somali REN
Research & Education Network

The role of RPKI in securing routing for Research and Education Networks

Ibar Osman Ibrahim

Why Does Routing Security Matter?

A Routing Overview

The Basics: How Routing Works

There are ~70,000 core networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks.

Routers use Border Gateway Protocol (BGP) to exchange “reachability information” - networks they know how to reach.

Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path.

The Honor System: Routing Issues

Border Gateway Protocol (BGP) is based entirely on trust between networks

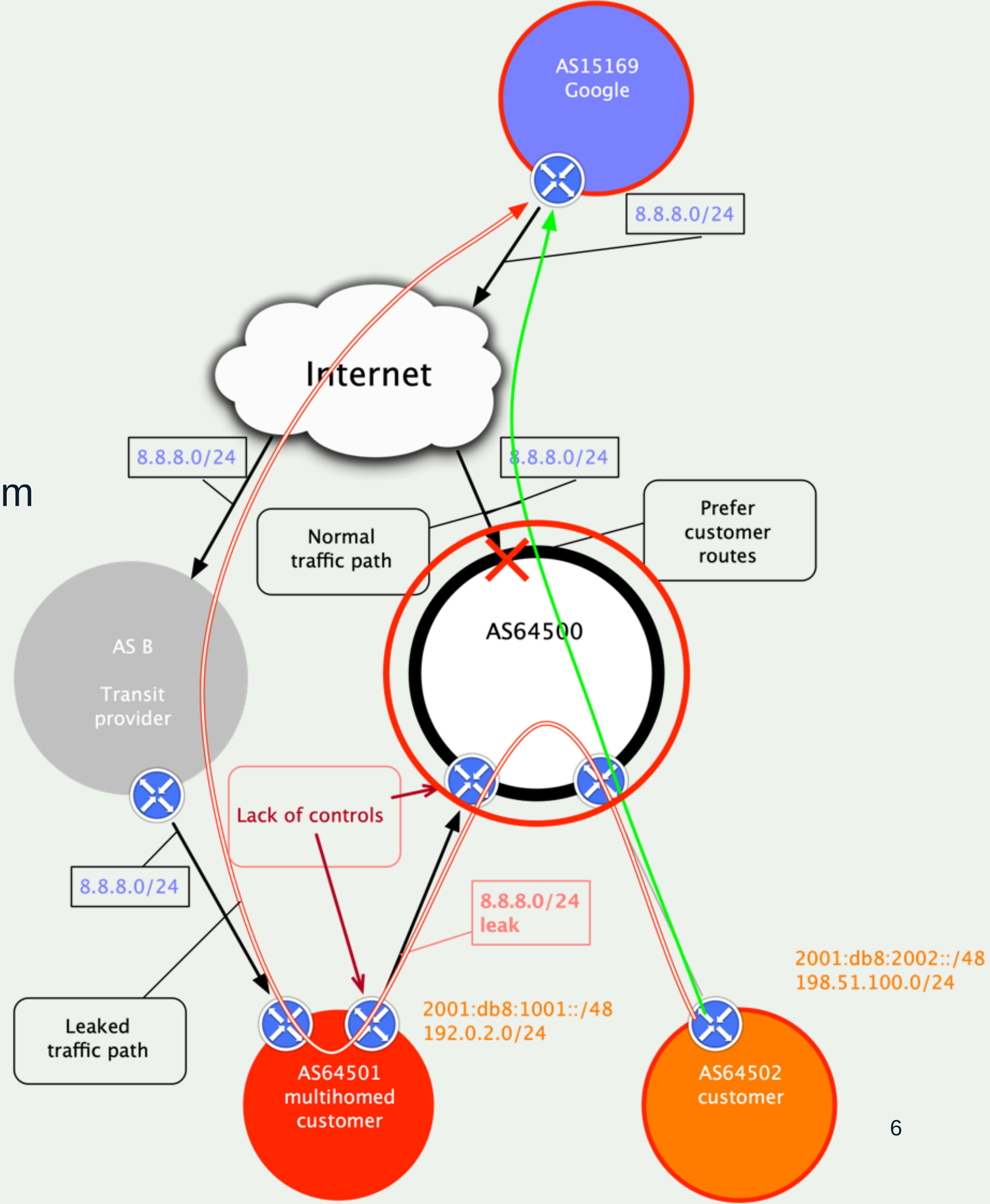
- Created before security was a concern
- Assumes all networks are trustworthy
- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data

What are Routing Incidents?

A Routing Security Overview

Route Leak

A route leak is where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that is has a route to a destination through the other upstream provider. This makes the network an intermediary network between the two upstream providers, with one sending traffic through the network to get to the other.

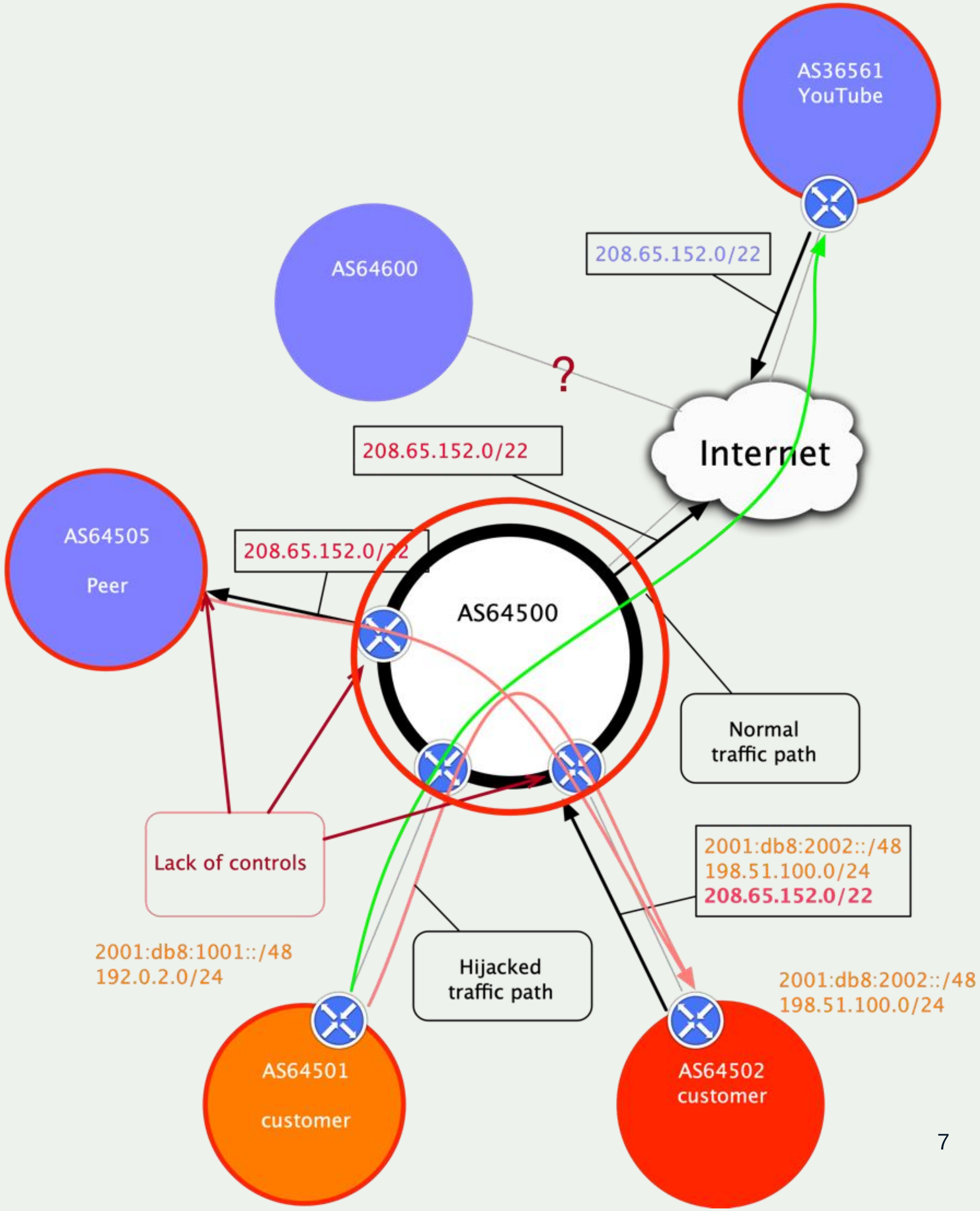


Prefix/Route Hijacking

Route hijacking, also known as “BGP hijacking,” is when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretends that a server or network is their client. This routes traffic to the wrong network operator, when another real route is available.

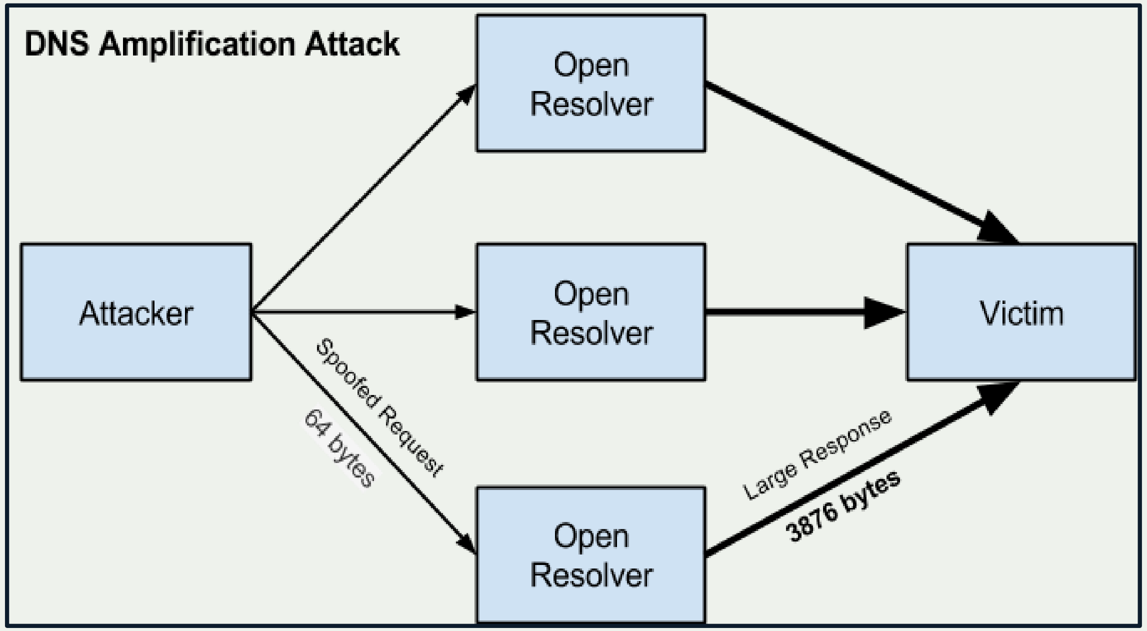
Example: The 2008 YouTube hijack; an attempt to block YouTube through route hijacking led to much of the traffic to YouTube being dropped around the world.

Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting false announcements).



IP Address Spoofing

IP address spoofing is used to hide the true identity of a server or to impersonate another server. This technique can be used to amplify an attack.



We Are In This Together

Network operators have a responsibility to ensure a globally robust and secure routing infrastructure.

Your network’s safety depends on a routing infrastructure that weeds out bad actors and accidental misconfigurations that wreak havoc on the Internet.

The more network operators work together, the fewer incidents there will be, and the less damage they can do.

The RPKI

What is RPKI ?

Resource **P**ublic **K**ey **I**nfrastructure:

❑ Specialized PKI framework: to secure the Internet’s routing infrastructure

❑ Cryptographic method of signing records that associate a BGP announcement with the correct originating ASN.

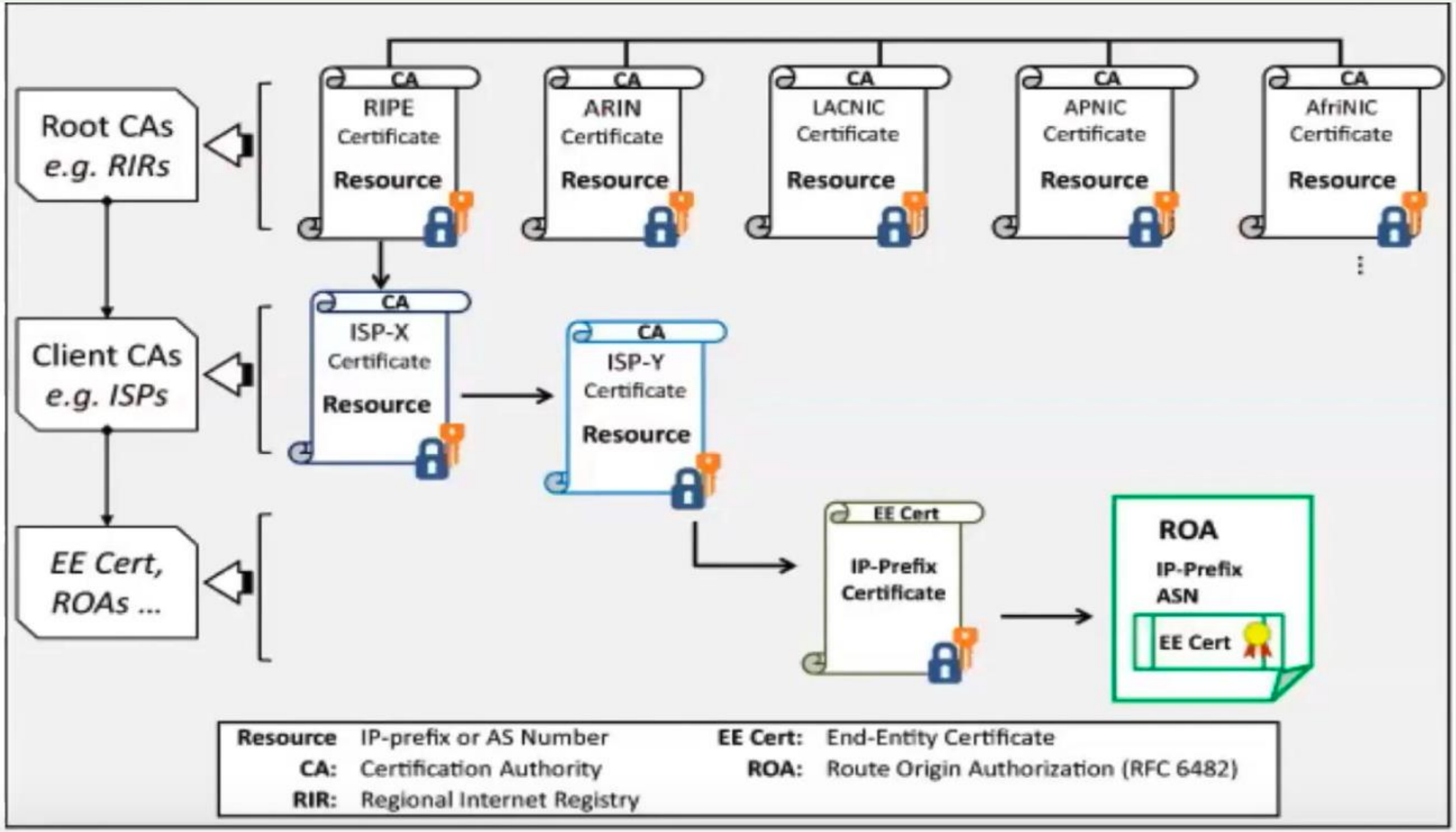
RPKI Objective

- ❑ Prove the right to use resource
- ❑ Sign Route Origin Authorizations (ROAs)
- ❑ Sign Internet Routing Objects
- ❑ Prove ownership of Internet number resource
- ❑ Secure inter-domain routing protocol by conveying the right-to-use of the resources and to validate routing information

RPKI overview

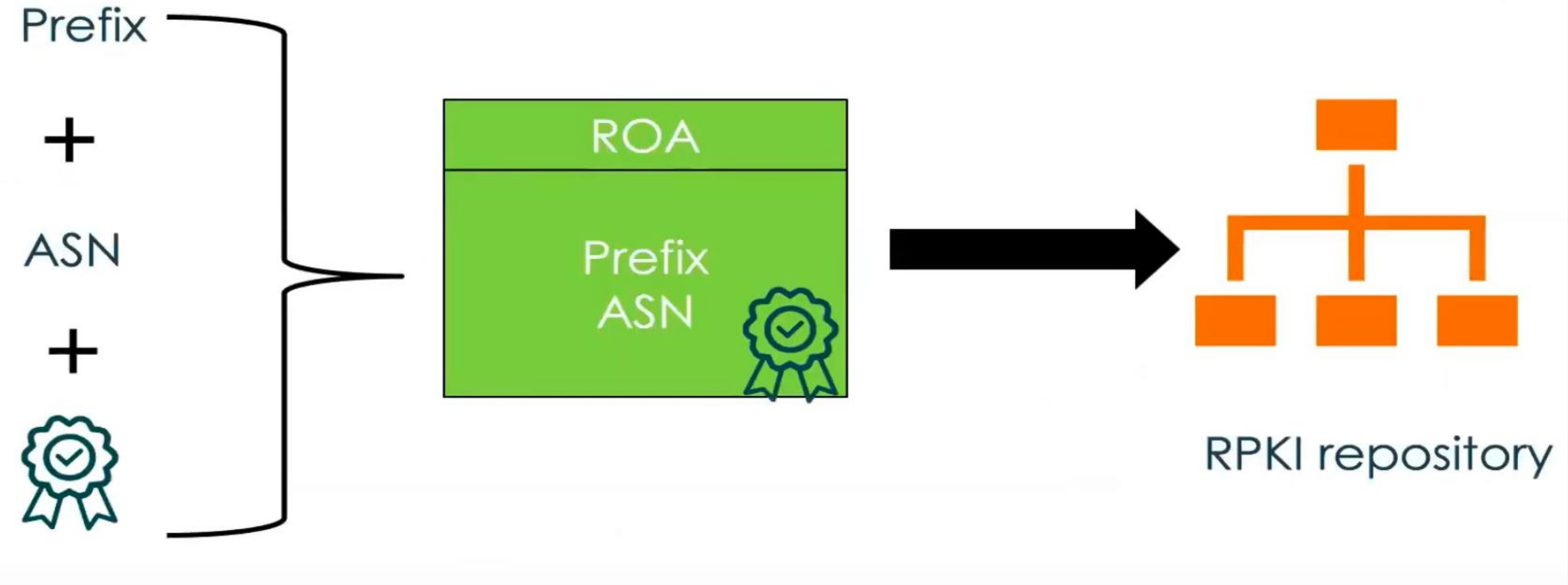
Component	Description
PKI	- CA Certificates - End-entity Certificates - Trust anchors
ROAs	Digital signed object
Repository	Store signed objects and make them available to download
Manifest	Signed object listing of all the signed objects issued by an authority responsible for a publication in the repository system
Local cache maintenance	Local copy of any relaying party

How it works

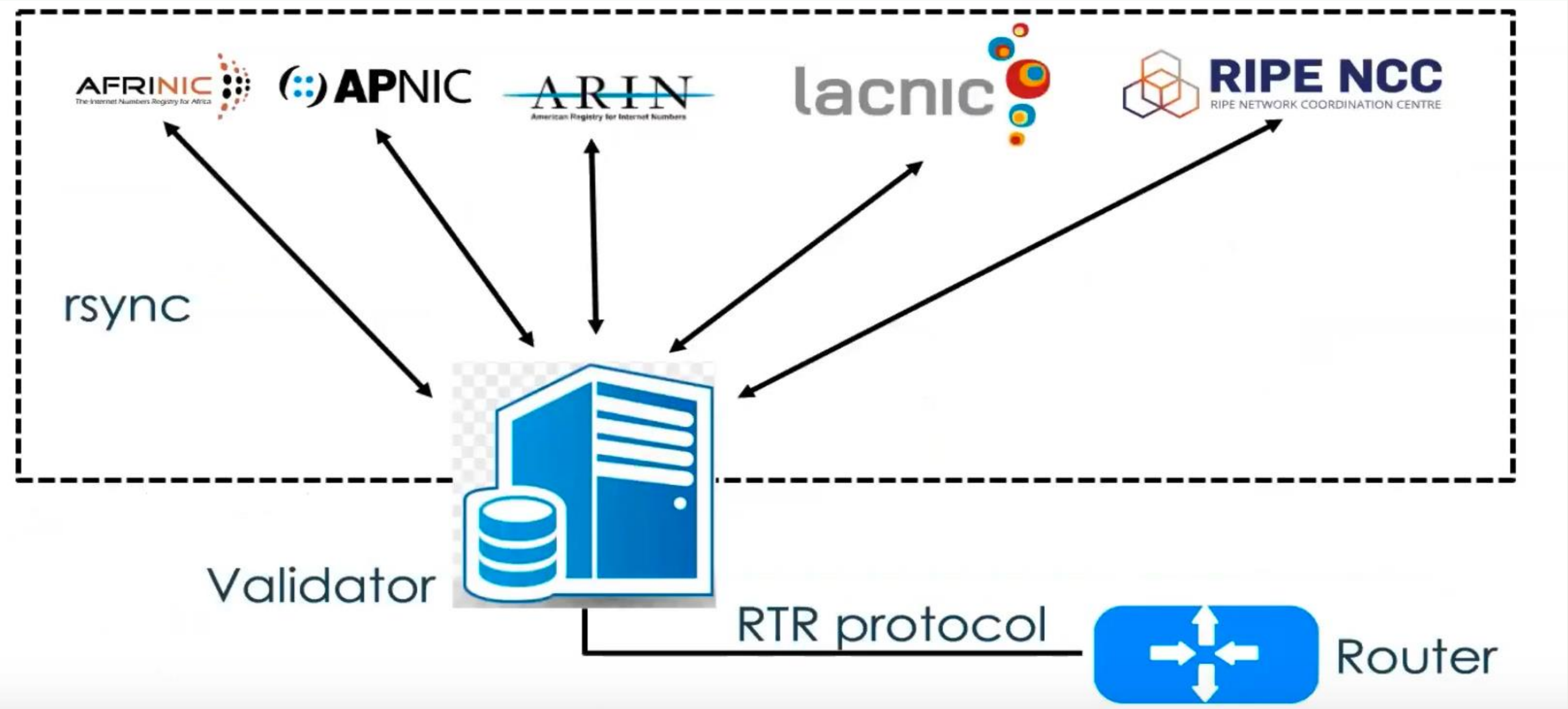


Resource	IP-prefix or AS Number	**EE Cert:**	End-Entity Certificate
CA:	Certification Authority	**ROA:**	Route Origin Authorization (RFC 6482)
RIR:	Regional Internet Registry		

How it works



How it works

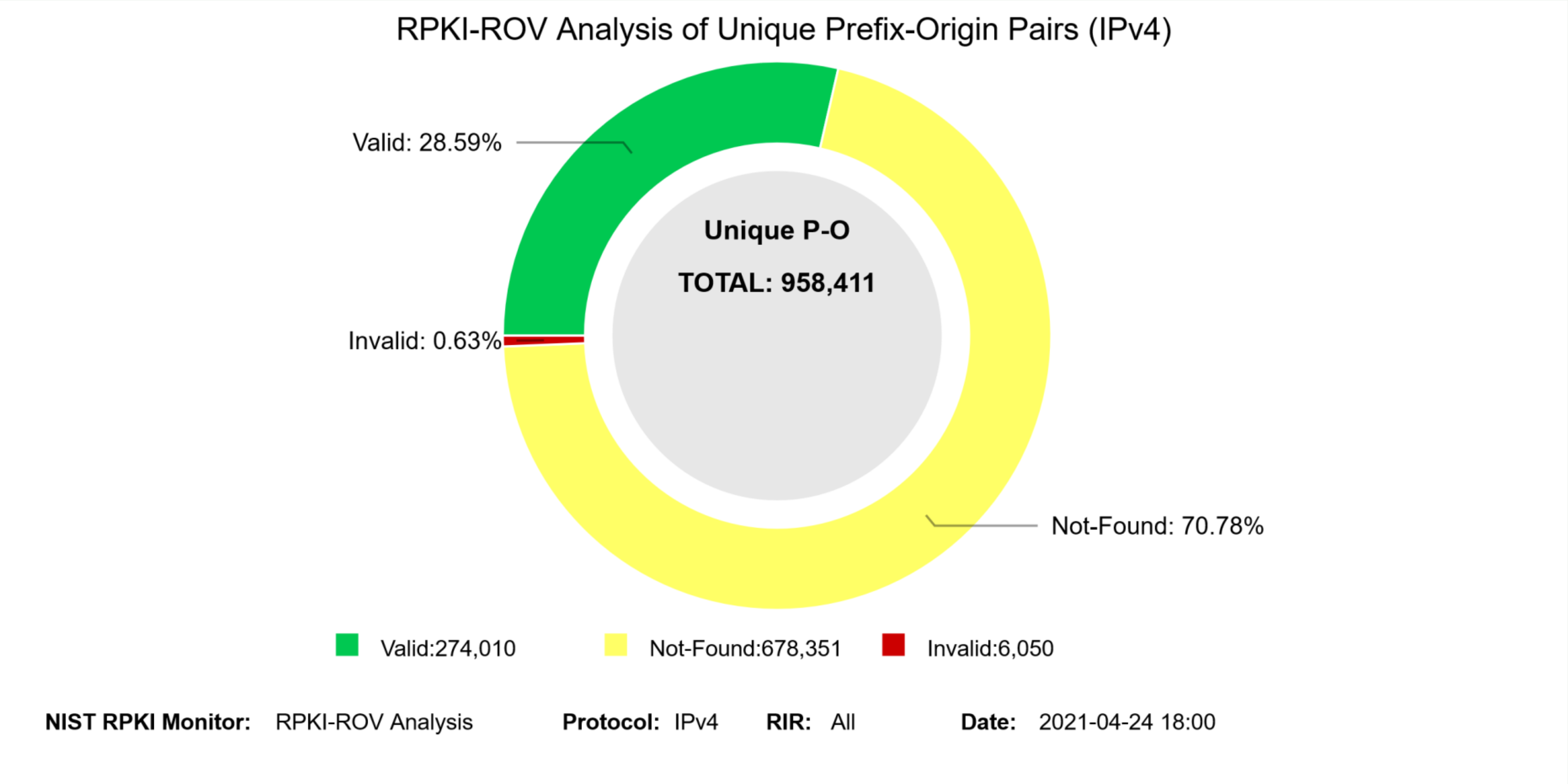

AFRINIC
The Internet Numbers Registry for Africa
APNIC
ARIN
American Registry for Internet Numbers
lacnic
RIPE NCC
RIPE NETWORK COORDINATION CENTRE
rsync
Validator
RTR protocol
Router

Benefits

- ❑ Establish a model of trust
- ❑ Every of part of the network can check the correctness of objects
- ❑ You don’t relay only from your peers/upstream to check the eligibility of routes

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

RPKI-ROV Analysis: Global Analysis

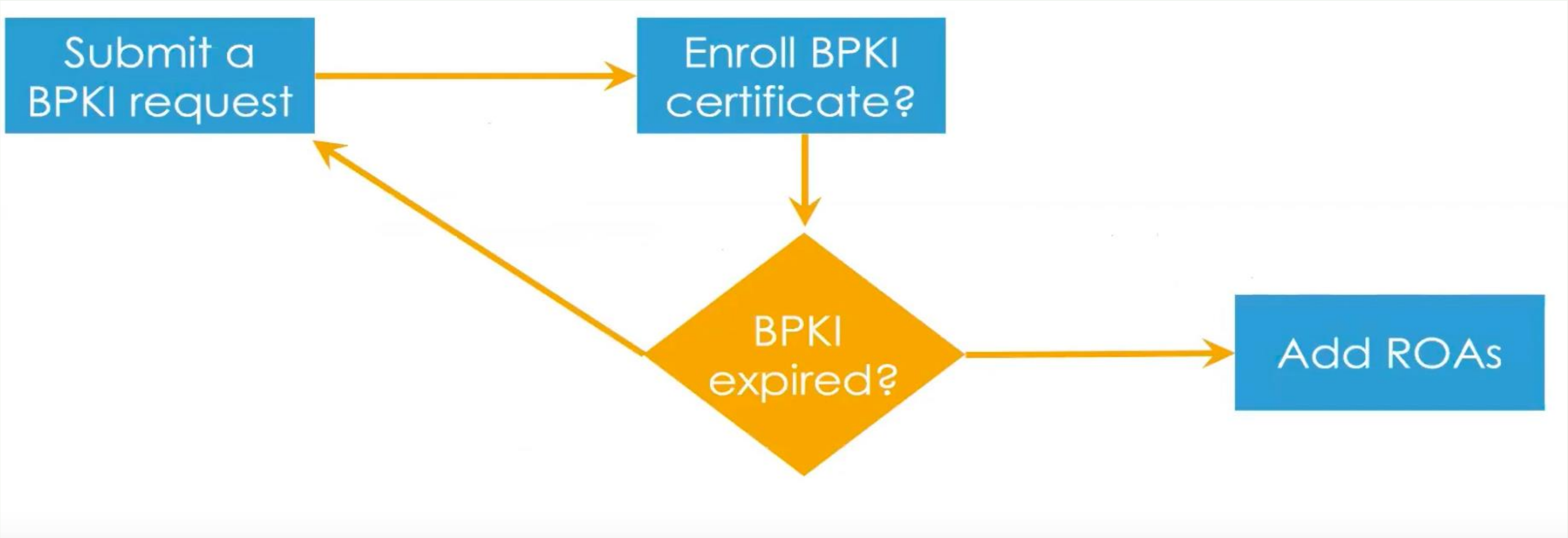


RPKI-ROV Analysis of Unique Prefix-Origin Pairs (IPv4)

NIST RPKI Monitor: RPKI-ROV Analysis **Protocol:** IPv4 **RIR:** All **Date:** 2021-04-24 18:00

Using the AFRINIC RPKI

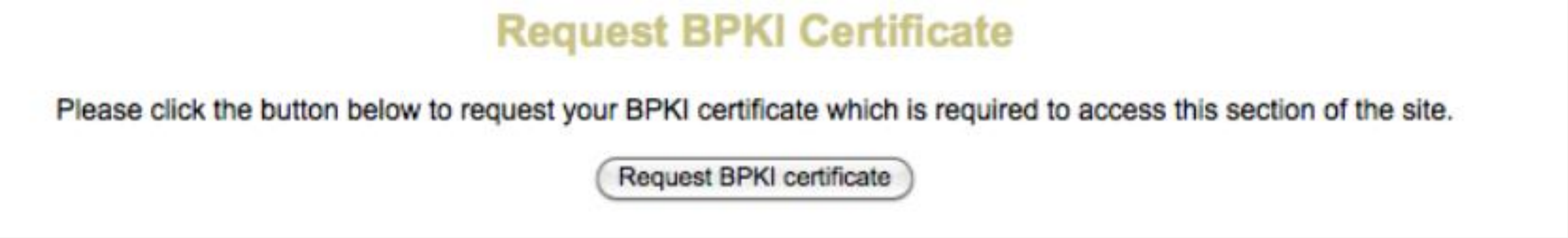
Object creating process



Submit BPKI request

❑ **Admin contact:** Send ID information to service-support@afrinic.net

❑ **No-admin contact:** use the interface to request authorization by admin-contact

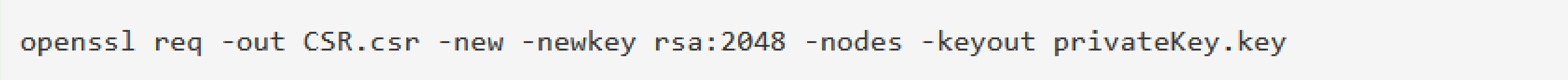


Request BPKI Certificate

Please click the button below to request your BPKI certificate which is required to access this section of the site.

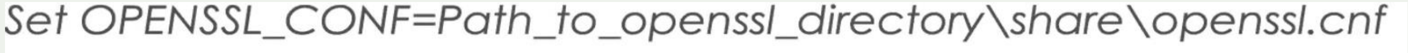
Enroll BPKI certificate

- ❑ Generating certificate



```
openssl req -out CSR.csr -new -newkey rsa:2048 -nodes -keyout privateKey.key
```

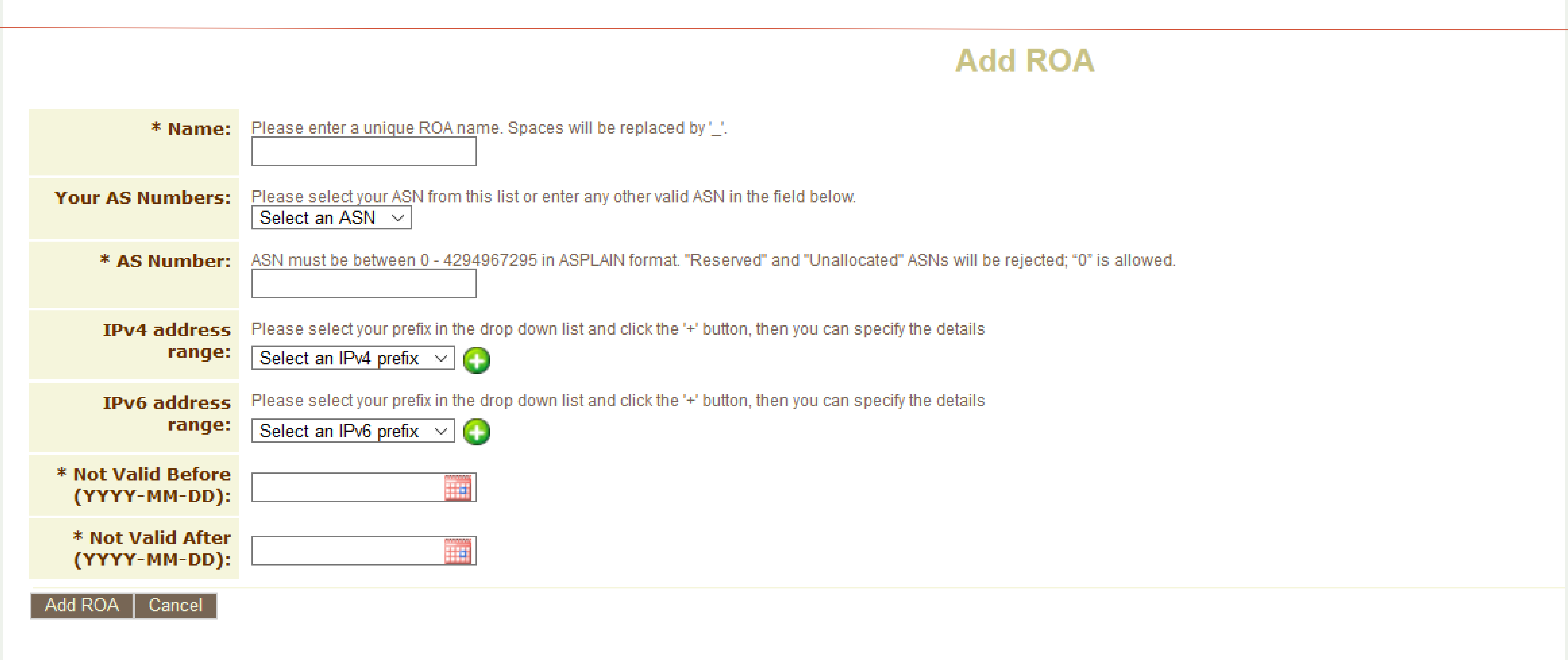
Note Windows users should specify openssl config



```
Set OPENSSL_CONF=Path_to_openssl_directory\share\openssl.cnf
```

- ❑ Enroll the certificate in the browser

Create ROAs



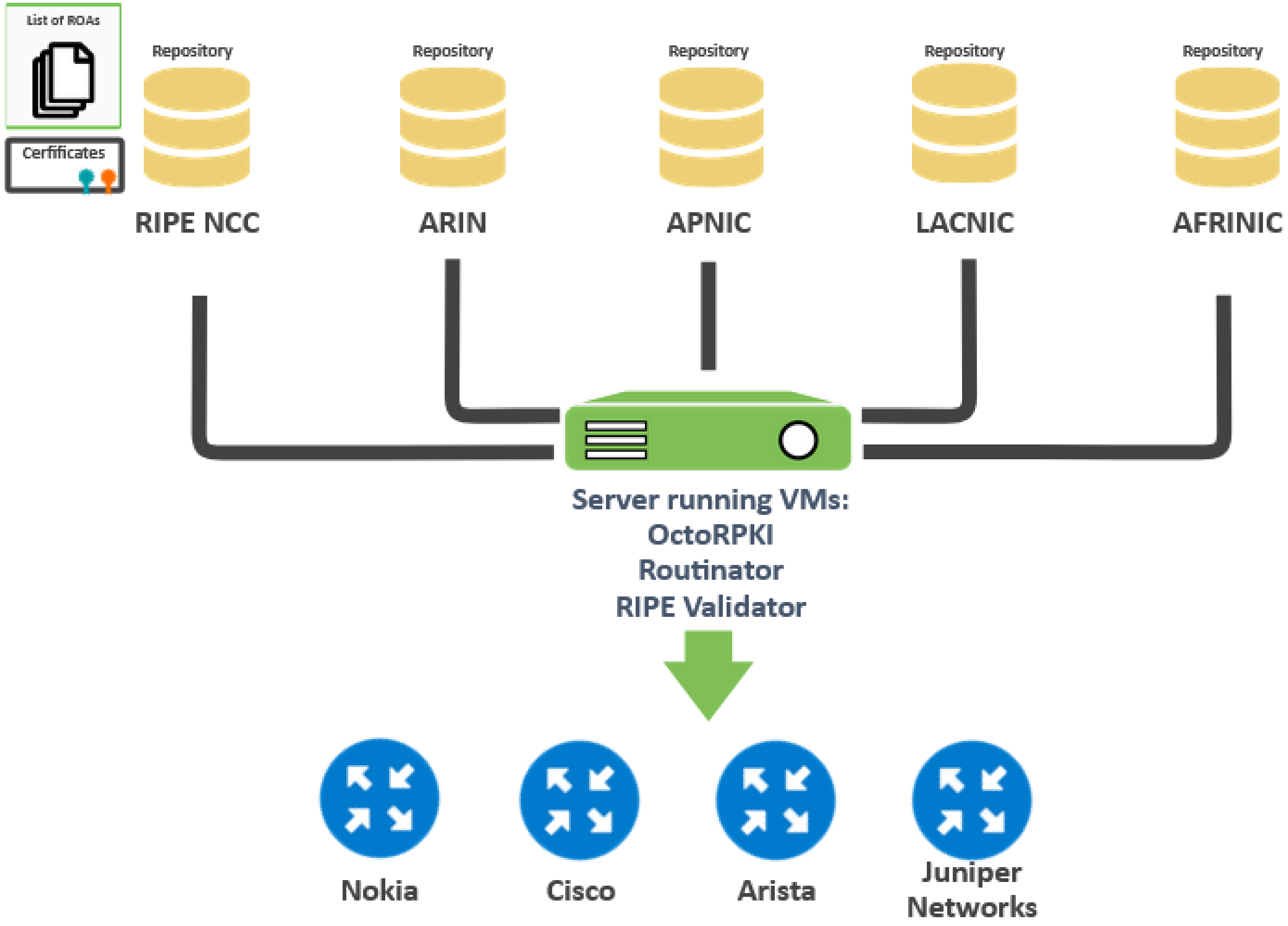
Add ROA

* Name:	Please enter a unique ROA name. Spaces will be replaced by '_'.
Your AS Numbers:	Please select your ASN from this list or enter any other valid ASN in the field below. Select an ASN
* AS Number:	ASN must be between 0 - 4294967295 in ASPLAIN format. "Reserved" and "Unallocated" ASNs will be rejected; "0" is allowed.
IPv4 address range:	Please select your prefix in the drop down list and click the '+' button, then you can specify the details Select an IPv4 prefix
IPv6 address range:	Please select your prefix in the drop down list and click the '+' button, then you can specify the details Select an IPv6 prefix
* Not Valid Before (YYYY-MM-DD):	
* Not Valid After (YYYY-MM-DD):	

Make sure your max length matches what you are advertising

RPKI validator

Topology



Server running VMs:
OctoRPKI
Routinator
RIPE Validator

Install your own validator

- ❑ Routinator

Installation steps

```
sudo apt install rsync build-essential
curl --proto '=https' --tlsv1.2 -sSf https://sh.rustup.rs | sh
source ~/.cargo/env
cargo install routinator
routinator init --accept-arin-rpa
routinator -v server --rtr 91.217.235.48:8323 –http 91.217.235.48:8080
```

https://routinator.readthedocs.io/en/latest/installation.html

Install your own validator

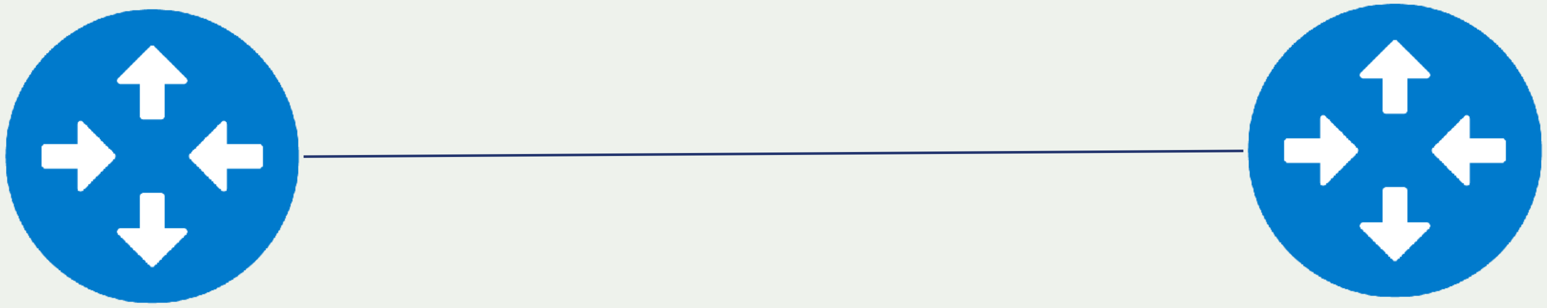
❑ OctoRPKI1

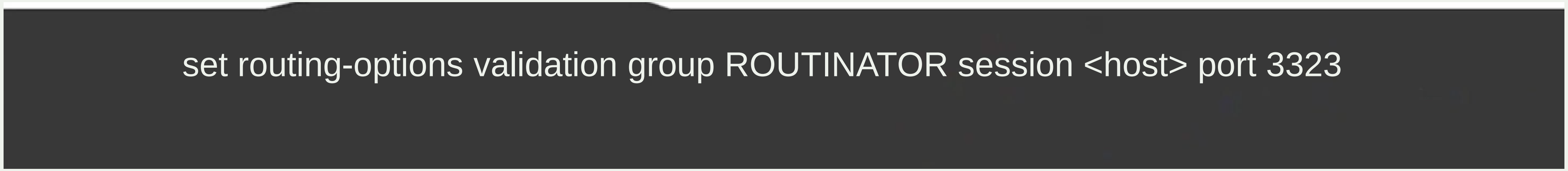
Installation steps

```
wget https://github.com/cloudflare/cfrpki/releases/download/v1.1.4/octorpki_1.1.4_amd64.deb
wget https://github.com/cloudflare/gortr/releases/download/v0.14.4/gortr_0.14.4_amd64.deb
sudo dpkg -i gortr_0.14.4_amd64.deb
sudo systemctl start gortr
sudo dpkg -i octorpki_1.1.4_amd64.deb
sudo wget https://www.arin.net/resources/manage/rpki/arin-rfc7730.tal -O /usr/share/octorpki/tals/arin.tal
echo OCTORPKI_ARGS=-output.sign=false -http.addr :8081 | sudo tee /etc/default/octorpki
sudo systemctl start octorpki
echo GORTR_ARGS=-verify=false -checktime=false -cache http://localhost:8081/output.json | sudo tee
/etc/default/gortr
sudo systemctl restart gortr
rtrdump -file "" | jq '.' | more
```

https://bit.ly/2V8f6XD

Configuring a validator on Juniper router

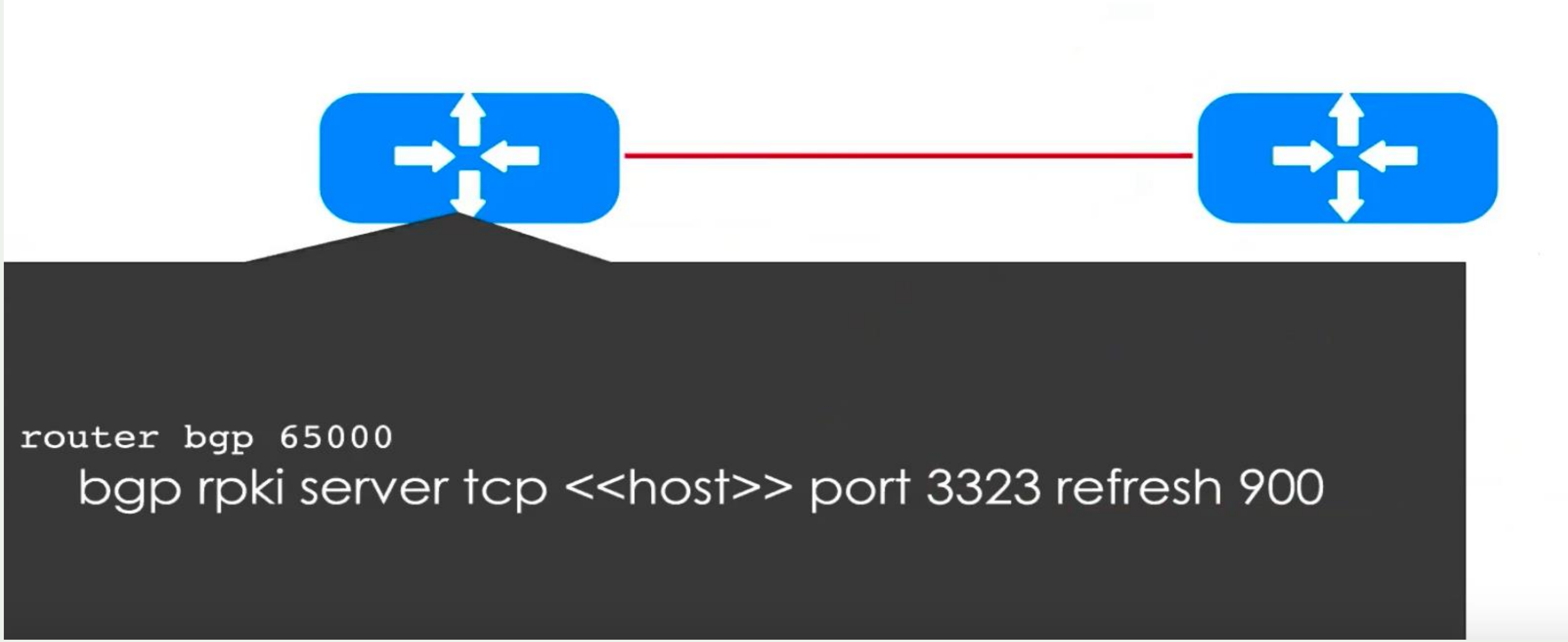




```
set routing-options validation group ROUTINATOR session <host> port 3323
```

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/bgp-origin-as-validation.html

Configuring a validator on cisco router



```
router bgp 65000
   bgp rpki server tcp <<host>> port 3323 refresh 900
```

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/15-s/irg-15-s-book/irg-origin-as.html

Thank you.

Ibar O Ibrahim

ibarosman@somaliren.org