



RIPE NCC

RIPE NETWORK COORDINATION CENTRE

RIPE NCC Open House

Hosted vs. Delegated RPKI

Alex Band and Nathalie Trenaman | 19 March 2021





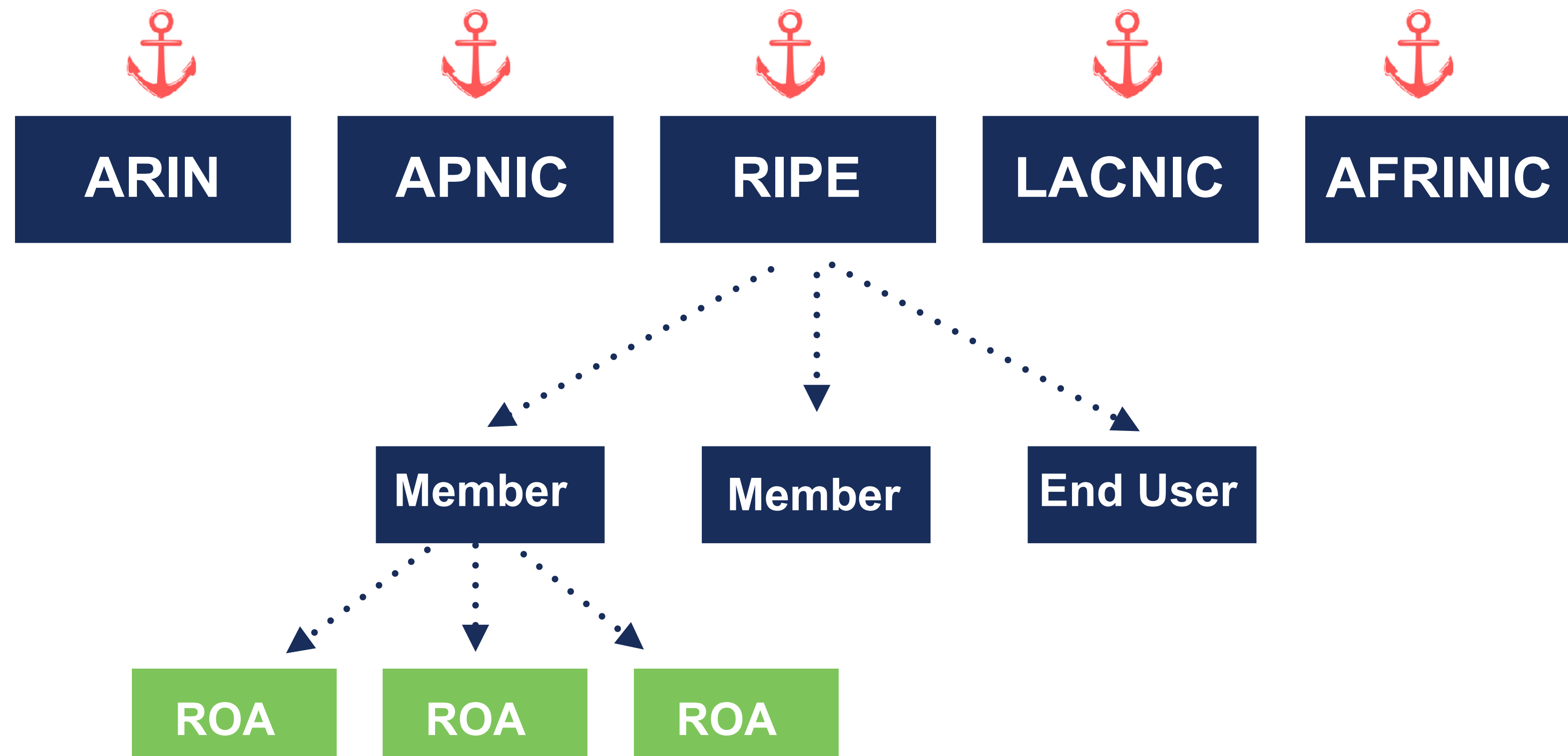
Resource Public Key Infrastructure

- 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

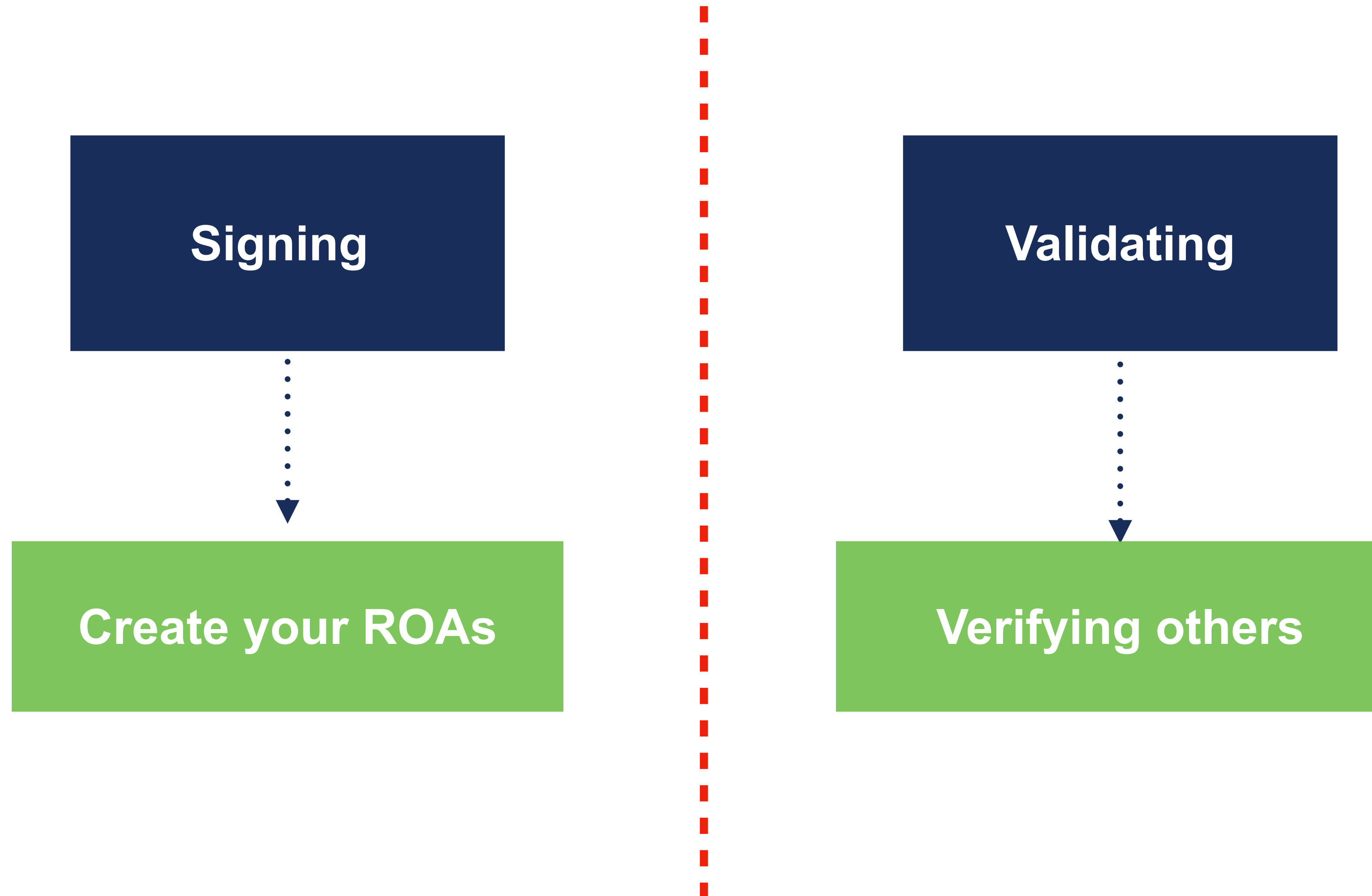
RPKI Certificate Structure



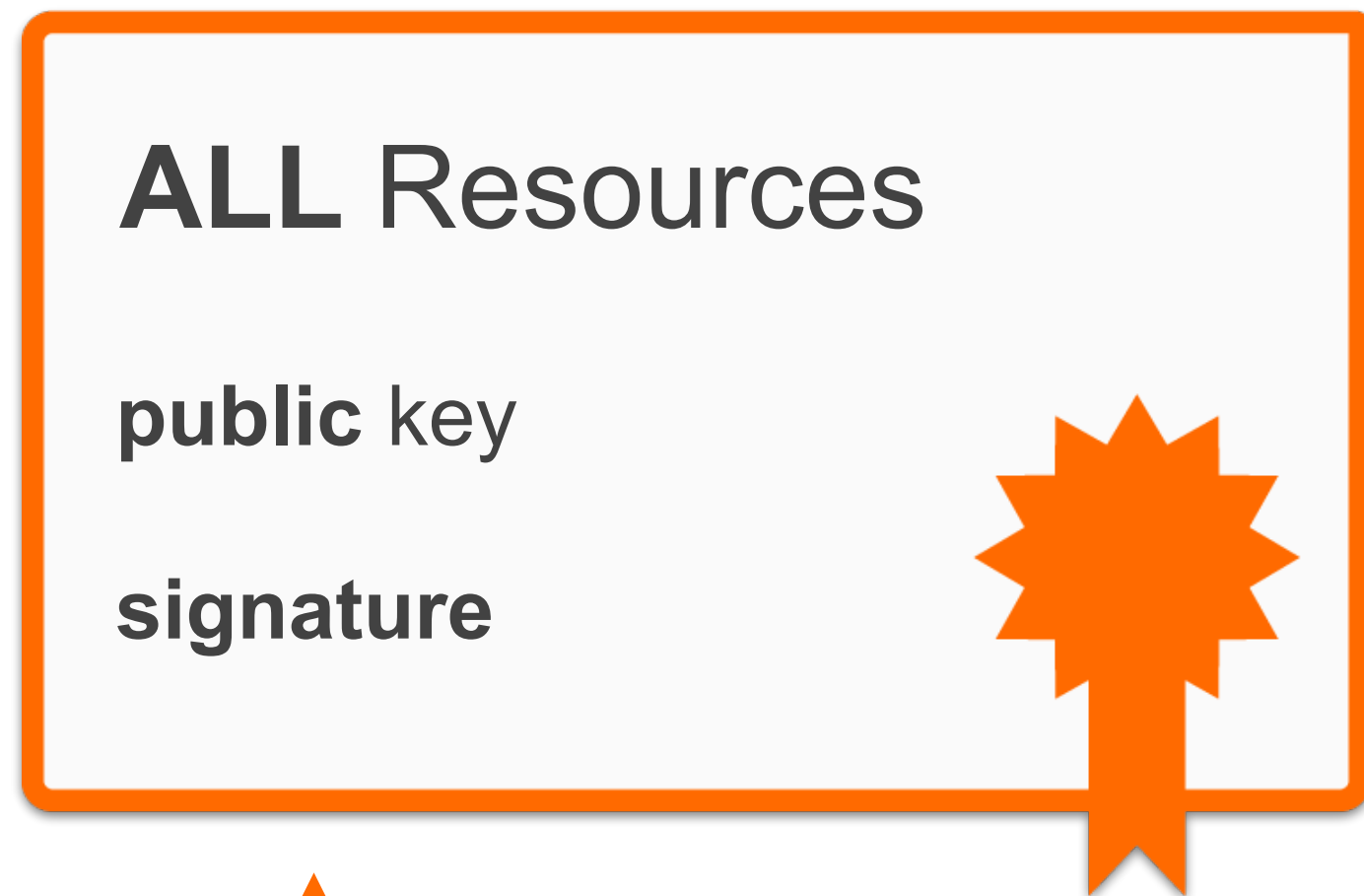
Certificate hierarchy follows allocation hierarchy



Two Elements of RPKI



RPKI Chain of Trust



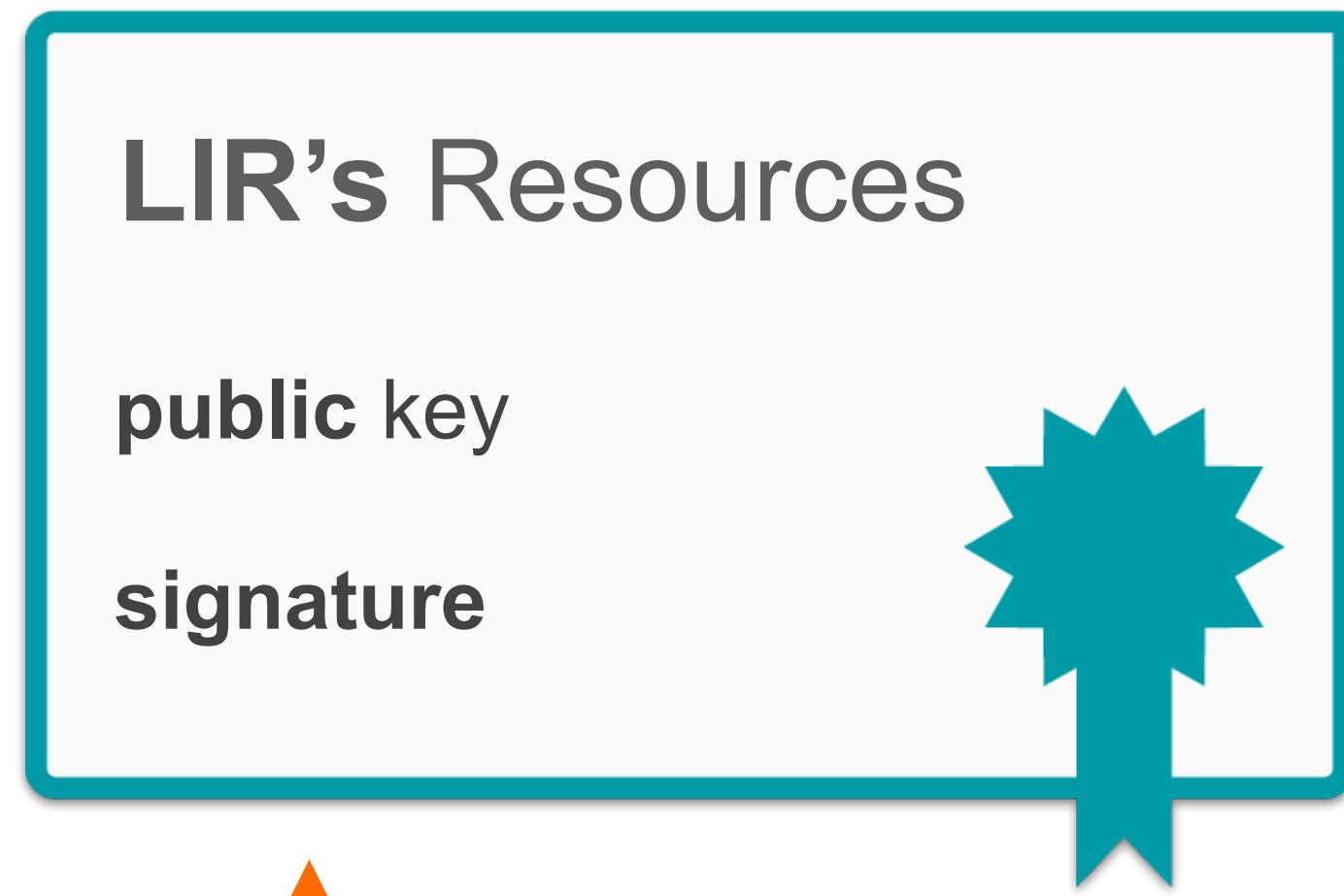
RIPE NCC Root Certificate

Self-signed



Root's **private** key

RPKI Chain of Trust



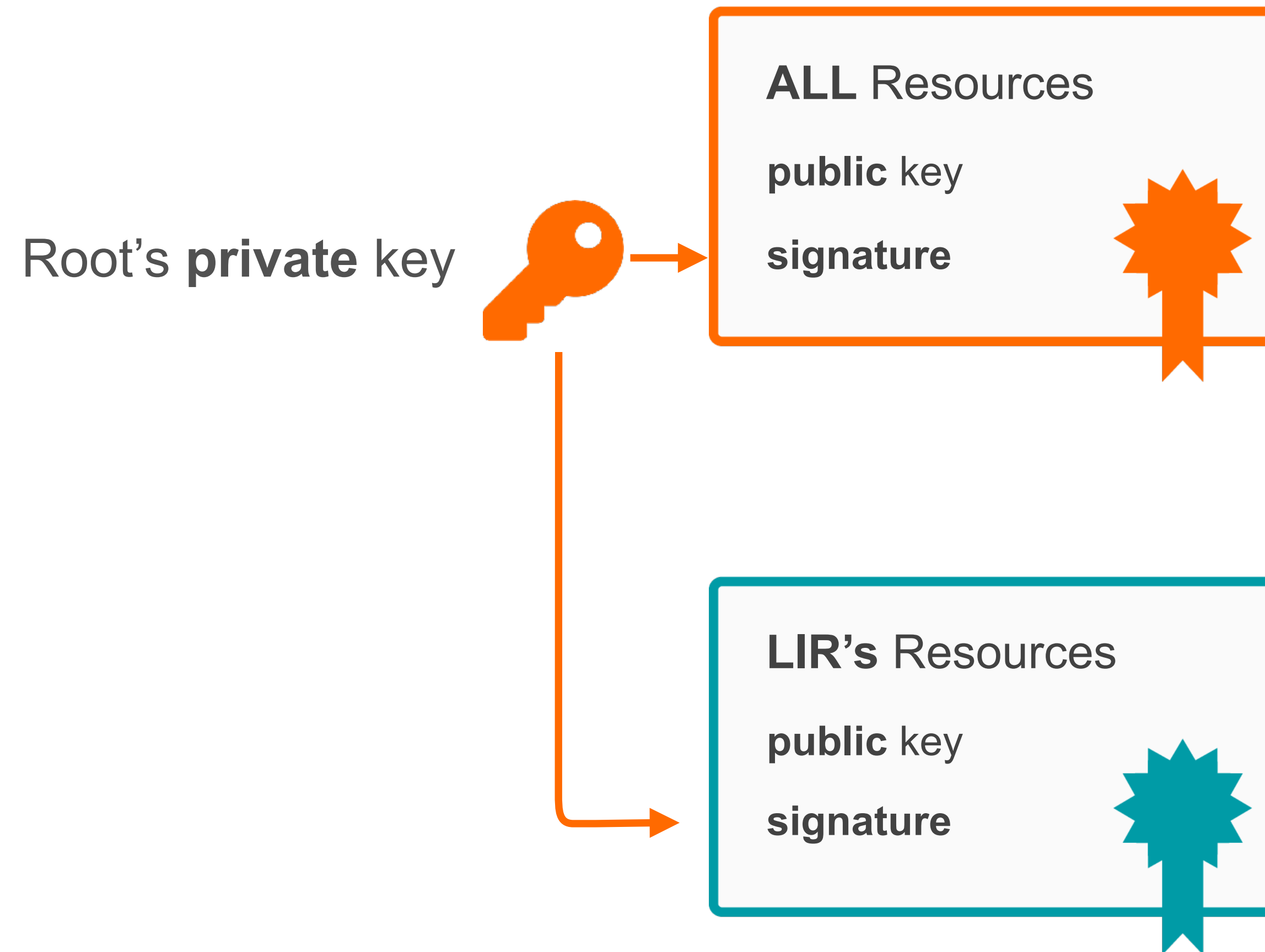
LIR Certificate

Signed by the Root private key

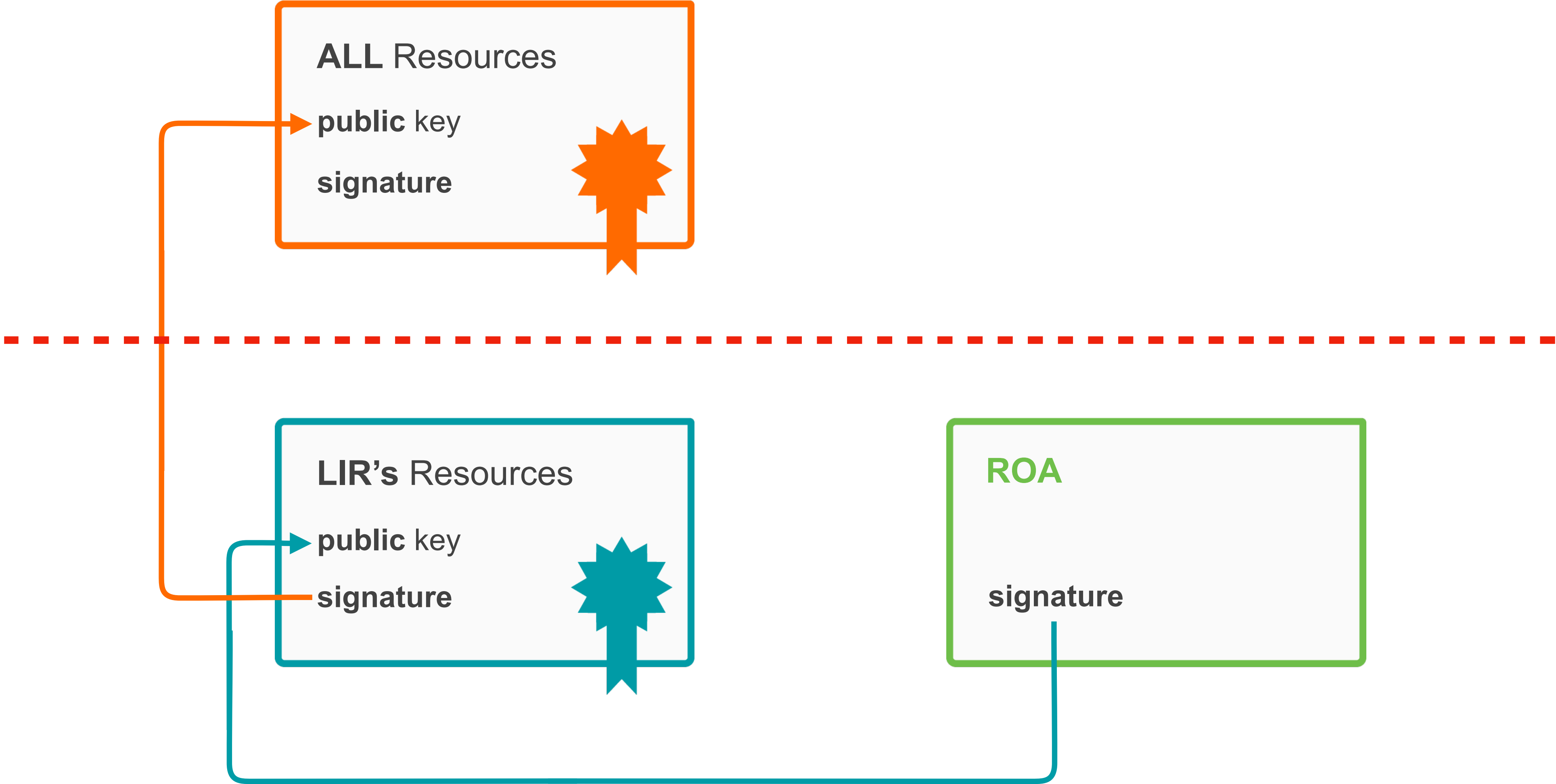


Root's private key

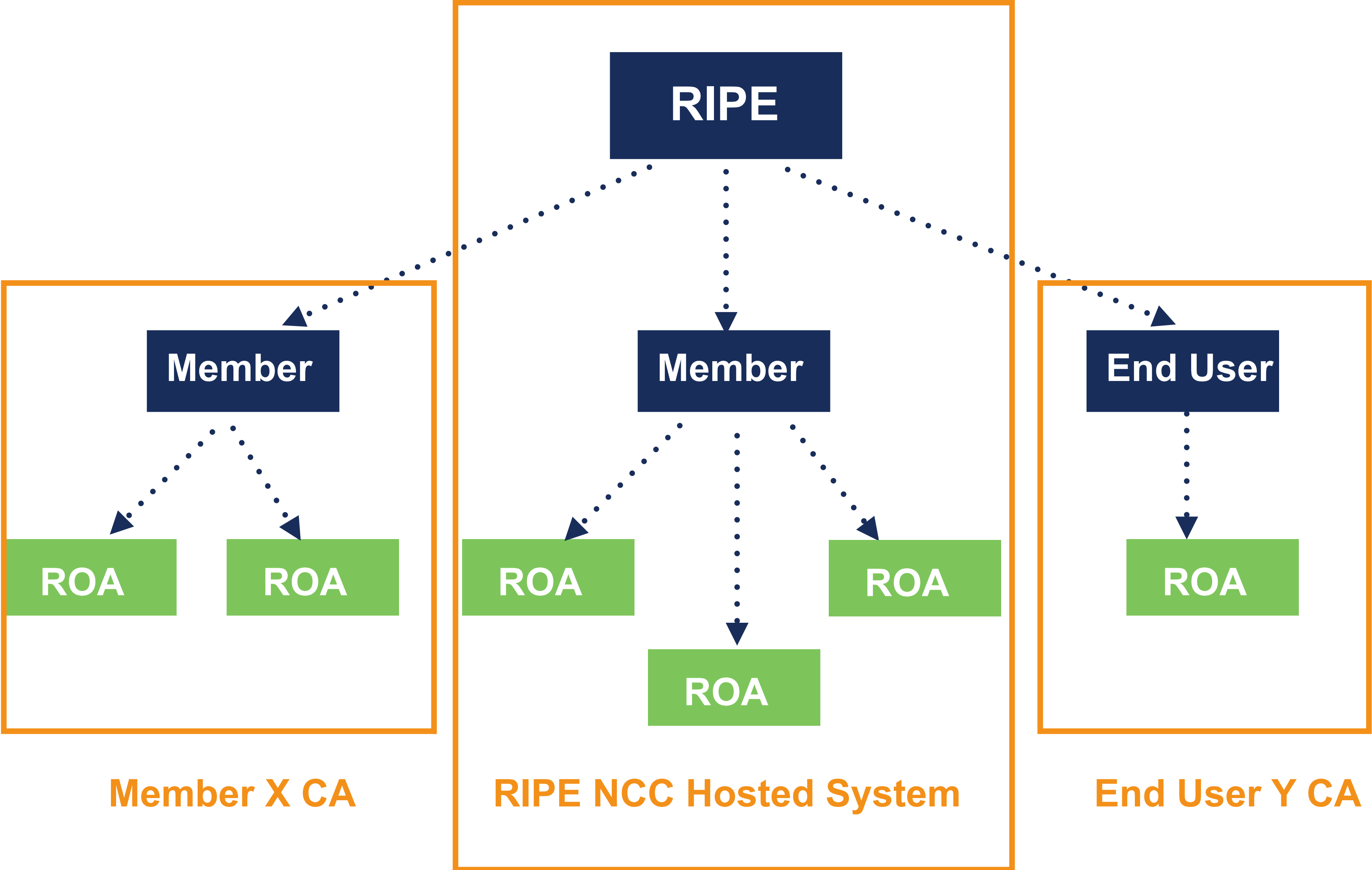
RPKI Chain of Trust



RPKI Chain of Trust



Hosted or Delegated RPKI



First Login to the 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

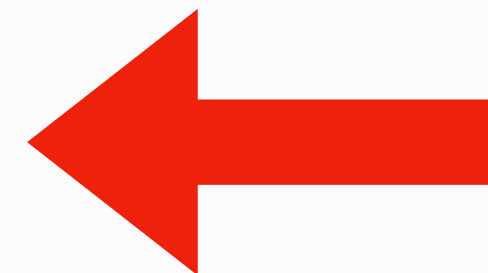
You can choose between asking the RIPE NCC to host your RPKI Certificate Authority (Hosted RPKI) or running your own Certificate Authority (Delegated RPKI).

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 and to host your own keys, ROAs, manifests etc. You will need to run additional software to proceed.

Hosted

Delegated




Hosted RPKI



- RIR hosts your Certification Authority and signs all ROAs
- Automated signing and key rollovers
- Not running your own repository
- Allows you to focus on creating and publishing ROAs
- If you have your IPs and AS numbers in one RIR
- If you don't have sub-allocations

Delegated RPKI



- Run your own Certification Authority software
 - Dragon research Labs, RPKI toolkit
 - NLNetLabs, Krill 
- Setup connection with RIPE NCC CA
- Generate your certificate and get it signed by the parent CA
- Run your own repository

RPKI Dashboard



RPKI Dashboard 3 CERTIFIED RESOURCES ALERTS ARE SENT TO 3 ADDRESSES

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 of 2 items

Certifying PI Resources



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



Sign in with your RIPE NCC Access Account

- Requested and managed by PI End User or by Sponsoring LIR
 - Complete the wizard successfully
 - Login to <https://my.ripe.net>, request a certificate
 - Manage your ROAs

“I want to revoke my CA”



- There is a button!

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

↓ Create ROAs for selected BGP Announcements | Valid | Invalid | Unknown

<input type="checkbox"/> Origin AS	Prefix	Current Status	
<input type="checkbox"/> AS8283	185.52.224.0/22	VALID	
<input type="checkbox"/> AS8283	185.52.225.0/24	VALID	
<input type="checkbox"/> AS8283	2a02:898::/32	VALID	
<input type="checkbox"/> AS8283	94.142.240.0/21	VALID	

Show 25

Looking for ROA Certification for PI resources?

Revoke hosted CA

Tour

“Are you really, really sure?”



Revoke hosted CA ×

Important

Once your hosted CA (Certificate Authority) will be revoked, **it cannot be restored**, and **all of your ROAs will be deleted**.

Please note that if you want to keep using RPKI, you will need to initialise a new hosted or non-hosted CA. We recommend that you keep a copy of your ROAs to be able to recreate them later.

When would you revoke a CA?

- You intend to switch from a hosted to a delegated CA.

Revoke CA

I want to revoke the hosted CA. I understand that I need to initialise a new CA to keep using RPKI.

I am aware that my ROAs are going to be deleted.

I am aware that alerts for conflicting announcements will no longer be sent.

I have made a backup of my ROAs (if needed).

Reg-ID

Confirmation of intention to REVOKE

Revoke



Questions



alex@nlnetlabs.nl
nathalie@ripe.net

@krillrpki