IP Resource Certification

Andy Davidson

Hurricane Electric / LONAP / IXLeeds

adavidson@he.net

TREX Workshop 2011

16th September, Tampere, Finland

Resource Certification

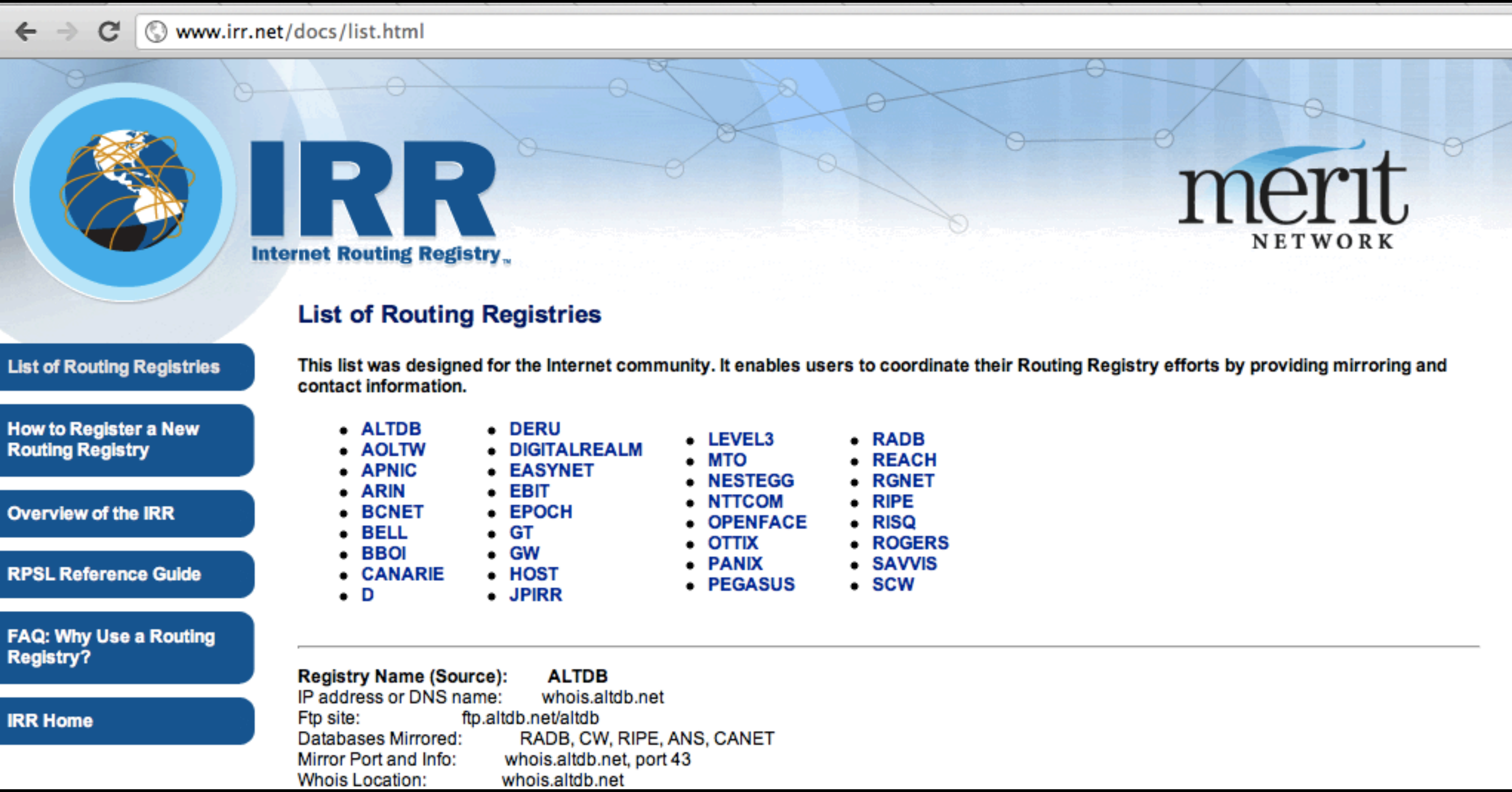
- Overview
- Certifying my resources with the RIPE NCC
- Verifying other's resources on my equipment

Attributions:
This slide deck acknowledges examples and concepts from the work of
Randy Bush (IIJ) and Alexander Band (RIPE NCC)

We <3 routing, but we **suck** at it.

- Accidental, huge customer impact
  - YouTube, Pakistan Telecom
  - AS7007
  - Unfiltered customers getting IP transit
- Deliberate, criminal activity?
  - Defcon/Pilosov – stealing traffic
  - Originating darknets for spam (blacklisting)
  - L-Root clones, discovered with ICANN renumbered

Can’t we mend this with IRR ?



www.irr.net/docs/list.html
IRR
Internet Routing Registry™
merit
NETWORK
List of Routing Registries
How to Register a New Routing Registry
Overview of the IRR
RPSL Reference Guide
FAQ: Why Use a Routing Registry?
IRR Home

List of Routing Registries

This list was designed for the Internet community. It enables users to coordinate their Routing Registry efforts by providing mirroring and contact information.

- ALTDB
- AOLTW
- APNIC
- ARIN
- BCNET
- BELL
- BBOI
- CANARIE
- D
- DERU
- DIGITALREALM
- EASYNET
- EBIT
- EPOCH
- GT
- GW
- HOST
- JPIRR
- LEVEL3
- MTO
- NESTEGG
- NTTCOM
- OPENFACE
- OTTIX
- PANIX
- PEGASUS
- RADB
- REACH
- RGNET
- RIPE
- RISQ
- ROGERS
- SAVVIS
- SCW

Registry Name (Source):	**ALTDB**
IP address or DNS name:	whois.altdb.net
Ftp site:	ftp.altdb.net/altdb
Databases Mirrored:	RADB, CW, RIPE, ANS, CANET
Mirror Port and Info:	whois.altdb.net, port 43
Whois Location:	whois.altdb.net

Let’s pretend for a moment that all of our customers will use *any* IRR…

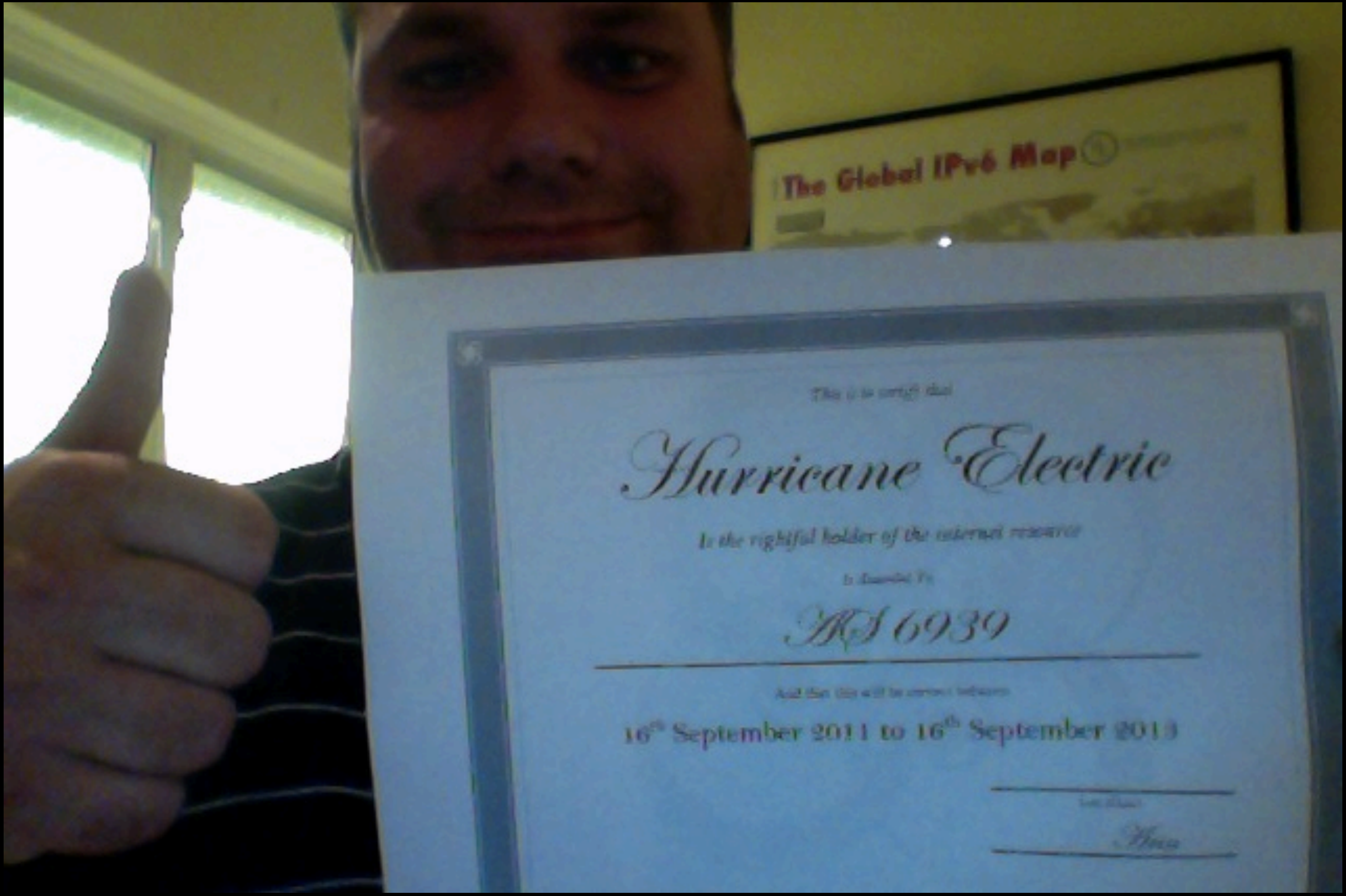
Certificates x509v3 and ROAs

Who owns?

Which Resource?

When?

According to?



This is to certify that

Hurricane Electric

Is the rightful holder of the internet resource

Is Awarded To

AS 6939

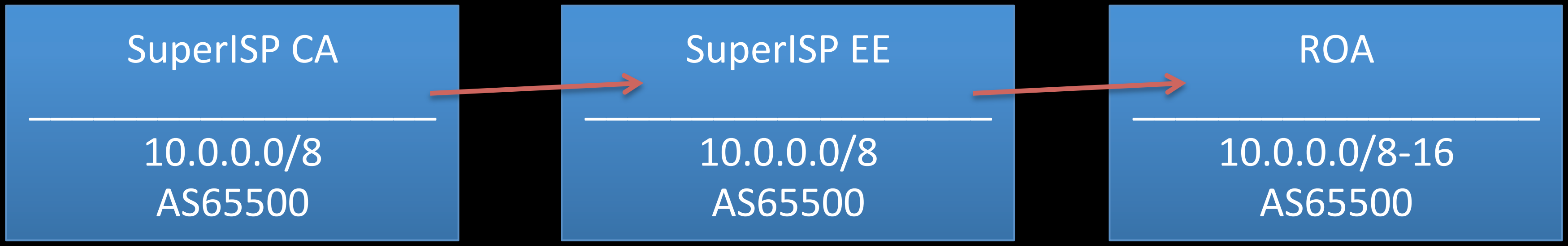
And that this will be correct between

16th September 2011 to 16th September 2013

[illegible]

ROA

- Route Origin Authorisation
- Not a certificate, a signed object.
- Prefix holder's explicit permission that a given prefix can be originated by a given ASN.



SuperISP CA
10.0.0.0/8
AS65500

SuperISP EE
10.0.0.0/8
AS65500

ROA
10.0.0.0/8-16
AS65500

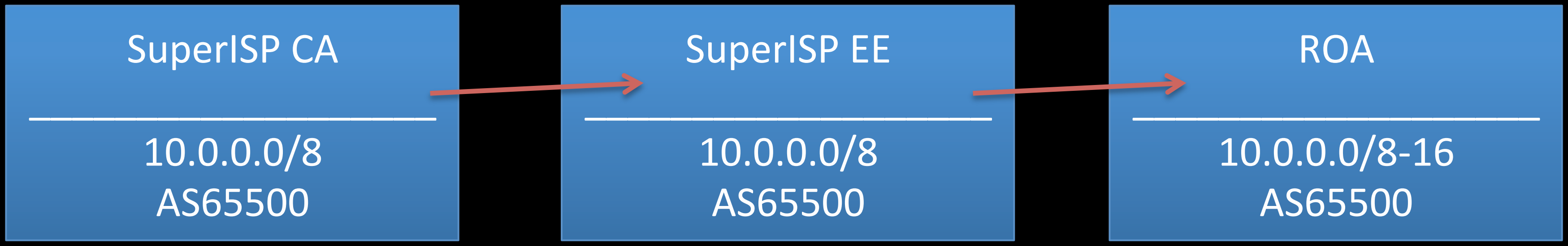
- This gives me data to do Origin validation with.

3 Step Process

Build a CA

Sign an EE

Publish a ROA



SuperISP CA

10.0.0.0/8
AS65500

SuperISP EE

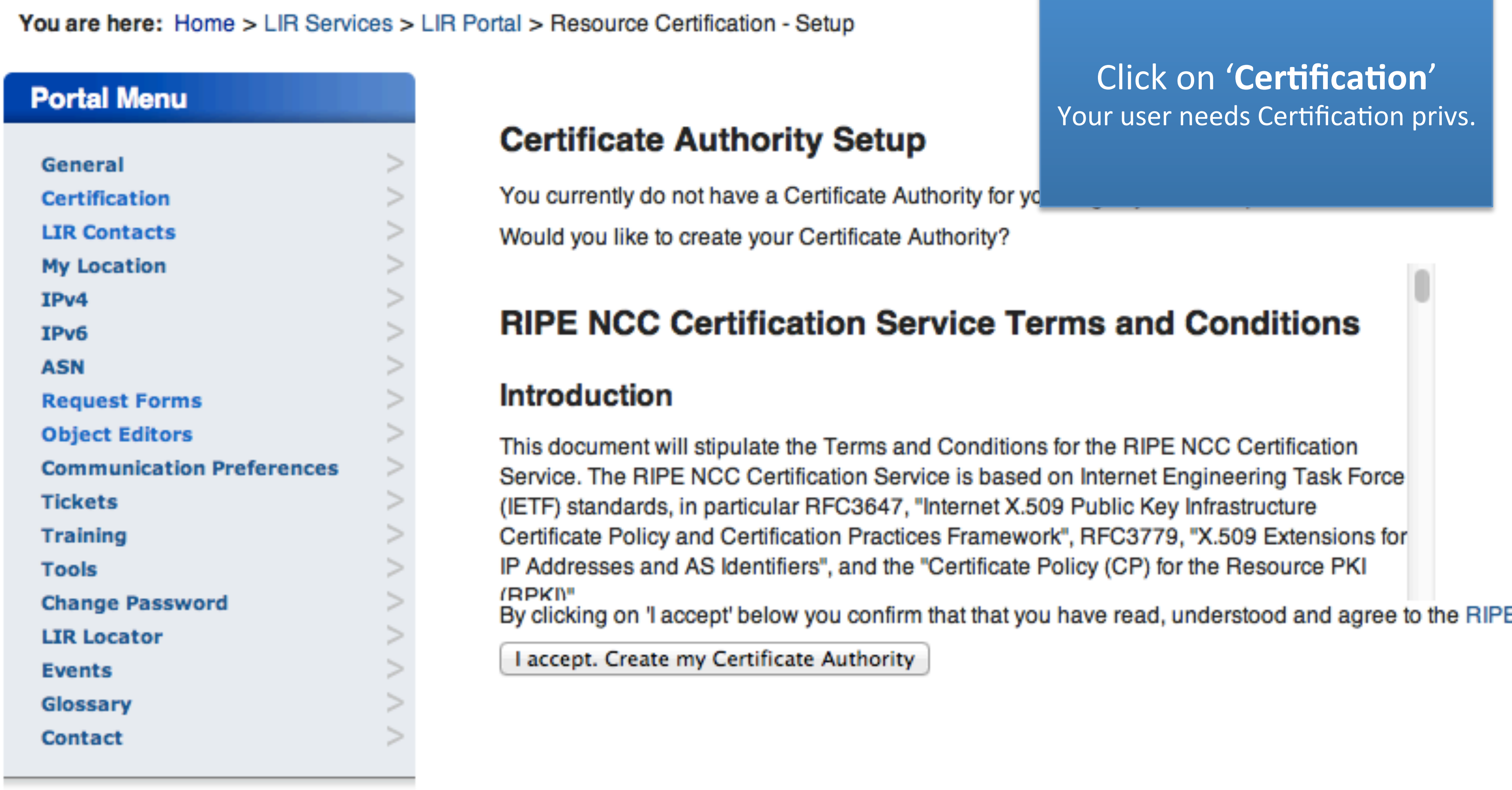
10.0.0.0/8
AS65500

ROA

10.0.0.0/8-16
AS65500

LIR PORTAL

Click on ‘**Certification**’
Your user needs Certification privs.



You are here: Home > LIR Services > LIR Portal > Resource Certification - Setup

Certificate Authority Setup

You currently do not have a Certificate Authority for yo

Would you like to create your Certificate Authority?

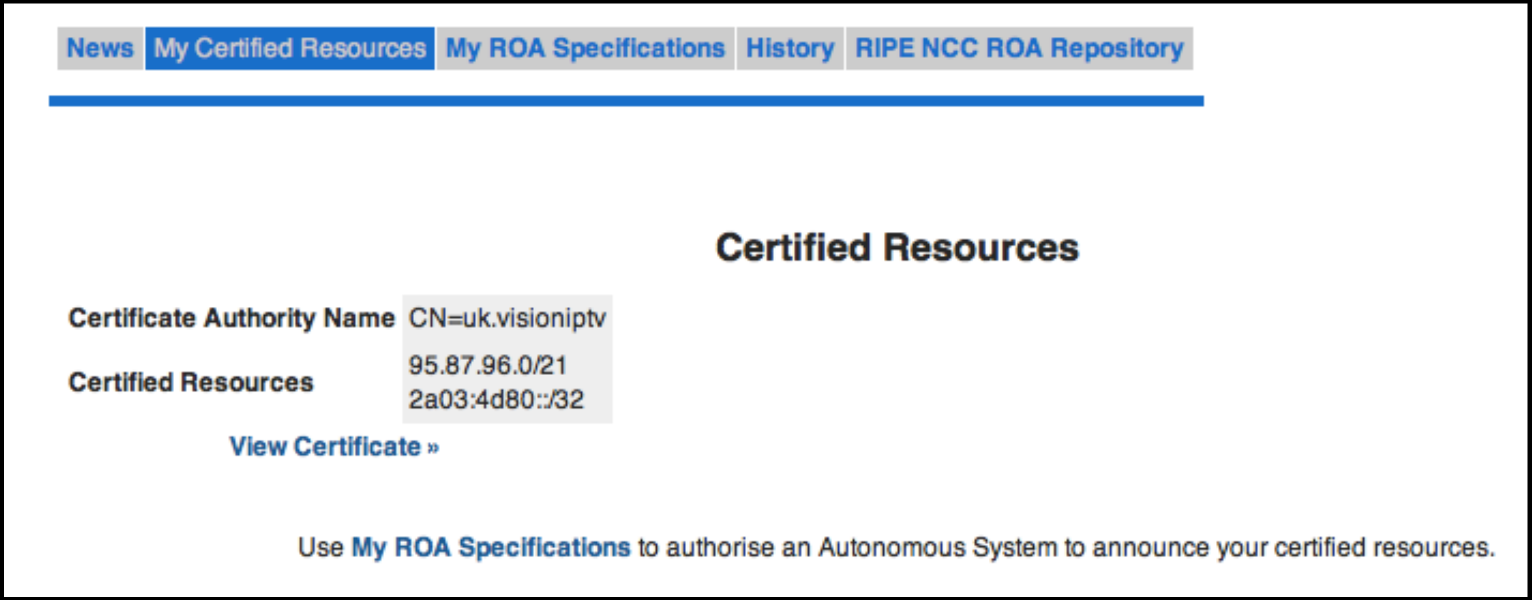
RIPE NCC Certification Service Terms and Conditions

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)"

By clicking on 'I accept' below you confirm that that you have read, understood and agree to the RIPE

Clicking through to build your CA also creates certificates for your aggregate resources.

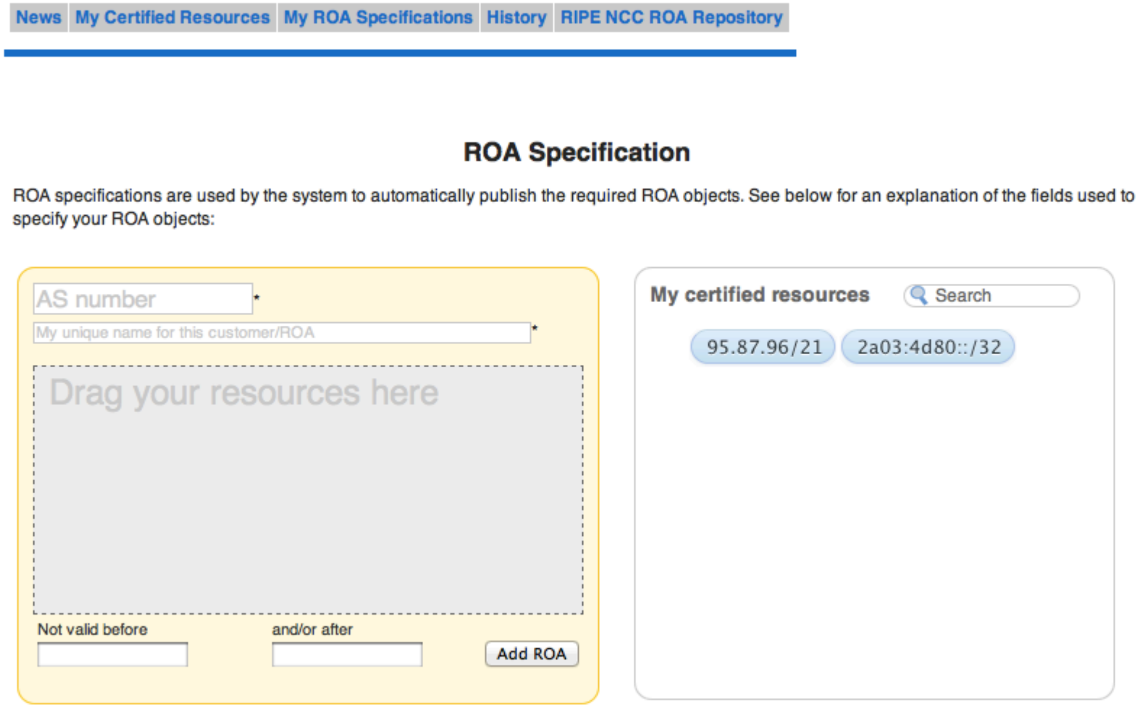


Certified Resources

Certificate Authority Name	CN=uk.visioniptv
Certified Resources	95.87.96.0/21 2a03:4d80::/32

View Certificate »

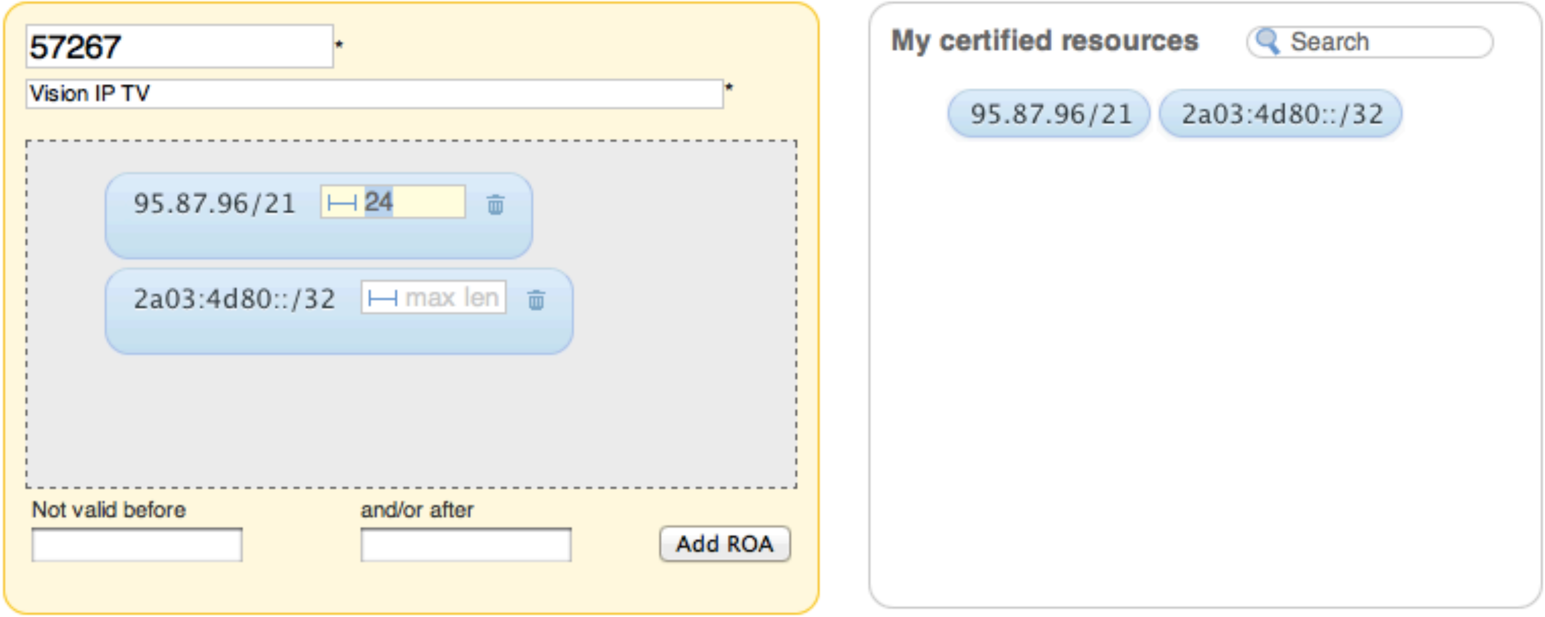
Use My ROA Specifications to authorise an Autonomous System to announce your certified resources.



ROA Specification

ROA specifications are used by the system to automatically publish the required ROA objects. See below for an explanation of the fields used to specify your ROA objects:

Drag and Drop your resources into the ROA Builder…

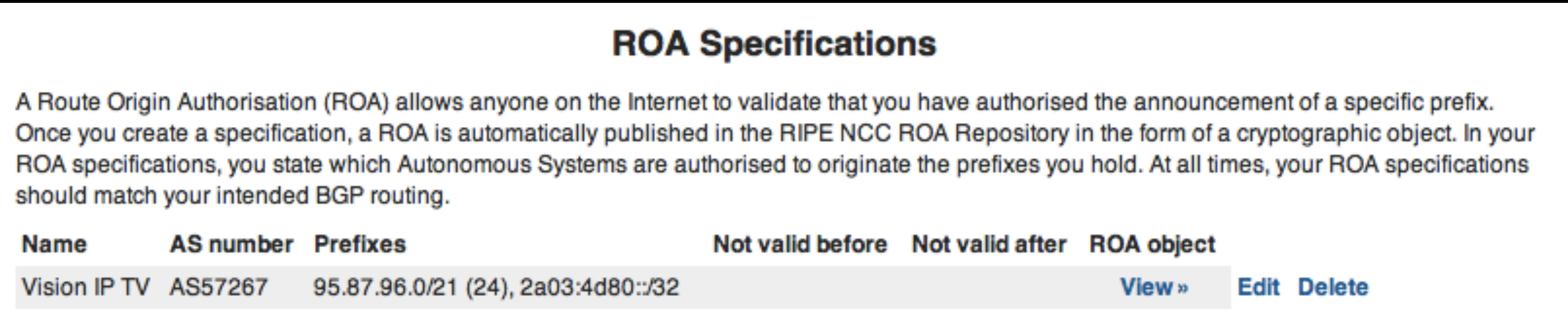


57267 *

Vision IP TV *

95.87.96/21 24

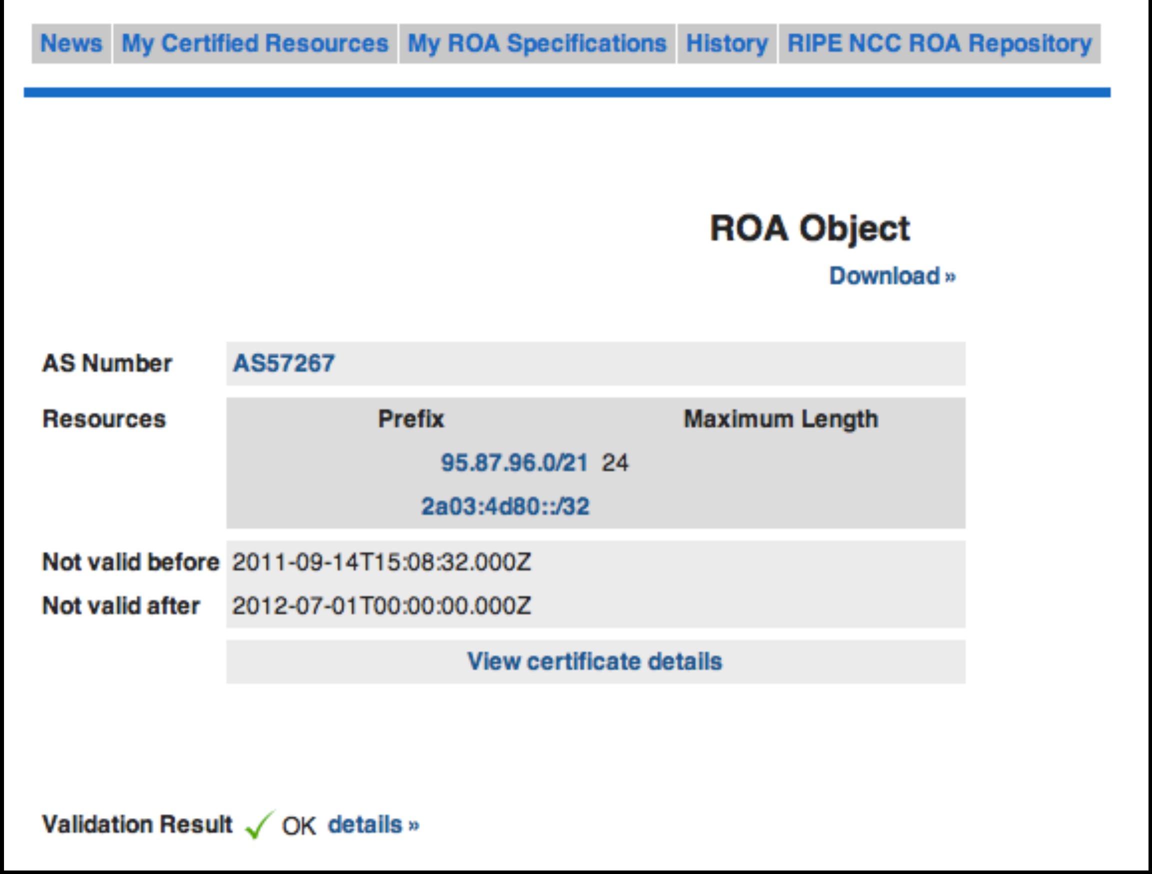
2a03:4d80::/32 max len



ROA Specifications

A Route Origin Authorisation (ROA) allows anyone on the Internet to validate that you have authorised the announcement of a specific prefix. Once you create a specification, a ROA is automatically published in the RIPE NCC ROA Repository in the form of a cryptographic object. In your ROA specifications, you state which Autonomous Systems are authorised to originate the prefixes you hold. At all times, your ROA specifications should match your intended BGP routing.

Name	AS number	Prefixes	Not valid before	Not valid after	ROA object	
Vision IP TV	AS57267	95.87.96.0/21 (24), 2a03:4d80::/32			View »	Edit Delete



ROA Object

Download »

AS Number AS57267

Resources

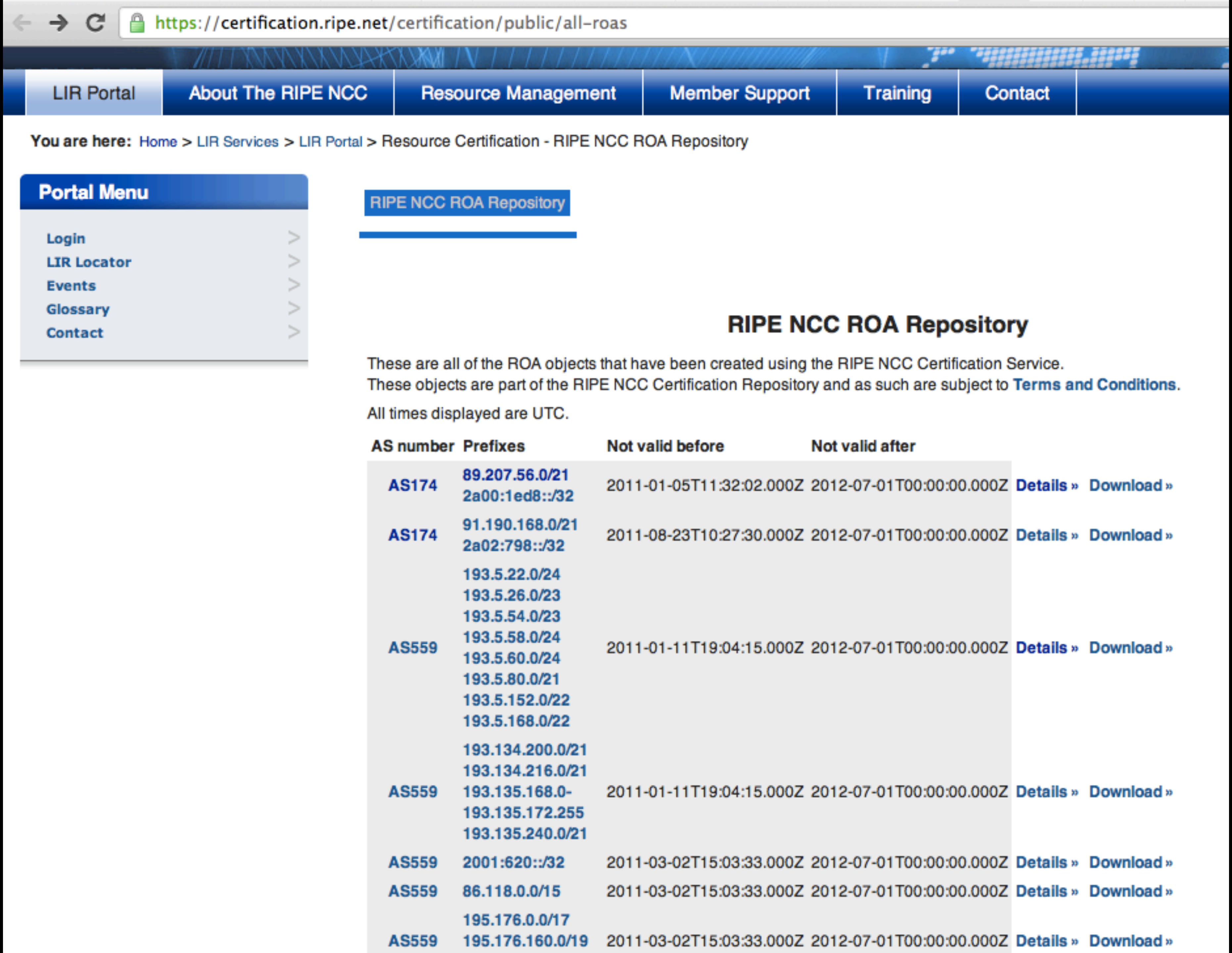
Prefix	Maximum Length
95.87.96.0/21	24
2a03:4d80::/32	

Not valid before 2011-09-14T15:08:32.000Z

Not valid after 2012-07-01T00:00:00.000Z

View certificate details

Validation Result ✓ OK details »

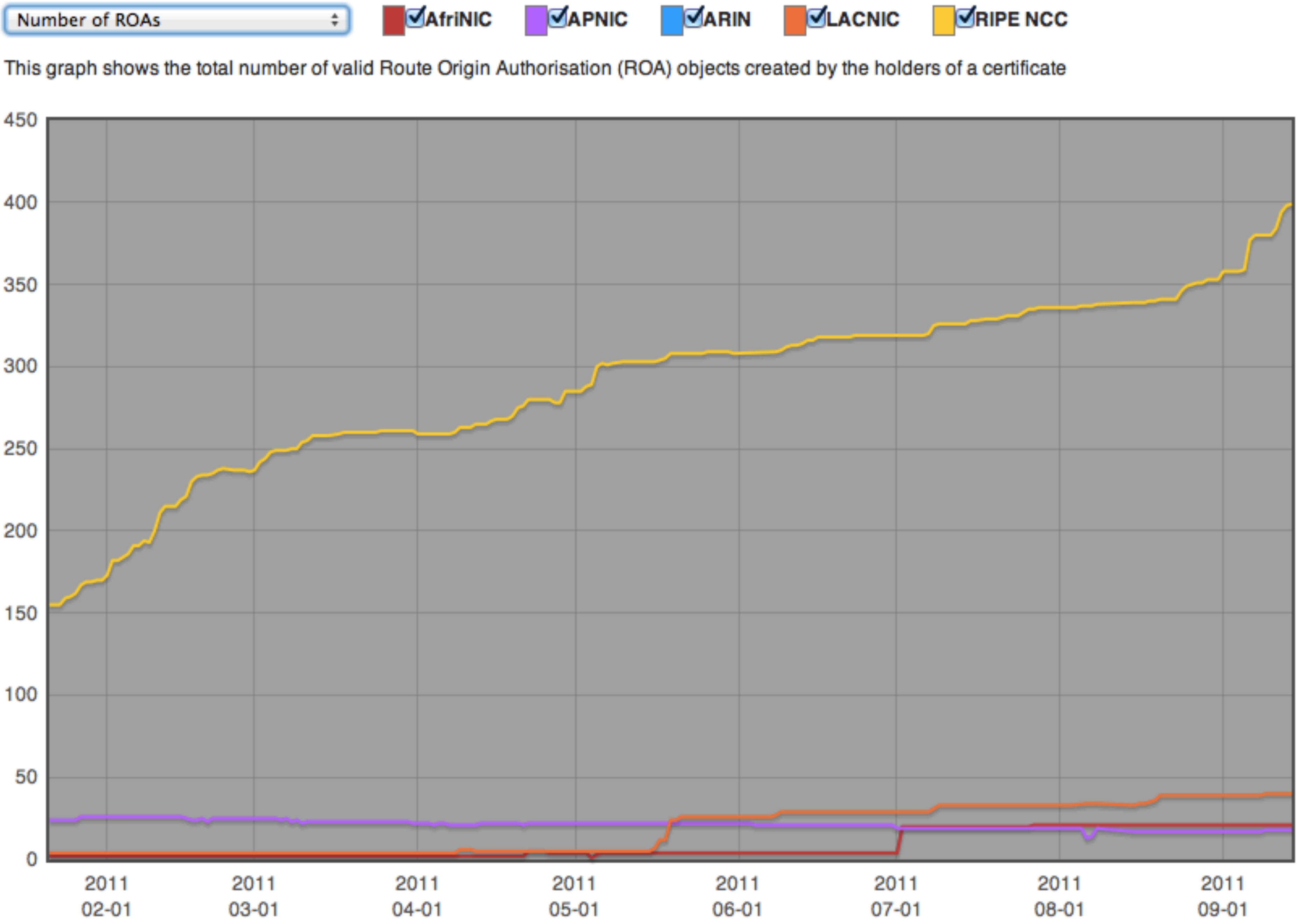

https://certification.ripe.net/certification/public/all-roas
LIR Portal
About The RIPE NCC
Resource Management
Member Support
Training
Contact
You are here: Home > LIR Services > LIR Portal > Resource Certification - RIPE NCC ROA Repository
Portal Menu
Login
LIR Locator
Events
Glossary
Contact
RIPE NCC ROA Repository

RIPE NCC ROA Repository

These are all of the ROA objects that have been created using the RIPE NCC Certification Service.
These objects are part of the RIPE NCC Certification Repository and as such are subject to Terms and Conditions.

All times displayed are UTC.

AS number	Prefixes	Not valid before	Not valid after		
AS174	89.207.56.0/21 2a00:1ed8::/32	2011-01-05T11:32:02.000Z	2012-07-01T00:00:00.000Z	Details »	Download »
AS174	91.190.168.0/21 2a02:798::/32	2011-08-23T10:27:30.000Z	2012-07-01T00:00:00.000Z	Details »	Download »
AS559	193.5.22.0/24 193.5.26.0/23 193.5.54.0/23 193.5.58.0/24 193.5.60.0/24 193.5.80.0/21 193.5.152.0/22 193.5.168.0/22	2011-01-11T19:04:15.000Z	2012-07-01T00:00:00.000Z	Details »	Download »
AS559	193.134.200.0/21 193.134.216.0/21 193.135.168.0-193.135.172.255 193.135.240.0/21	2011-01-11T19:04:15.000Z	2012-07-01T00:00:00.000Z	Details »	Download »
AS559	2001:620::/32	2011-03-02T15:03:33.000Z	2012-07-01T00:00:00.000Z	Details »	Download »
AS559	86.118.0.0/15	2011-03-02T15:03:33.000Z	2012-07-01T00:00:00.000Z	Details »	Download »
AS559	195.176.0.0/17 195.176.160.0/19	2011-03-02T15:03:33.000Z	2012-07-01T00:00:00.000Z	Details »	Download »

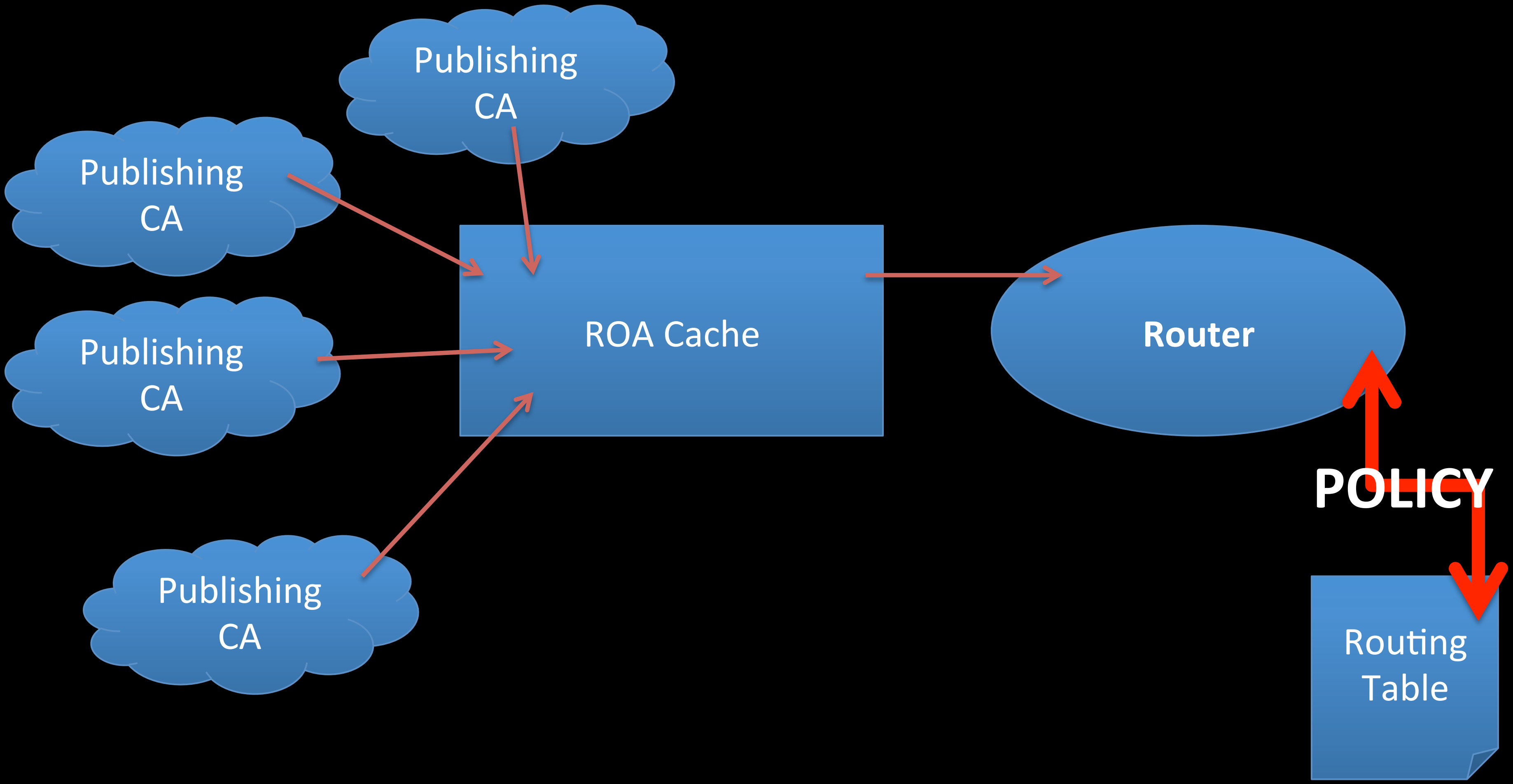


Number of ROAs

🟥 ☑ AfriNIC 🟪 ☑ APNIC 🟦 ☑ ARIN 🟧 ☑ LACNIC 🟨 ☑ RIPE NCC

This graph shows the total number of valid Route Origin Authorisation (ROA) objects created by the holders of a certificate

How can I verify others’ ROA?



VALID
Matching ROA and AS Number

INVALID
Matching ROA found but AS number did not match!

NOT FOUND
No ROA

I can write policies on my router which cause different behaviours depending on the response from my RPKI cache….

Example Router Configuration

```
router bgp 10
   bgp log-neighbor-changes
   bgp rpki cache 192.168.10.10 port-number 32000 refresh-time 5
   network 192.168.10.0
   neighbor 192.168.0.2 remote-as 20
   neighbor 192.168.0.2 soft-reconfiguration inbound
   neighbor 192.168.0.6 remote-as 66
   neighbor 192.168.0.6 soft-reconfiguration inbound
   neighbor 192.168.0.6 route-map PERMIT-INVALID in


route-map PERMIT-INVALID permit 10
   match rpki-invalid
   set local-preference 50
```

Make a valid alternative prefix become best-path.

Better Example with route-policy in XR

```
route-policy validity-0
 if origin-validation-state is valid then
   set local-preference 100
   else set local-preference 50
   endif
end-policy

route-policy validity-2
 if origin-validation-state is valid then
   set metric 100
elseif origin-validate-state is not-found
   set metric 50
 else set metric 25
   endif
end-policy
```

One day safe?

```
route-map validity-0
   match rpki-invalid
   drop
route-map validity-1
   match rpki-not-found
   set localpref 1
```

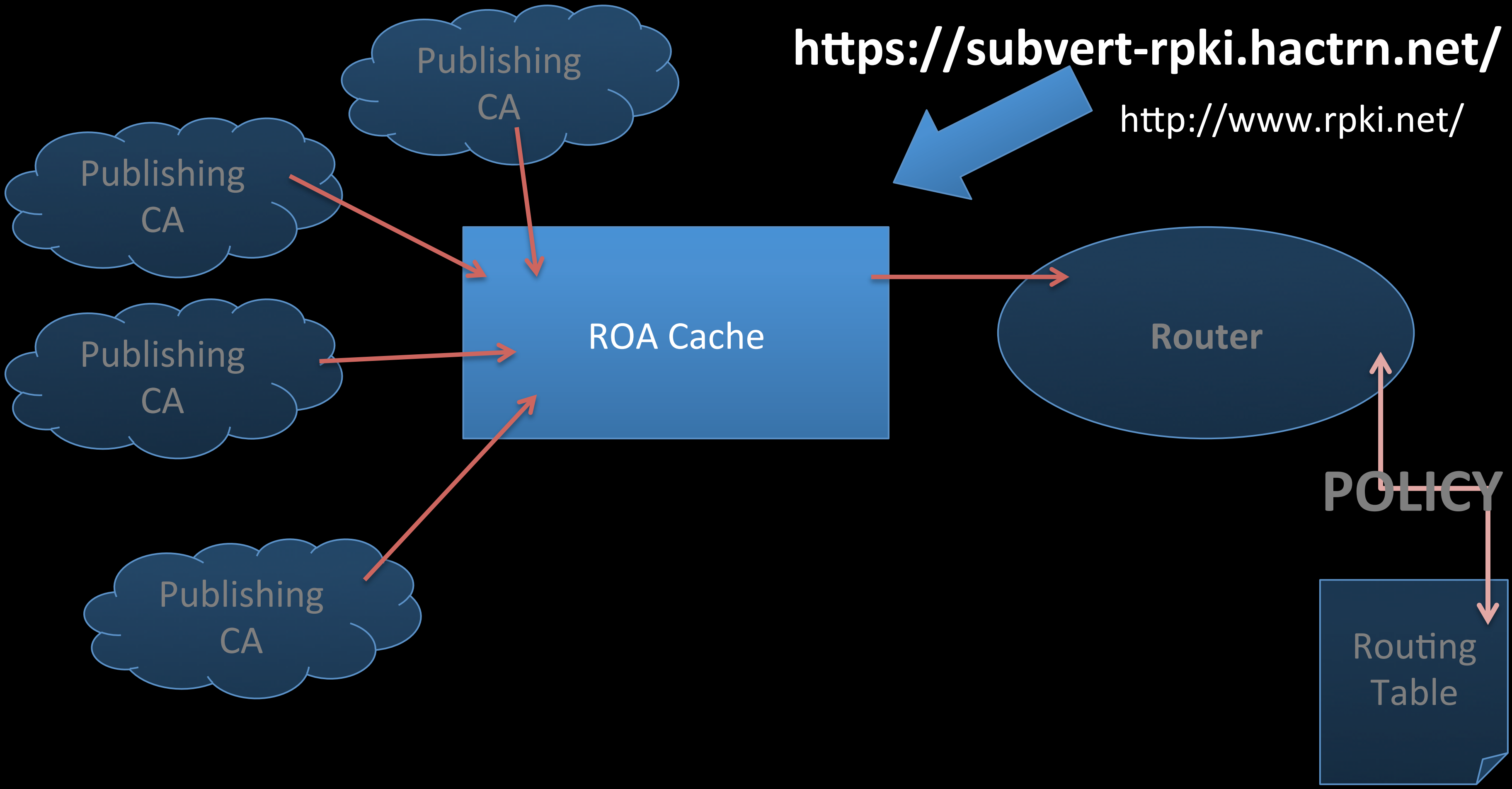
See ya, sucker!!!!

Maybe I want an certified peer pfx to score lower than a valid route from transit..

Only import signed objects

```
route-map validity-0
   match rpki-valid
   set localpref 110
route-map validity-1
   drop
```

Open Source ROA Processor



https://subvert-rpki.hactrn.net/

http://www.rpki.net/

Not a magic bullet

- Path Validation missing
  - Still vulnerable to MITM attacks.
- Early code from vendors
  - Lots of testing work to do!
- Address Policy, Trust relationships
  - RPKI – is it an "off" switch for networks?
- Huge and paranoid organisations will want to run their own CAs, not the RIR one.

Questions ?

Feedback ?

Abuse ?

@andyd