



RIPE NCC

RIPE NETWORK COORDINATION CENTRE

RPKI Signing Party

CAPIF 1 | Almaty | November 2022



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outdated or incorrect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?

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

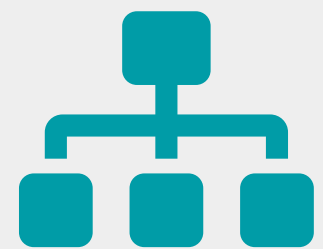




How does it work [now]?



Ties IP addresses and ASNs to public keys



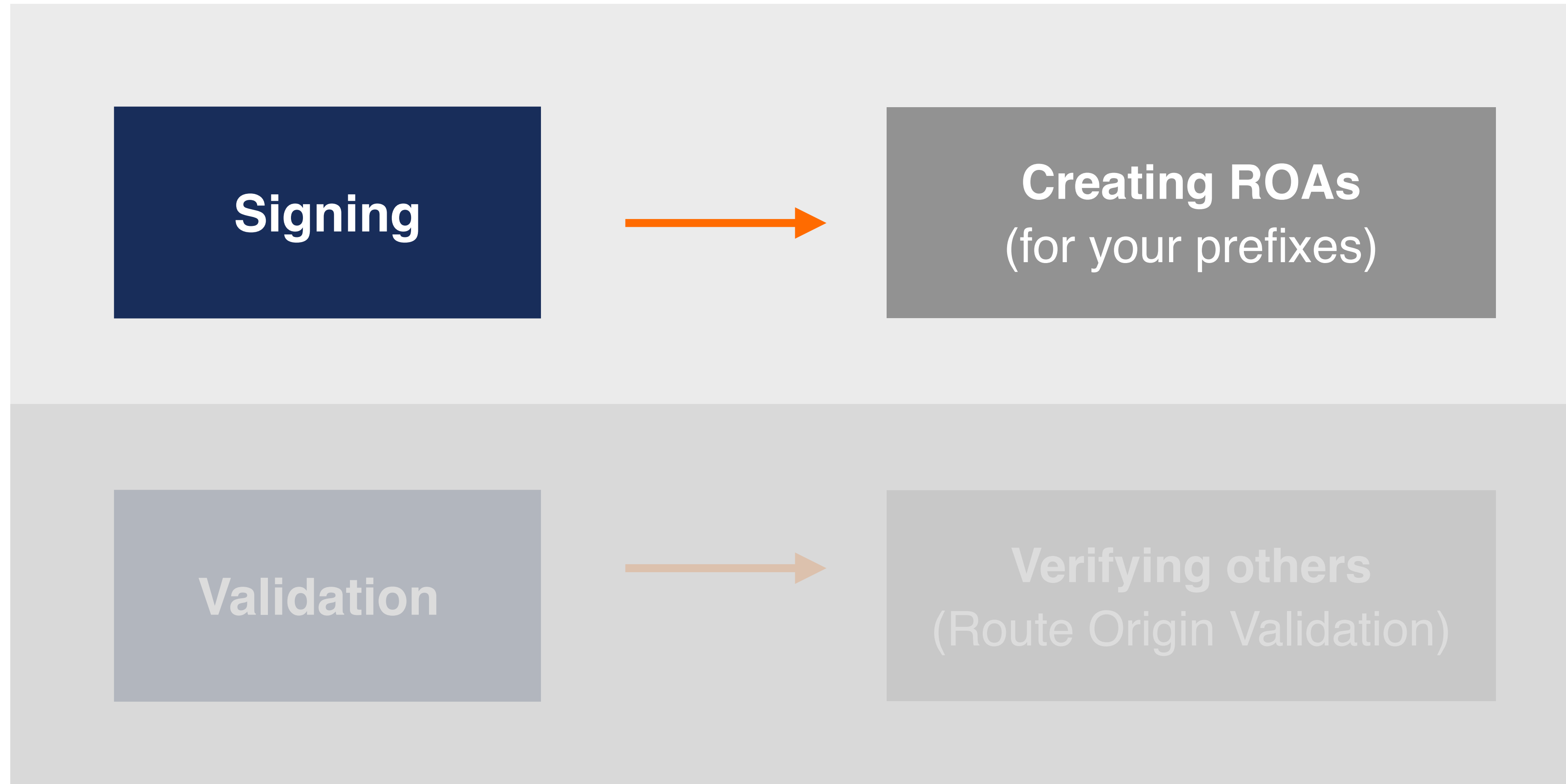
Follows the RIR hierarchy



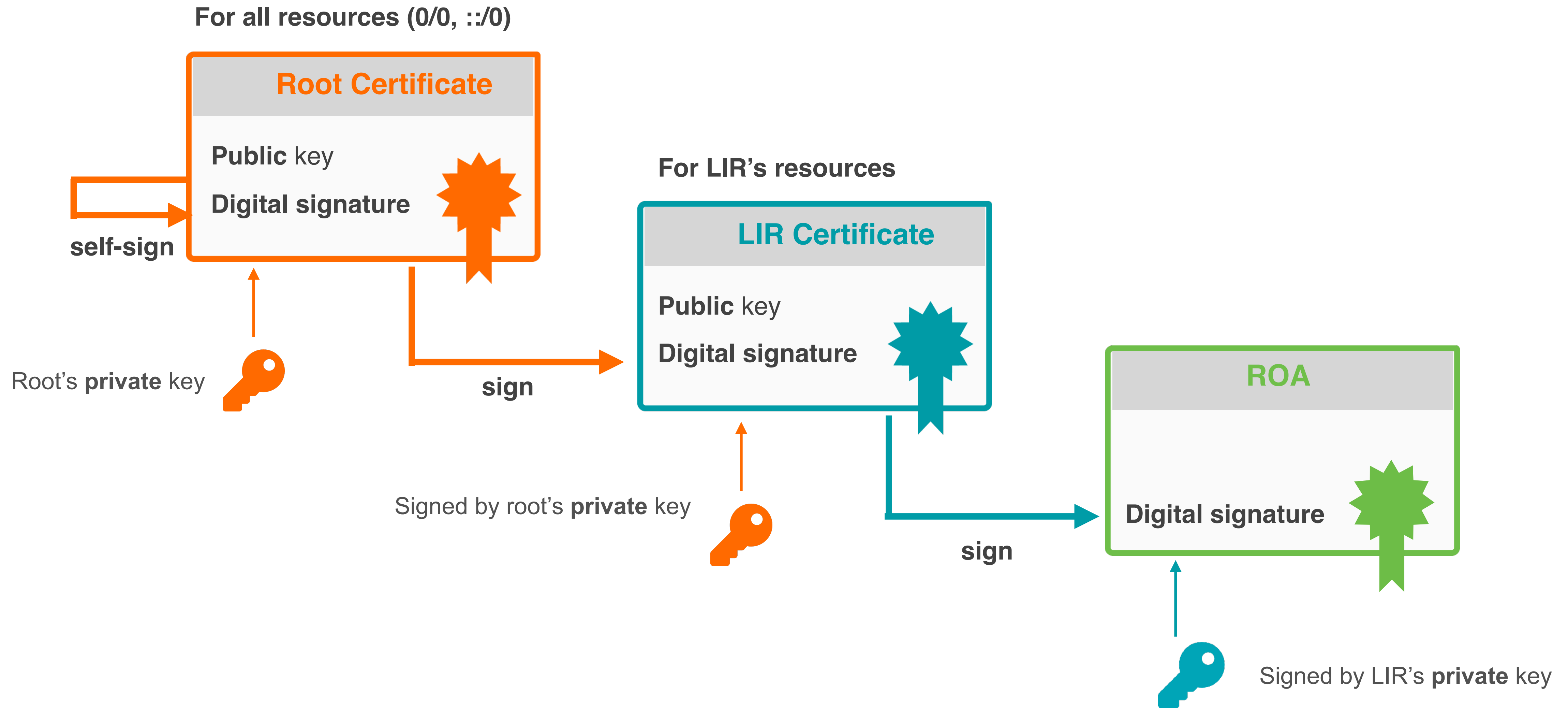
Authorised statements from resource holders

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

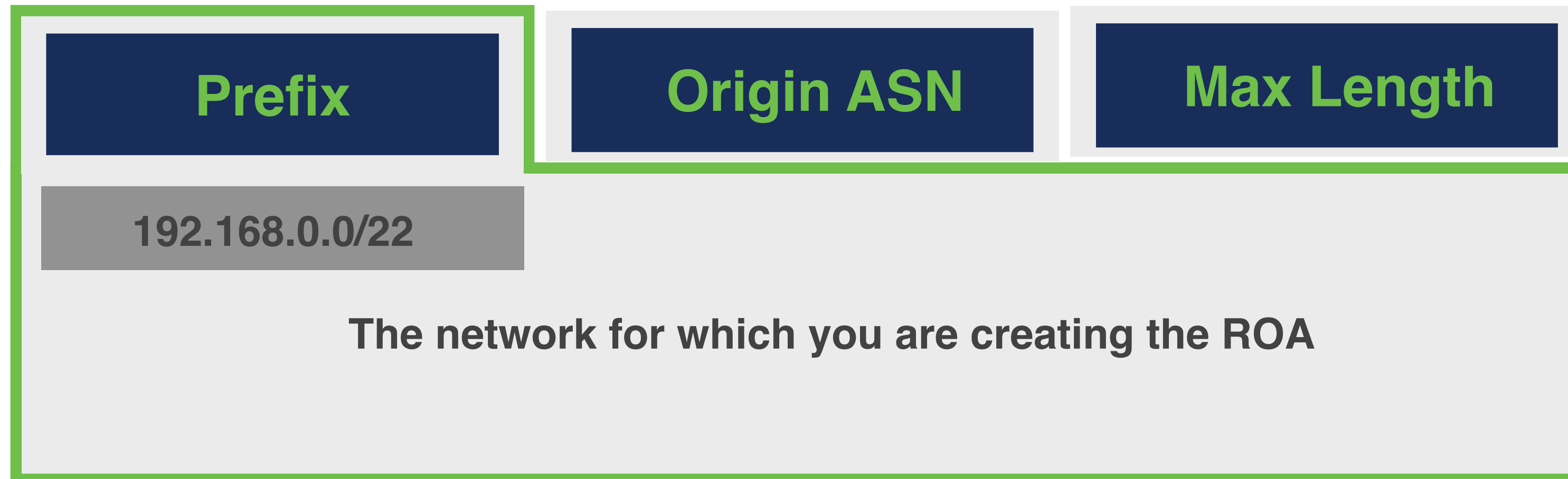
RPKI has two elements



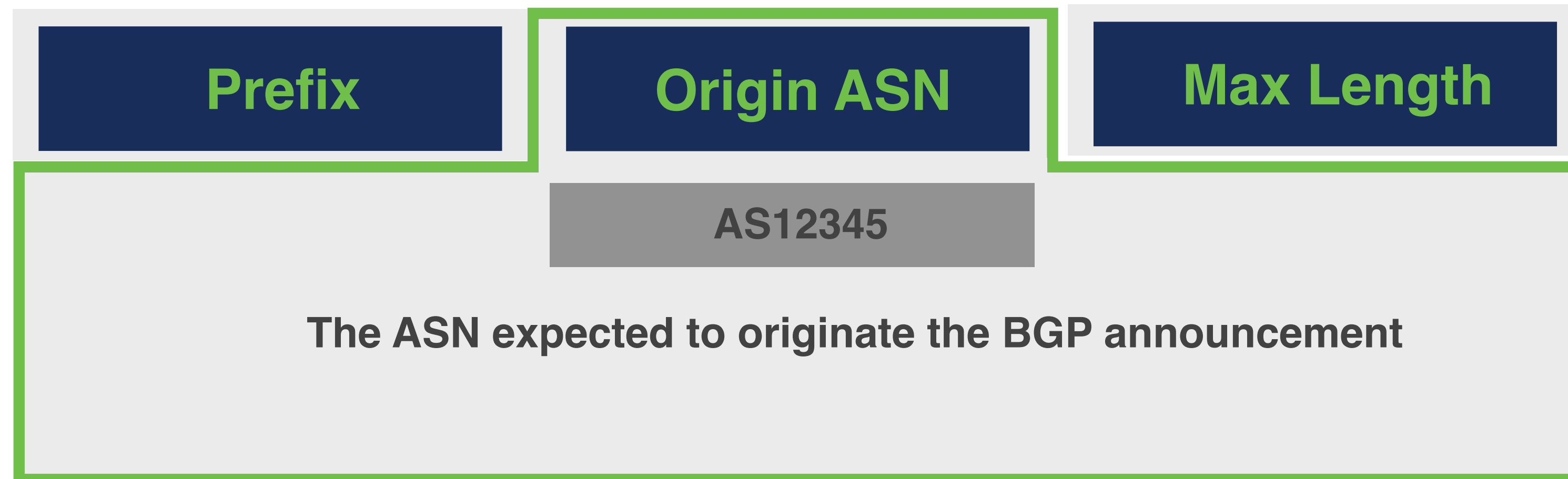
RPKI Chain of Trust



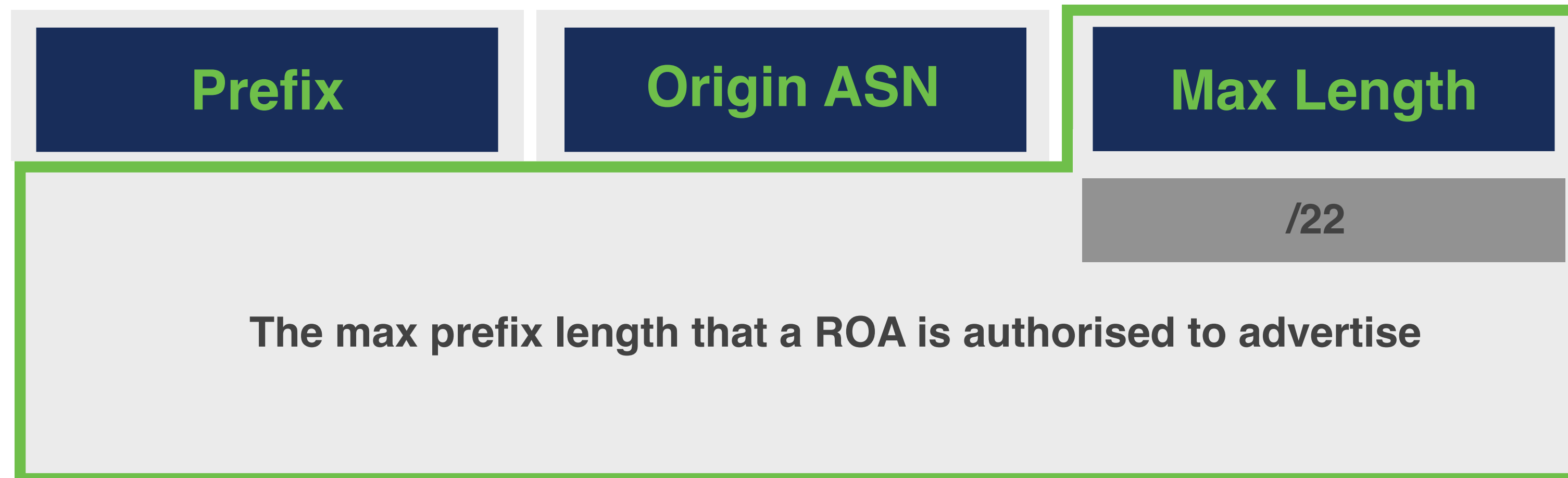
What is in a ROA?



What is in a ROA?



What is in a ROA?

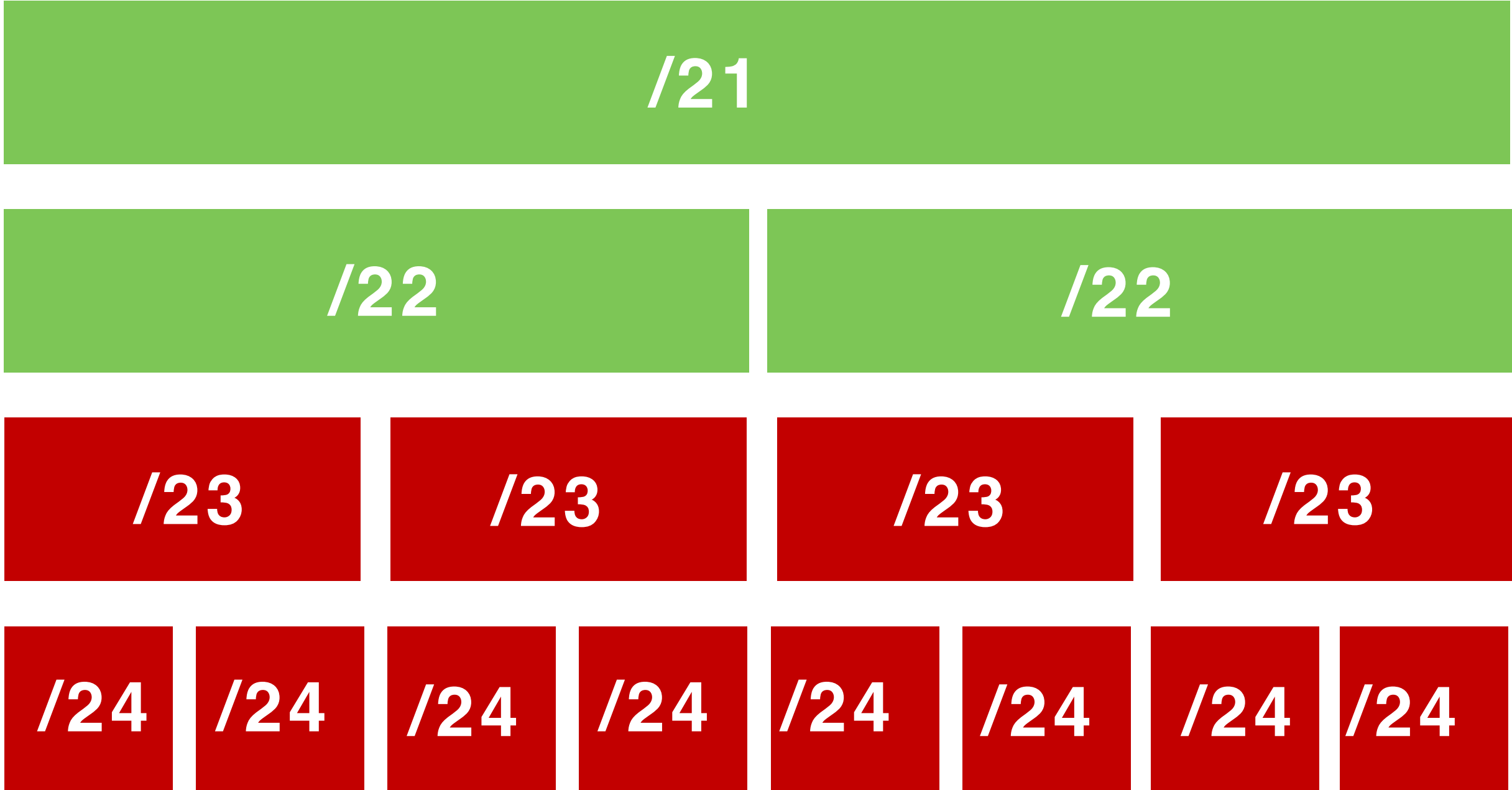


Max Length

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 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

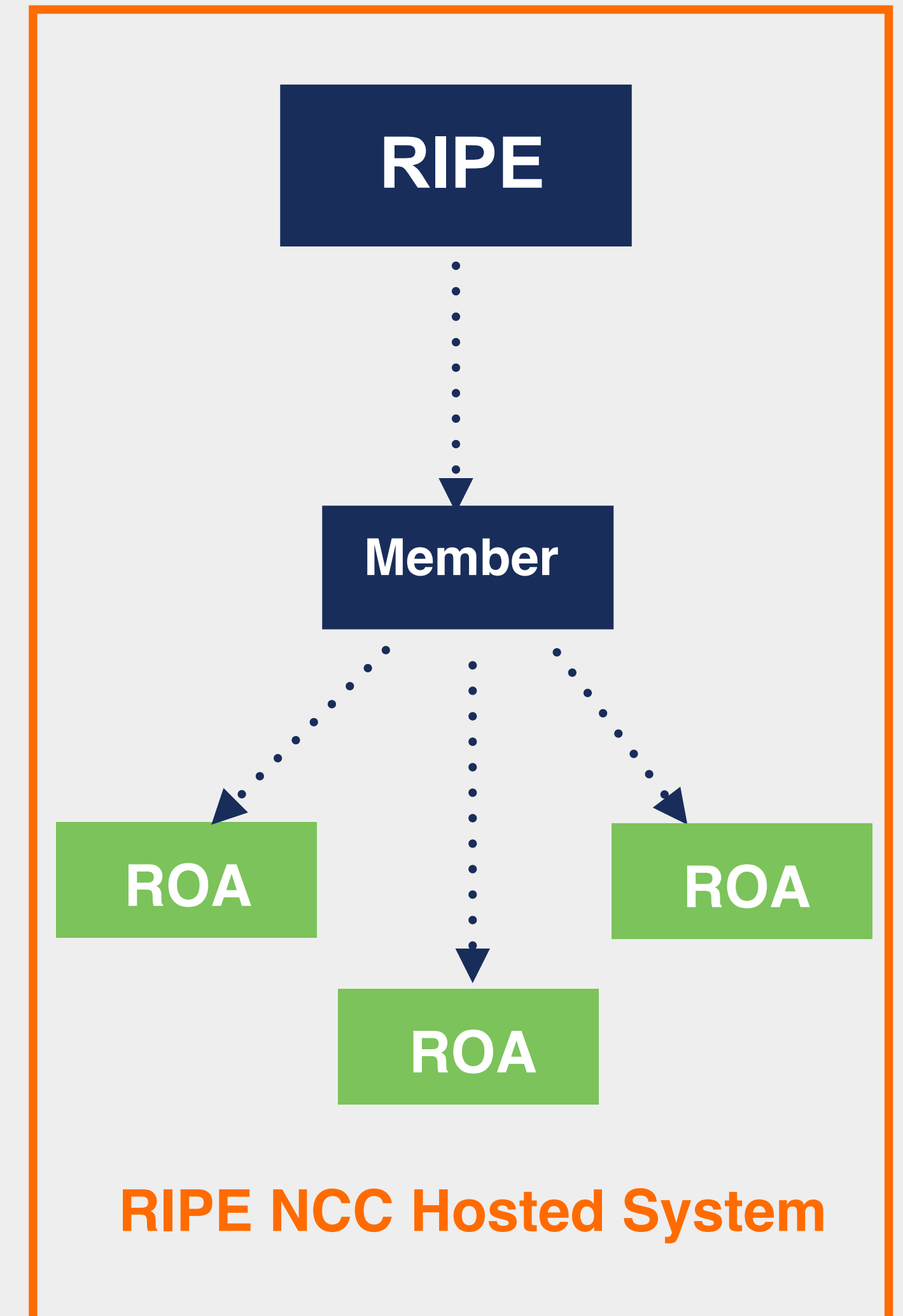
Delegated

The screenshot shows the LIR Portal navigation menu. The 'RPKI RPKI Dashboard' item is highlighted with an orange box, and an orange arrow points from it towards the right. Other menu items include 'My LIR', 'Requests', 'Resources', and 'RIPE Database'.

The screenshot shows the 'Create a Certificate Authority for bh.viacloud' page in the RPKI Dashboard. It includes the title 'RIPE NCC Certification Service Terms and Conditions', an introduction paragraph, and a section titled 'Type of Certificate Authority'. This section explains the difference between 'Hosted RPKI' and 'Delegated RPKI'. At the bottom, there are two radio button options: 'Hosted' and 'Delegated', both of which are highlighted with orange boxes. An orange arrow points from the 'Hosted' option box towards the 'Hosted' text box in the diagram above.

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



RIPE NCC 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, ROAs, manifests etc. you will need to run additional software to proceed.

- Hosted
- Delegated




RIPE NCC Hosted Solution




RPKI Dashboard 3 CERTIFIED RESOURCES ALERTS ARE SENT TO 5 ADDR





2 BGP Announcements

 2 Valid  0 Invalid  0 Unknown





2 ROAs

 2 OK  0 Causing problems

BGP Announcements **Route Origin Authorisations (ROAs)** HistorySearch...

↕ Valid Invalid Unknown

<input type="checkbox"/> Origin AS	Prefix	Current Status	
<input type="checkbox"/> AS2121	193.0.24.0/21	VALID	
<input type="checkbox"/> AS2121	2001:67c:64::/48	VALID	

Show ▾

Looking for ROA Certification for PI resources?

Revoke hosted CA

RIPE NCC Hosted Solution



RPKI Dashboard 3 CERTIFIED RESOURCES ALERTS ARE SENT TO 5 ADDR

2 BGP Announcements

✓ 2 Valid ! 0 Invalid ? 0 Unknown

2 ROAs

✓ 2 OK ! 0 Causing problems

BGP Announcements [Route Origin Authorisations \(ROAs\)](#) [History](#)

↓ Valid Invalid Unknown

<input type="checkbox"/> Origin AS	Prefix	Current Status	
<input type="checkbox"/> AS2121	193.0.24.0/21	VALID	
<input type="checkbox"/> AS2121	2001:67c:64::/48	VALID	

Show ▾

Looking for ROA Certification for PI resources?

Revoke hosted CA



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



Questions

