Resource Certification (RPKI)

Alex Band – Product Manager

The RIPE NCC involvement in RPKI

- The authority on who is the registered holder of an Internet Number Resource in our region
  - IPv4 and IPv6 Address Blocks
  - Autonomous System Numbers

- Information is kept in the Registry

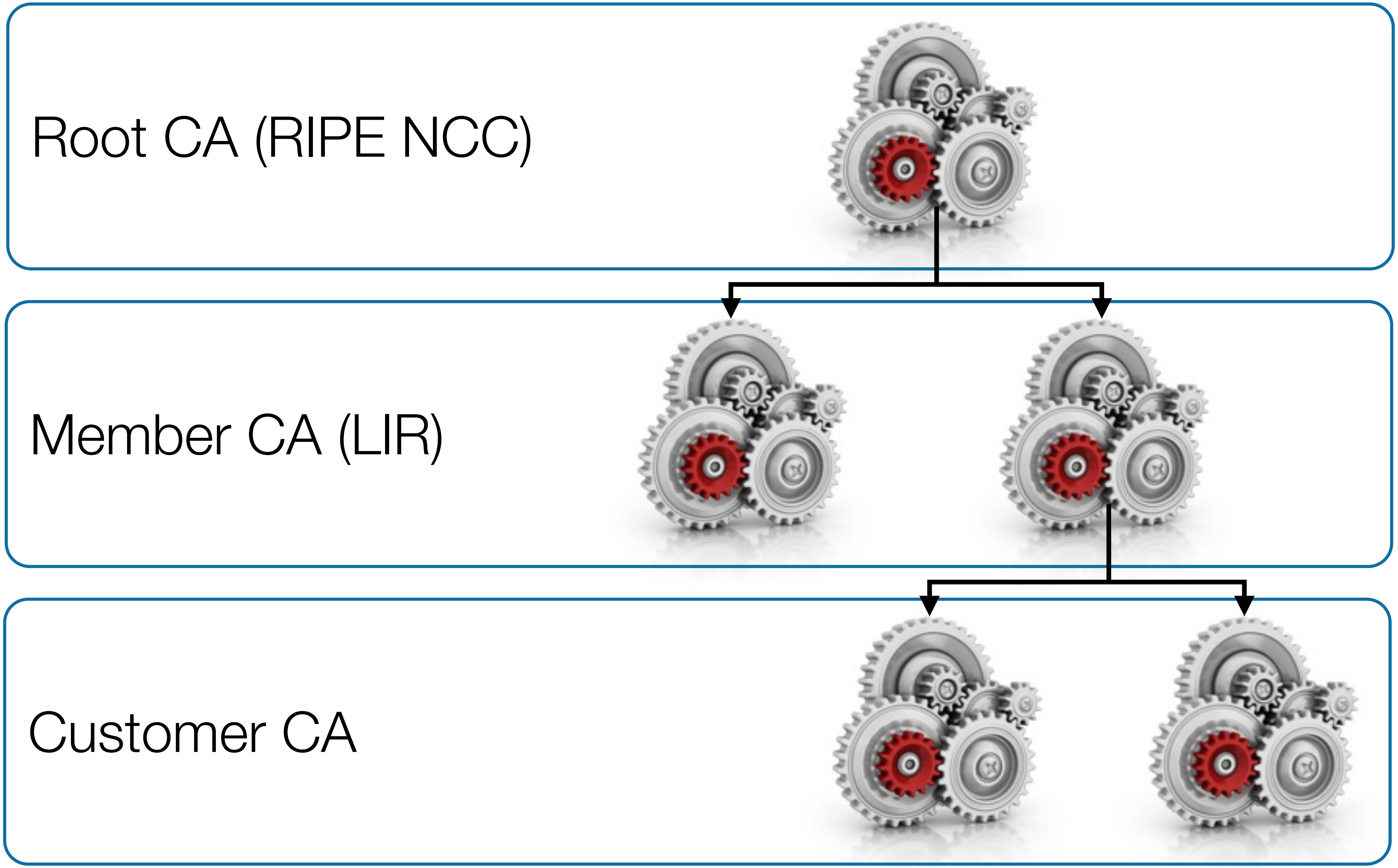
- Accuracy and completeness are key

Digital Resource Certificates

- Resource Certification is a free, opt-in service
  - Your choice to request a certificate
    - Linked to registration
    - Renewed every 12 months

- Certificate does not list any identity information

Certificate Authority (CA) Structure



Root CA (RIPE NCC)

Member CA (LIR)

Customer CA

Applications for Certificates

BGP Origin Validation

RIPE NCC

Management: Your Choice

- Open Source Software to run a member CA
  - Use the RIPE NCC as parent CA (trust anchor)
  - Generate and publish Certificate yourself

- RIPE NCC Hosted Platform
  - All processes are secured and automated
  - One click set-up of Resource Certificate
  - WebUI to manage Certificates in LIR Portal

Certification to Secure Internet Routing

- Members can use their resource certificate to make statements about their BGP Routing

Route Origin Authorisation (ROA):

“I authorise this Autonomous System to originate these IP prefixes”

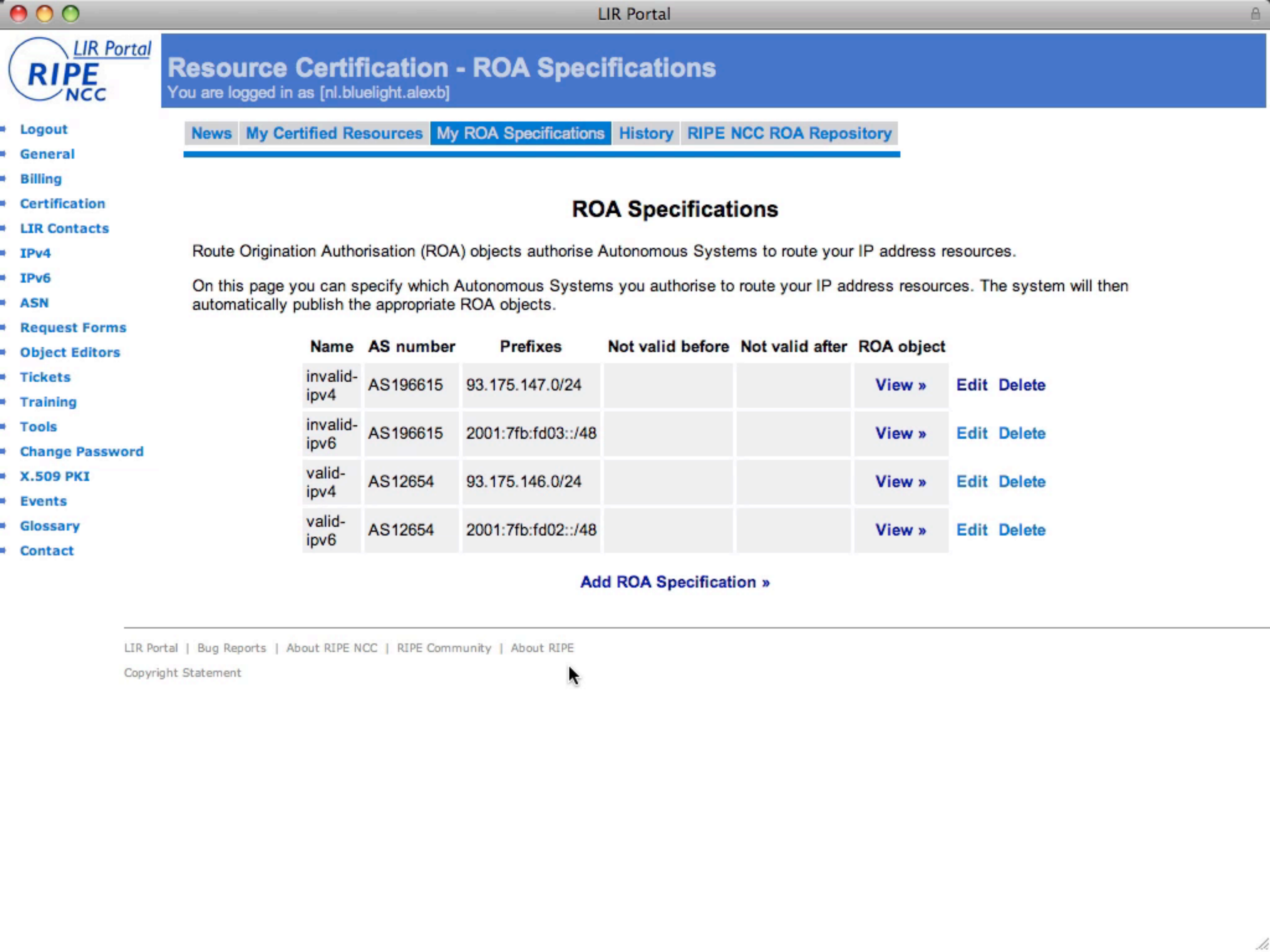
- Other network operators can set their routing preferences based on this information

Route Origin Authorisations

- Only the registered holder of a Internet number resource can create a valid ROA
- A ROA affects the RPKI validity of a route announcement:
  - VALID: ROA found, authorised announcement
  - INVALID: ROA found, unauthorised announcement
  - UNKNOWN: No ROA found (resource not yet signed)

ROA Creation

Demo



Resource Certification - ROA Specifications

You are logged in as [nl.bluelight.alexb]

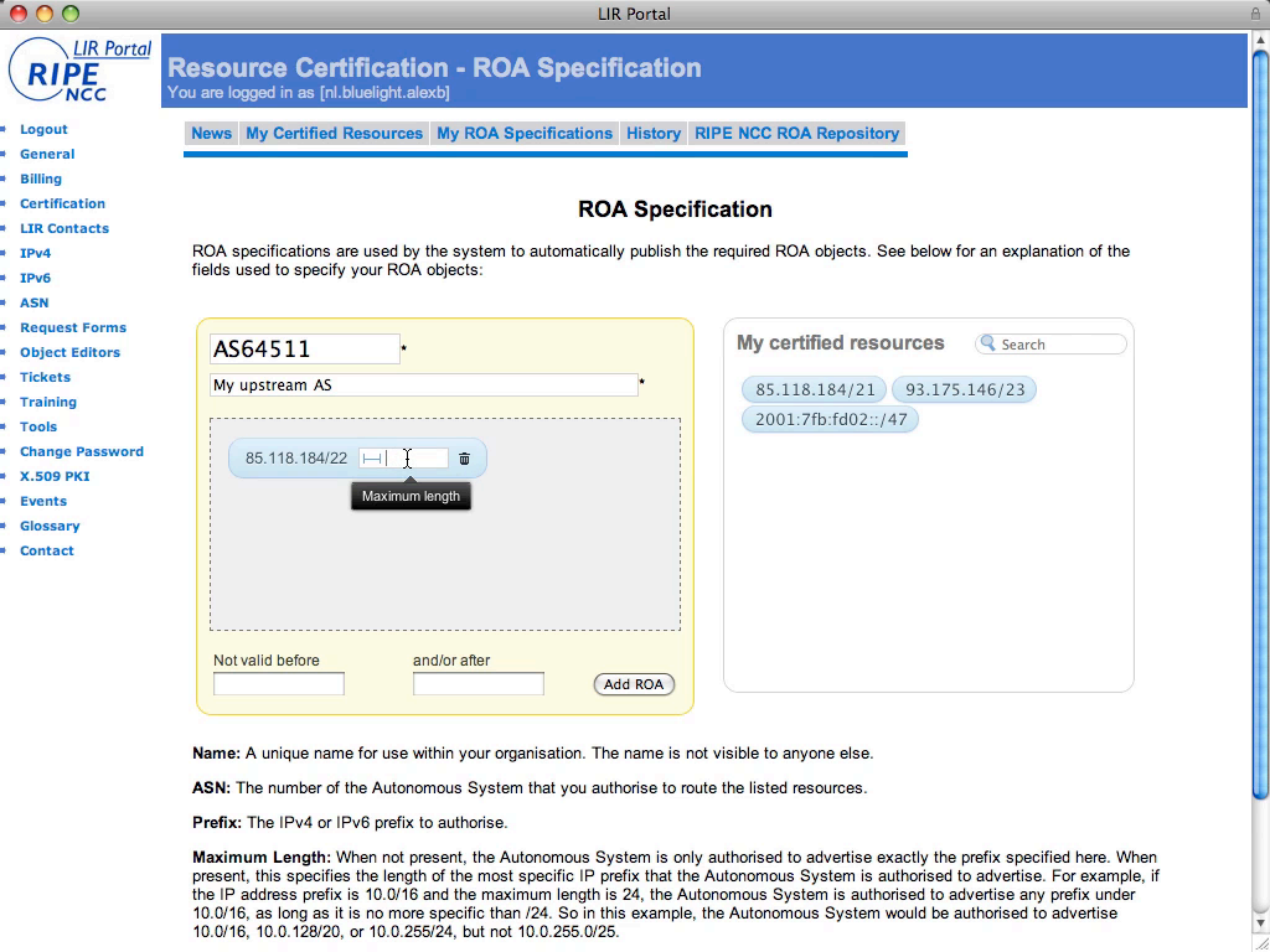
ROA Specifications

Route Origination Authorisation (ROA) objects authorise Autonomous Systems to route your IP address resources.

On this page you can specify which Autonomous Systems you authorise to route your IP address resources. The system will then automatically publish the appropriate ROA objects.

Name	AS number	Prefixes	Not valid before	Not valid after	ROA object	
invalid-ipv4	AS196615	93.175.147.0/24			View »	Edit Delete
invalid-ipv6	AS196615	2001:7fb:fd03::/48			View »	Edit Delete
valid-ipv4	AS12654	93.175.146.0/24			View »	Edit Delete
valid-ipv6	AS12654	2001:7fb:fd02::/48			View »	Edit Delete

Add ROA Specification »
LIR Portal | Bug Reports | About RIPE NCC | RIPE Community | About RIPE
Copyright Statement



Resource Certification - ROA Specification

You are logged in as [nl.bluelight.alexb]

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:

AS64511 *

My upstream AS *

85.118.184/22

Not valid before

and/or after

My certified resources

85.118.184/21

93.175.146/23

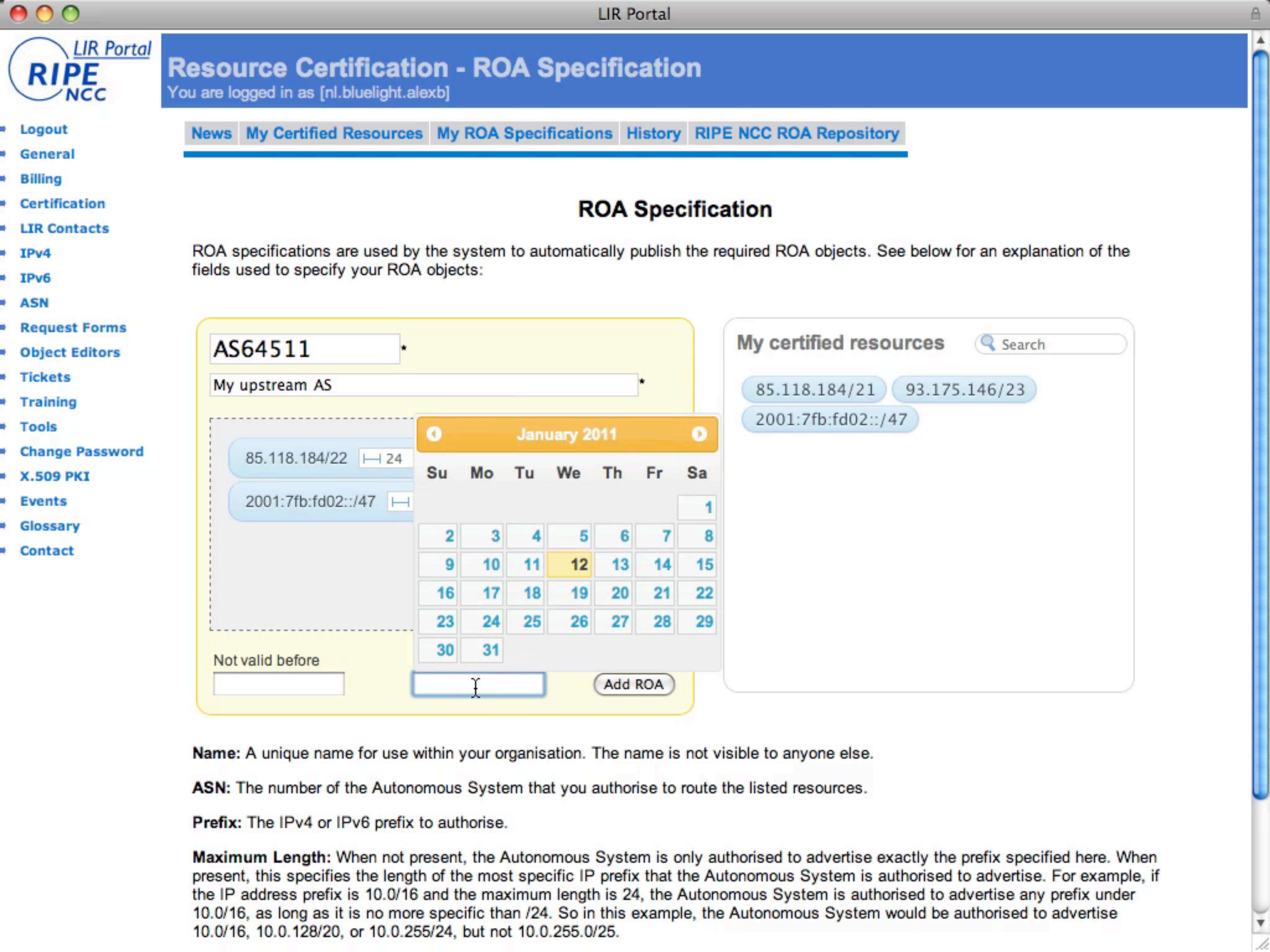
2001:7fb:fd02::/47

Name: A unique name for use within your organisation. The name is not visible to anyone else.

ASN: The number of the Autonomous System that you authorise to route the listed resources.

Prefix: The IPv4 or IPv6 prefix to authorise.

Maximum Length: When not present, the Autonomous System is only authorised to advertise exactly the prefix specified here. When present, this specifies the length of the most specific IP prefix that the Autonomous System is authorised to advertise. For example, if the IP address prefix is 10.0/16 and the maximum length is 24, the Autonomous System is authorised to advertise any prefix under 10.0/16, as long as it is no more specific than /24. So in this example, the Autonomous System would be authorised to advertise 10.0/16, 10.0.128/20, or 10.0.255/24, but not 10.0.255.0/25.



Resource Certification - ROA Specification

You are logged in as [nl.bluelight.alexb]

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:

AS64511 *

My upstream AS *

85.118.184/22 ⊢⊣ 24

2001:7fb:fd02::/47 ⊢⊣

Not valid before

My certified resources

85.118.184/21 93.175.146/23

2001:7fb:fd02::/47

Name: A unique name for use within your organisation. The name is not visible to anyone else.

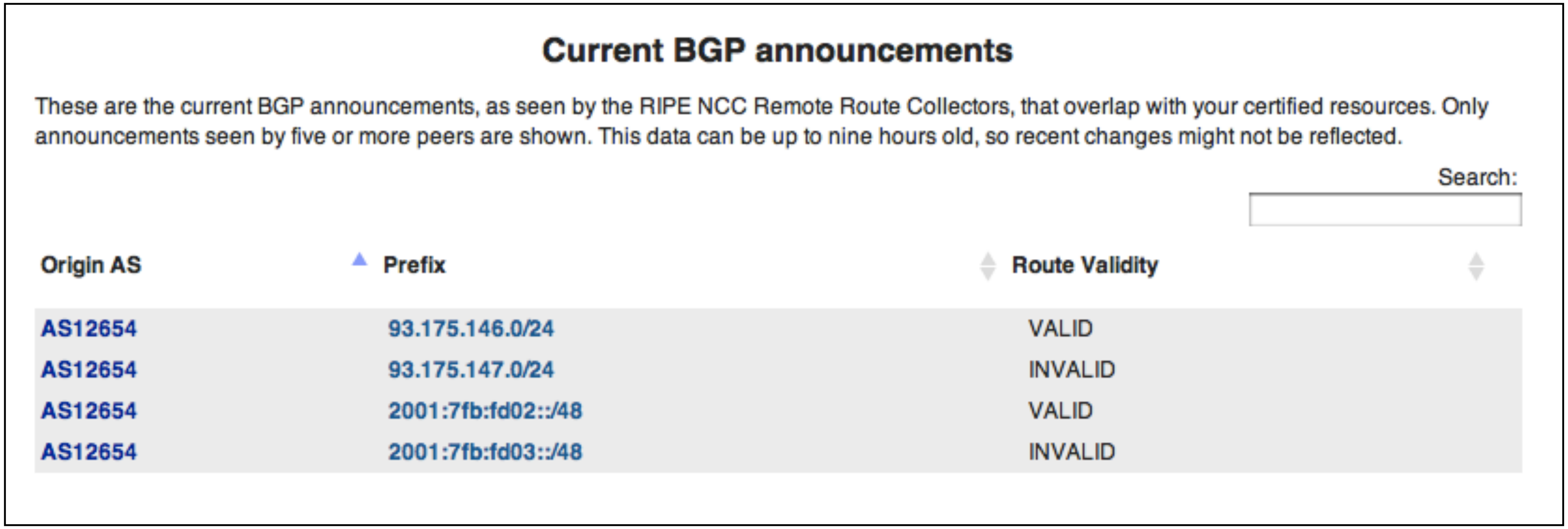
ASN: The number of the Autonomous System that you authorise to route the listed resources.

Prefix: The IPv4 or IPv6 prefix to authorise.

Maximum Length: When not present, the Autonomous System is only authorised to advertise exactly the prefix specified here. When present, this specifies the length of the most specific IP prefix that the Autonomous System is authorised to advertise. For example, if the IP address prefix is 10.0/16 and the maximum length is 24, the Autonomous System is authorised to advertise any prefix under 10.0/16, as long as it is no more specific than /24. So in this example, the Autonomous System would be authorised to advertise 10.0/16, 10.0.128/20, or 10.0.255/24, but not 10.0.255.0/25.

Data Quality and Integrity

- Use RIS Route Collectors to support Certification
  - Show the RPKI validity state of a route announcement
  - Trigger alert when ROAs mismatch BGP



Current BGP announcements

These are the current BGP announcements, as seen by the RIPE NCC Remote Route Collectors, that overlap with your certified resources. Only announcements seen by five or more peers are shown. This data can be up to nine hours old, so recent changes might not be reflected.

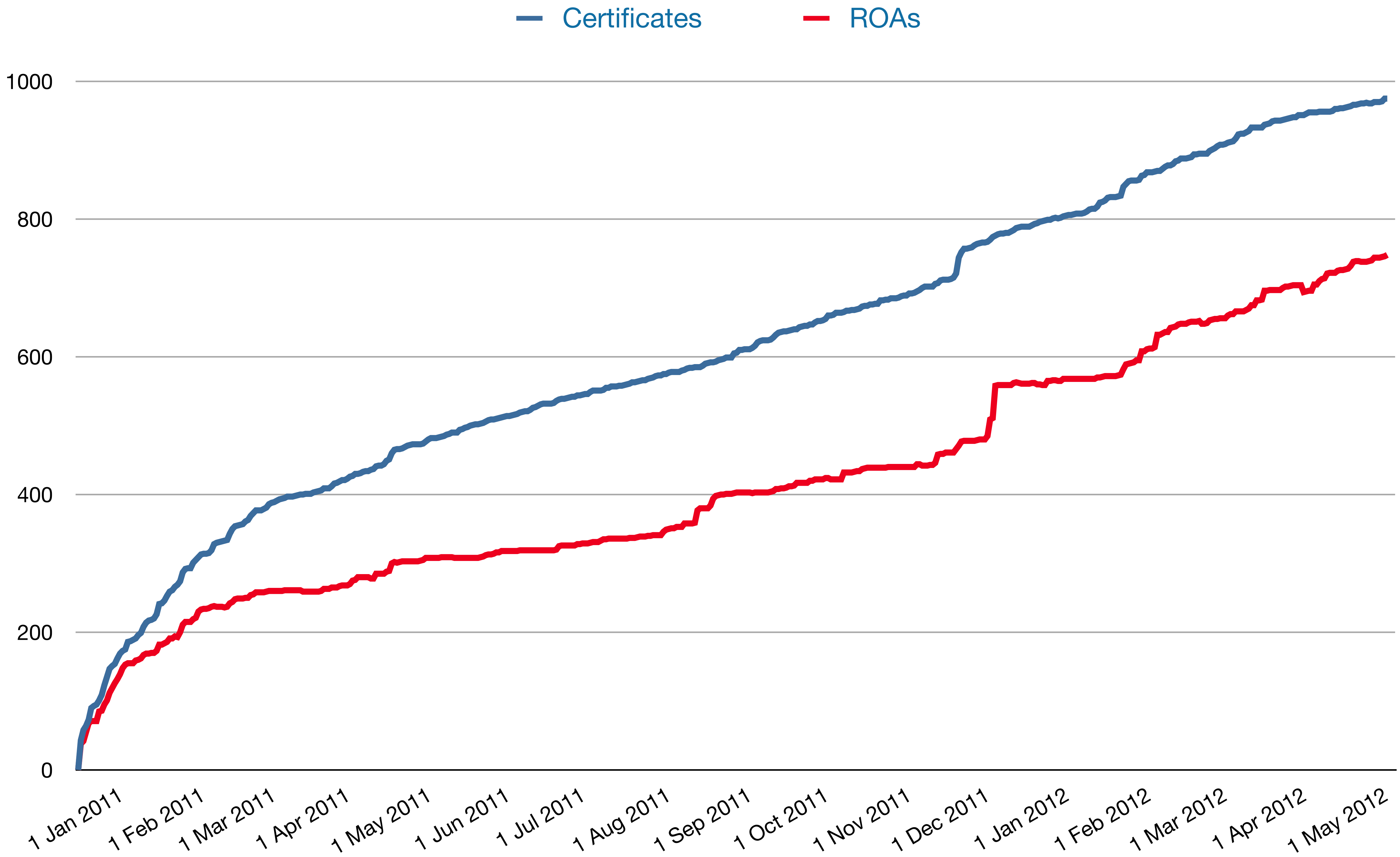
Search:

Origin AS	Prefix	Route Validity
AS12654	93.175.146.0/24	VALID
AS12654	93.175.147.0/24	INVALID
AS12654	2001:7fb:fd02::/48	VALID
AS12654	2001:7fb:fd03::/48	INVALID

Publication of cryptographic objects

- Publication is distributed by design
  - Publish yourself or publish through a 3rd party
- Each RIR has a public repository
  - Holds Certificates, ROAs, etc.
  - Refreshed at least every 24 hrs
- Accessed using a Validation tool
  - Communication via rsync
  - Builds up a local validated cache

Resource Certification Adoption



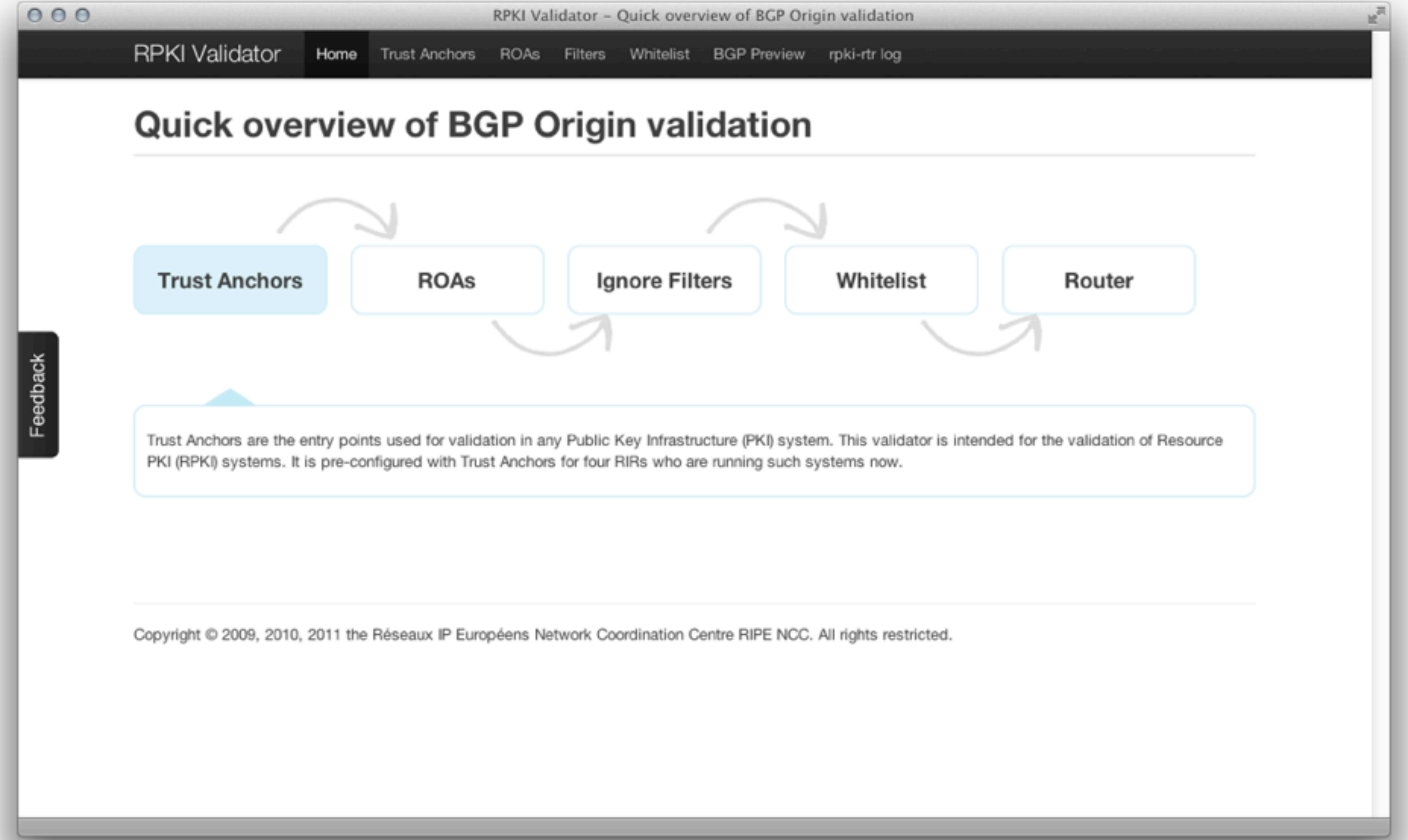
RIPE NCC RPKI Validation tool

RIPE NCC RPKI-RTR Validator

- Web-based user interface
- Periodically validates all ROA repositories
  - Downloads and processes changes automatically
- Ignore Filters (Apply RPKI status ‘Unknown’)
- Whitelist (Apply RPKI status ‘Valid’)
- RPKI-Router Support
  - Cisco, Juniper, Quagga...

Open source, BSD License

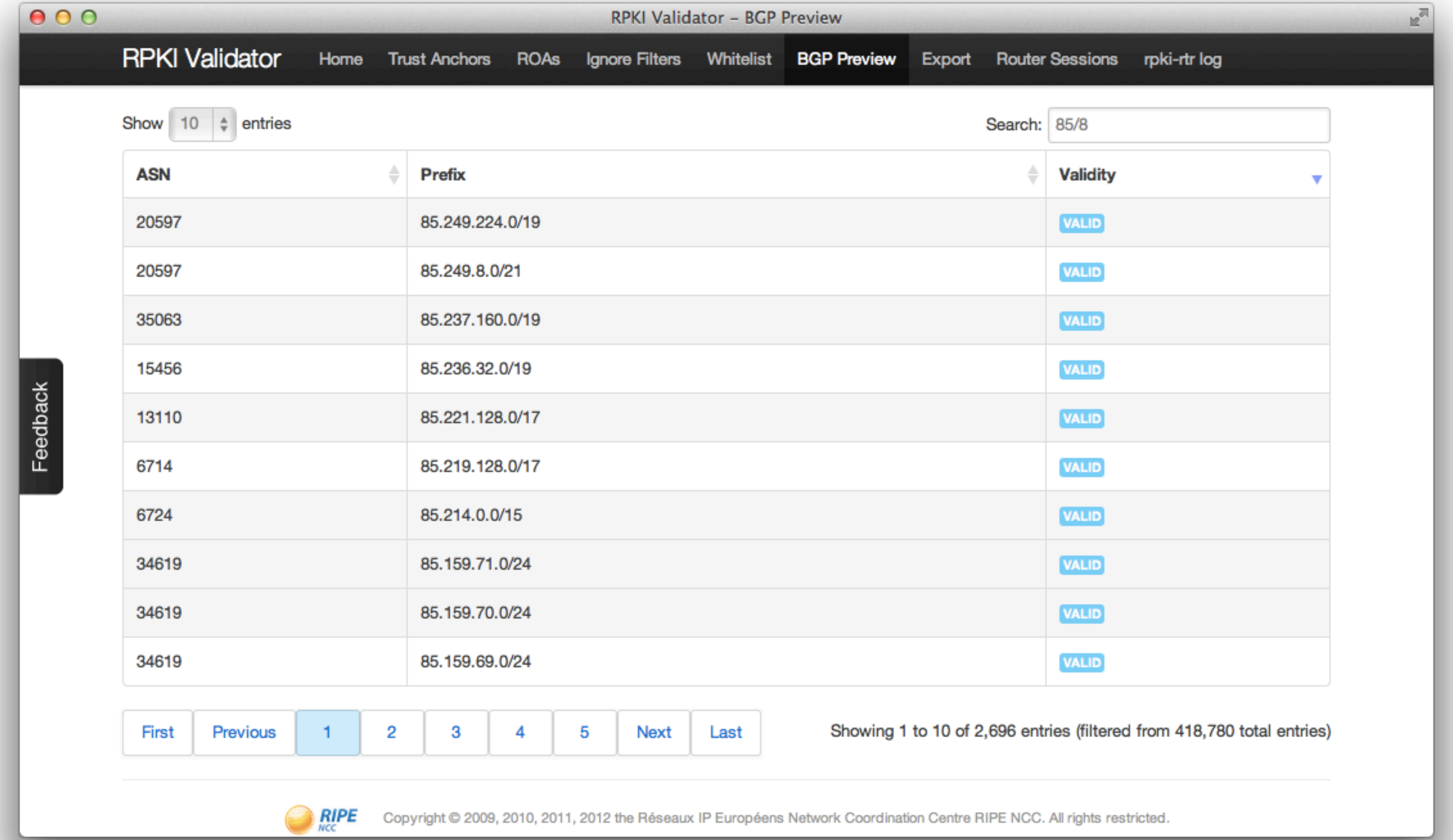
RIPE NCC RPKI-RTR Validator



Quick overview of BGP Origin validation

Trust Anchors are the entry points used for validation in any Public Key Infrastructure (PKI) system. This validator is intended for the validation of Resource PKI (RPKI) systems. It is pre-configured with Trust Anchors for four RIRs who are running such systems now.

RIPE NCC RPKI Validator 2.3



Show 10 entries

Search: 85/8

ASN	Prefix	Validity
20597	85.249.224.0/19	VALID
20597	85.249.8.0/21	VALID
35063	85.237.160.0/19	VALID
15456	85.236.32.0/19	VALID
13110	85.221.128.0/17	VALID
6714	85.219.128.0/17	VALID
6724	85.214.0.0/15	VALID
34619	85.159.71.0/24	VALID
34619	85.159.70.0/24	VALID
34619	85.159.69.0/24	VALID

Showing 1 to 10 of 2,696 entries (filtered from 418,780 total entries)

RPKI support in routers

- The RPKI-RTR Protocol is an IETF standard
- Production Cisco Support:
  - ASR1000, 7600, ASR903 and ASR901
    in releases 15.2(1)S or XE 3.5
- Cisco Early Field Trial (EFT):
  - ASR9000, CRS1, CRS3 and c12K (IOS-XR)
- Juniper planning support in 12.2 (Q3 2012)
- Quagga has support through BGP-SRX

Router Configuration – Cisco

```
!
route-map rpki-loc-pref permit 10
 match rpki invalid
 set local-preference 90
!
route-map rpki-loc-pref permit 20
 match rpki not-found
 set local-preference 100
!
route-map rpki-loc-pref permit 30
 match rpki valid
 set local-preference 110
```

Public Testbeds

- RIPE NCC has a Cisco:
  - Telnet to rpki-rtr.ripe.net
  - Username: ripe, no password
- Netsign has a Juniper:
  - Telnet to juniper.rpki.netsign.net
  - Username: rpki, password: testbed

- http://ripe.net/certification/router-configuration

RPKI Webinars

NEW

- One hour online session
- Theory and practical examples
- Live interaction
- Next session 5 June 2012
- Sign up now:

ripe.net/training/e-learning/webinars

Information and Announcements

http://ripe.net/certification

🐦 #RPKI

Questions?

✉ certification@ripe.net

✉ alexb@ripe.net

@alexander_band

RIPE NCC