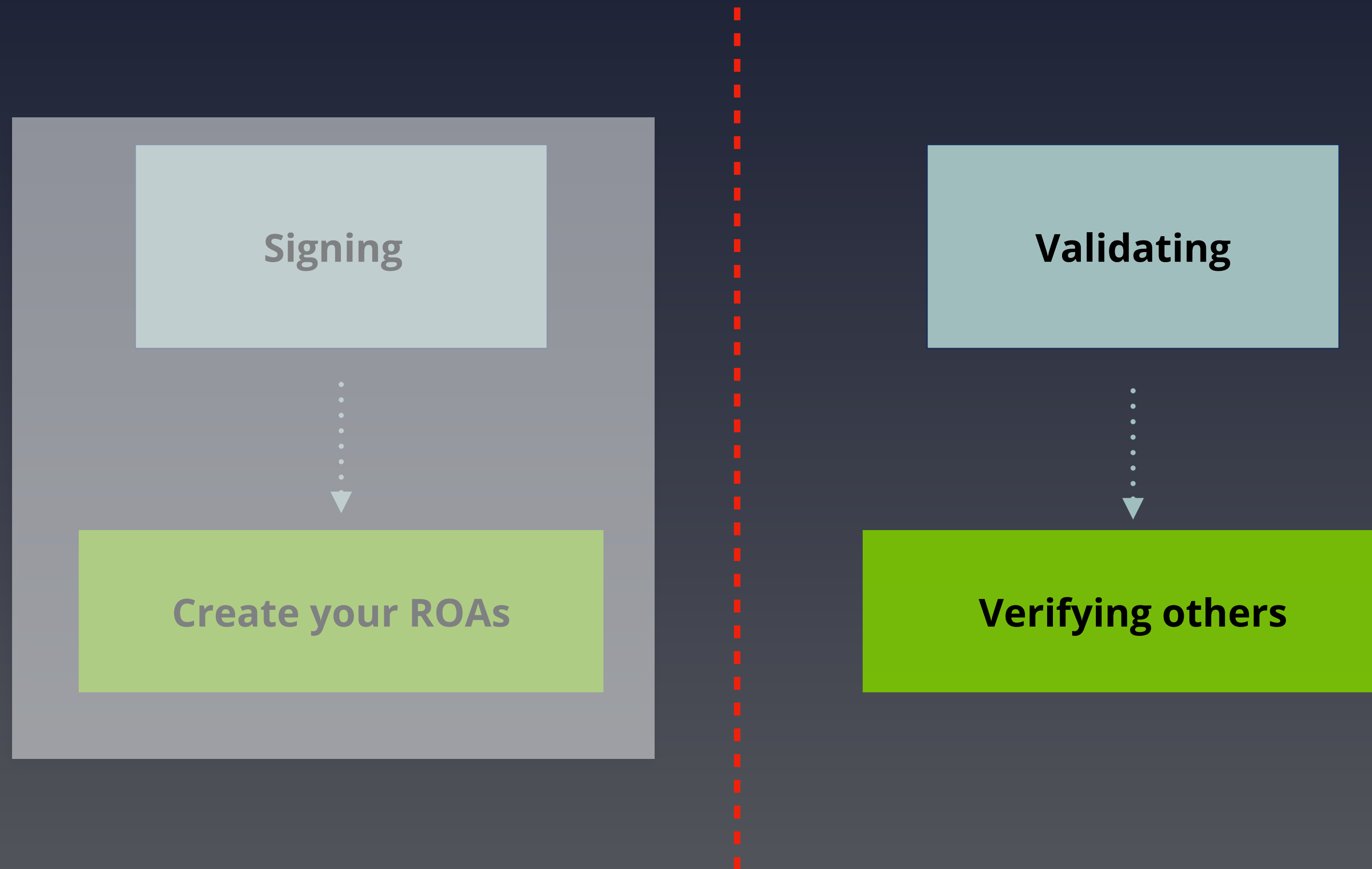# ROA (Route Origin Authorisation)

- 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 IP prefix for which you are creating the ROA

Origin ASN ······▶ The ASN that is authorised to be the originating ASN of the prefix in BGP

Max. Length ······▶ The maximum prefix length accepted for this ROA

Two elements of RPKI

Signing

Create your ROAs

Validating

Verifying others

Validating routes

Validation part 1

List of ROAs

Certificates

Repository   **Repository**   **Repository**   **Repository**   **Repository**

ARIN   **APNIC**   **RIPE NCC**   **LACNIC**   **AFRINIC**

Validator

Validation part 2

ROA

Validator

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
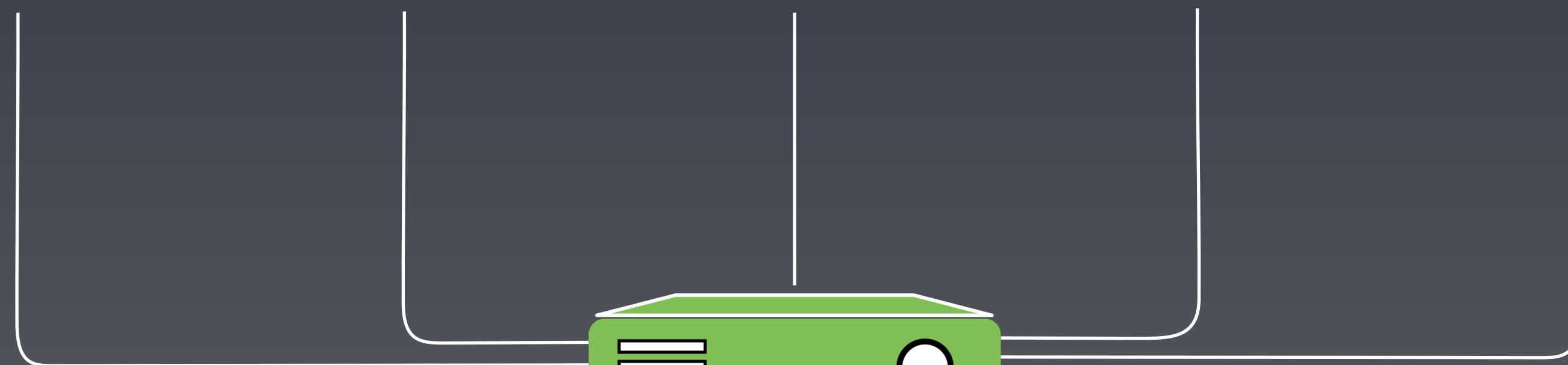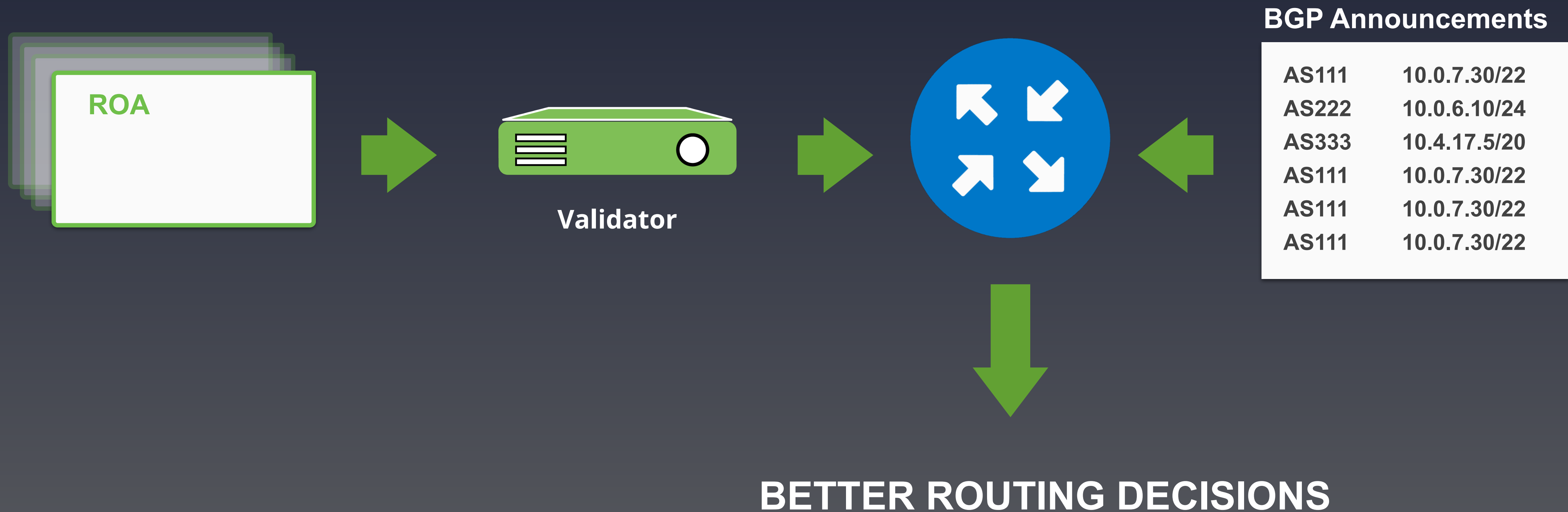
How to Get Started?

First of All...

- Read up!

- This is a great starting point:

    - https://rpki.readthedocs.io/en/latest/

- You can also take the BGP Security e-learning course at the RIPE NCC Academy

    - https://academy.ripe.net/enrol/index.php?id=15

The Easy Way

- Speak to your management/internal stakeholders

- Protect your announcements:

  - Create ROAs

  - https://my.ripe.net/#/rpki (or the relevant RIR)

The Not-So-Easy Way

- Speak to your management/internal stakeholders

- Protect your announcements:

  - Create ROAs

- Validate the data you receive from others:

  - Setup local validator, configure routers, monitoring, etc.

  - Check for INVALIDs, take a deep breath, then start rejecting INVALIDs

  - https://isbgpsafeyet.com

Questions

rpki@ripe.net
https://ripe.net/rpki