Resource Certification

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

A RIPE NCC Activity Since 2006

- ripe-365 – RIPE NCC Activity Plan 2006
  - "The RIPE NCC will support its members and the Internet community to better secure the inter-domain routing system. As part of this support, the RIPE NCC will improve the quality of Internet number resource distribution data."
- ripe-364 - RIPE NCC Budget 2006
  - "the expenses for Membership Services show an increase due to the new activity to support routing security."

Digital Resource Certificates

- Based on open IETF standards (sidr)
  - RFC 5280: X.509 PKI Certificates
  - RFC 3779: Extensions for IP Addresses and ASNs

- Issued by the RIRs

- State that an Internet number resource has been registered by the RIPE NCC

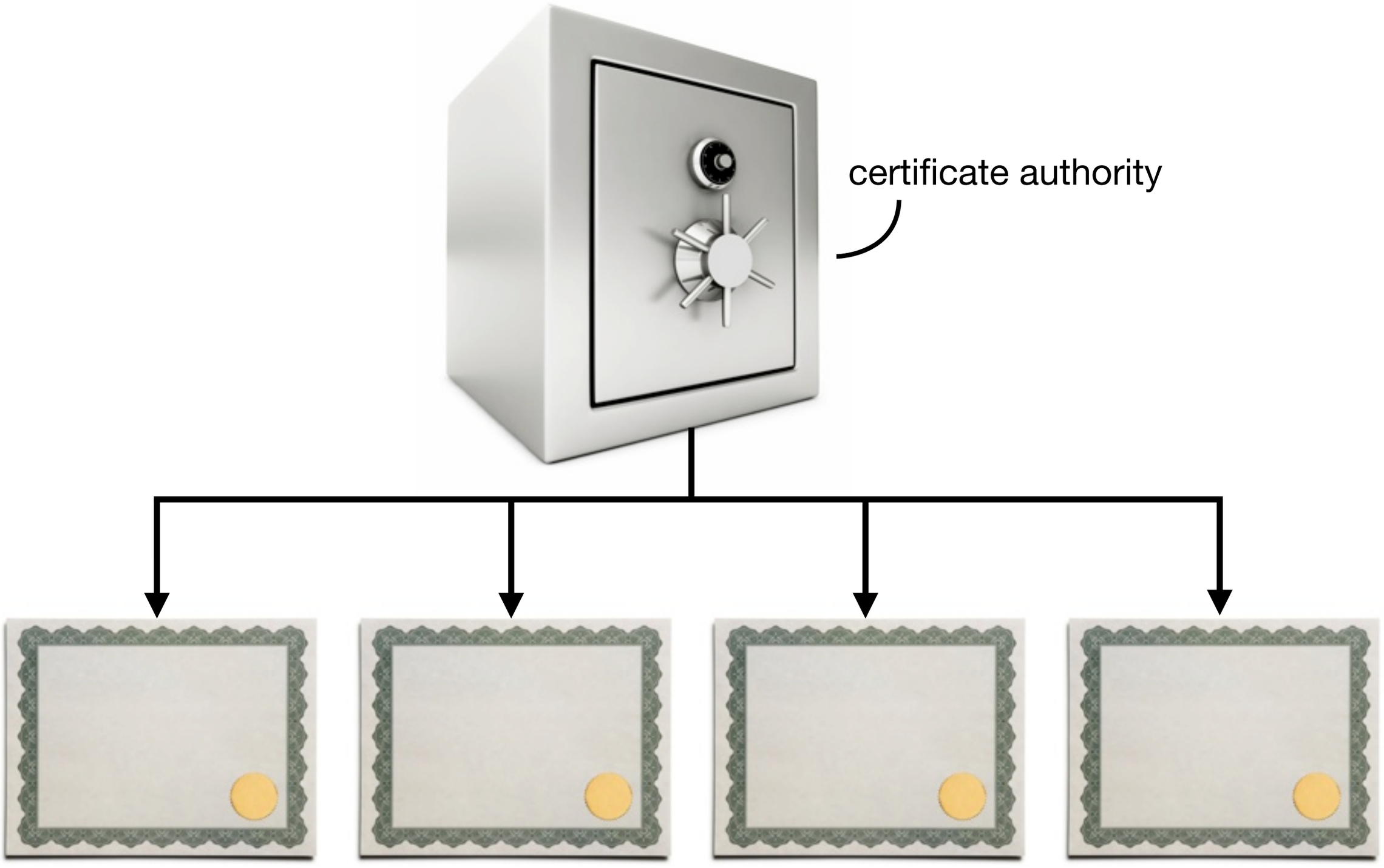
Digital Resource Certificates

- List only Provider Aggregatable address space
  - No Provider Independent, ERX, etc. yet
  - Do not list any identity information
- Automatically renewed every 12 months

The system

certificate authority

The system



Management

- RIPE NCC Hosted Platform
  - All processes are secured and automated
  - One click set-up of Resource Certificate
  - WebUI to manage ‘Route Origin Authorisations’ (ROAs)

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

  - A valid ROA can only be created by the legitimate holder of the IP address block

ROA Creation

Demo

LIR Portal
RIPE NCC

Resource Certification - ROA Specifications

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

- Logout
- General
- Billing
- Certification
- LIR Contacts
- IPv4
- IPv6
- ASN
- Request Forms
- Object Editors
- Tickets
- Training
- Tools
- Change Password
- X.509 PKI
- Events
- Glossary
- Contact

News | My Certified Resources | My ROA Specifications | History | RIPE NCC ROA Repository

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
RIPE NCC

Resource Certification - ROA Specification

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

- Logout
- General
- Billing
- Certification
- LIR Contacts
- IPv4
- IPv6
- ASN
- Request Forms
- Object Editors
- Tickets
- Training
- Tools
- Change Password
- X.509 PKI
- Events
- Glossary
- Contact

News | My Certified Resources | My ROA Specifications | History | RIPE NCC ROA Repository

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 Maximum length

Not valid before and/or after

Add ROA

My certified resources Search

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.

LIR Portal
RIPE NCC

Resource Certification - ROA Specification

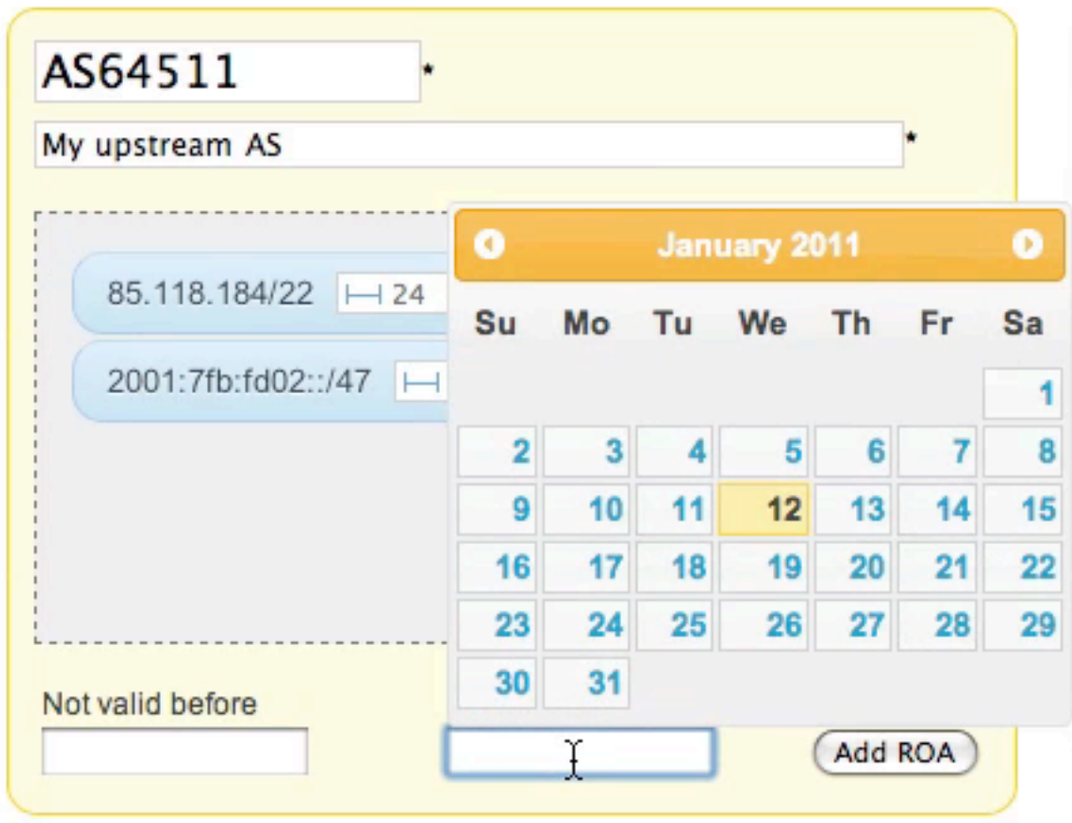
You are logged in as [nl.bluelight.alexb]

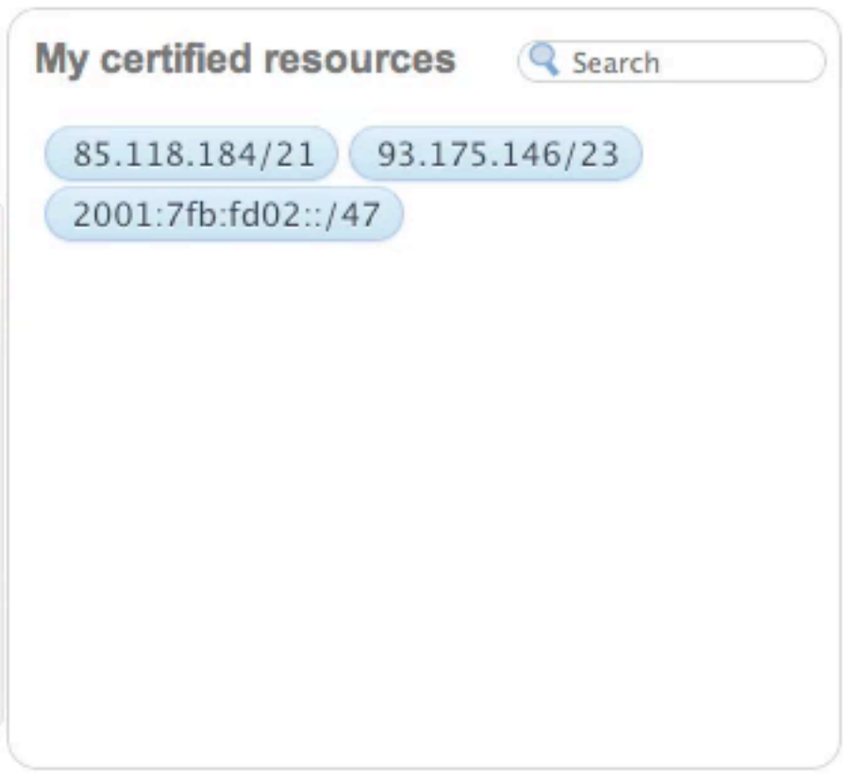
- Logout
- General
- Billing
- Certification
- LIR Contacts
- IPv4
- IPv6
- ASN
- Request Forms
- Object Editors
- Tickets
- Training
- Tools
- Change Password
- X.509 PKI
- Events
- Glossary
- Contact

News | My Certified Resources | My ROA Specifications | History | RIPE NCC ROA Repository

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:





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.

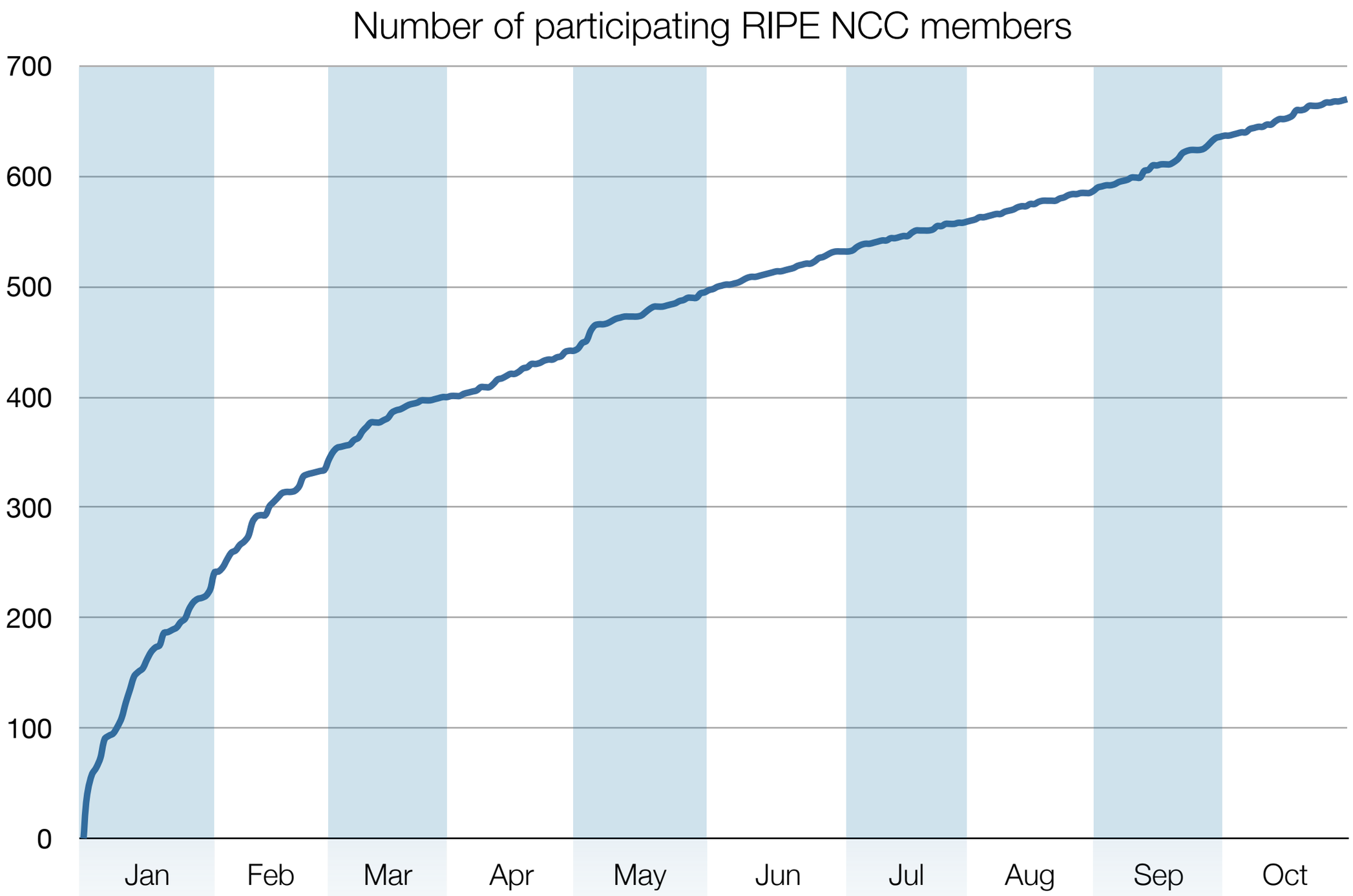
Search:

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

- Each RIR has a public repository
  - Holds certificates, ROAs, CRLs and manifests
  - Refreshed at least every 24 hrs
- Accessed using a Validation tool
  - Finds repository using a
    Trust Anchor Locator (TAL)
  - Communication via rsync
  - Builds up a local validated cache

Adoption


Number of participating RIPE NCC members
700
600
500
400
300
200
100
0
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct

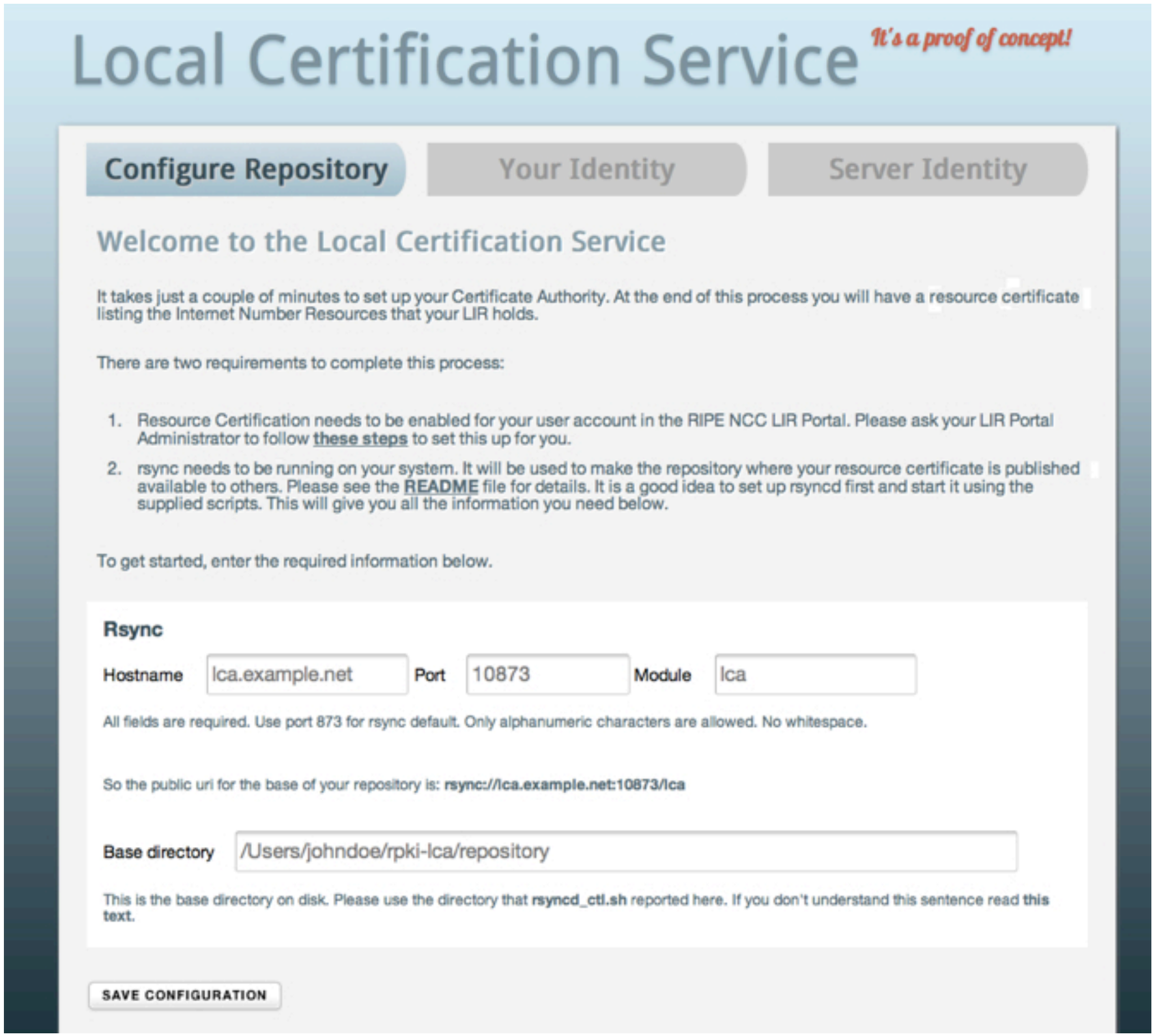
Non-Hosted Software

RIPE NCC Local Certificate Authority (LCA)

- Generate your own key pair
  - Secure interface with RIPE NCC parent system
- No dependency on LIR Portal for management
  - Runs as service, Local Web UI
- Publish crypto objects yourself

Open source, BSD License

Easy Setup and Configuration



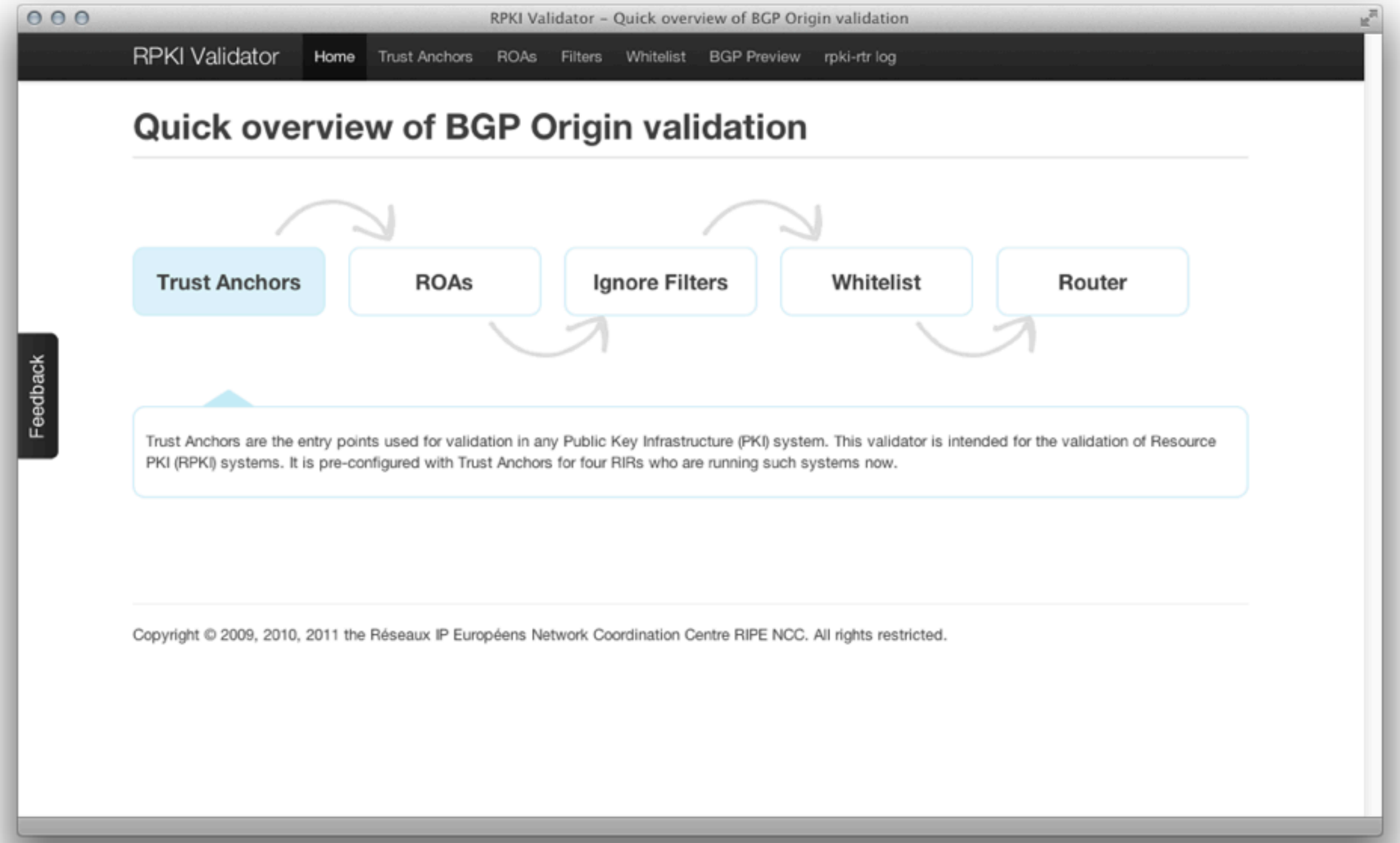
RIPE NCC RPKI Validation tool

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



RIPE NCC RPKI-RTR Validator

RPKI Validator – Quick overview of BGP Origin validation

RPKI Validator | Home | Trust Anchors | ROAs | Filters | Whitelist | BGP Preview | rpki-rtr log

Validated ROAs

Validated ROAs from **APNIC RPKI Root**, **AfriNIC RPKI Root**, **LACNIC RPKI Root**, **RIPE NCC RPKI Root**.

Download validated ROAs as CSV

Show 10 entries Search: 85/8

ASN	Prefix	Maximum Length	Trust Anchor
1126	85.90.64.0/19	19	RIPE NCC RPKI Root
3303	85.0.0.0/13	24	RIPE NCC RPKI Root
6714	85.219.128.0/17	17	RIPE NCC RPKI Root
6724	85.214.0.0/15	16	RIPE NCC RPKI Root
9146	85.92.224.0/19	21	RIPE NCC RPKI Root
13110	85.221.128.0/17	24	RIPE NCC RPKI Root
13301	85.14.192.0/18	24	RIPE NCC RPKI Root
15456	85.236.32.0/19	19	RIPE NCC RPKI Root
15527	85.157.0.0/16	16	RIPE NCC RPKI Root
31549	85.15.0.0/18	24	RIPE NCC RPKI Root

RPKI-Router Integration

- Local Validator Tool feeds RPKI capable router with processed data set
  - Router does not do the crypto!

- Set router prefs based on three RPKI states of a route announcement:
  - VALID: ROA found, authorised announcement
  - INVALID: ROA found, unauthorised announcement
  - UNKNOWN: No ROA found (resource not yet signed)

Information and Announcements

http://ripe.net/certification

#RPKI

Questions?

alexb@ripe.net

alexander_band

linkedin.com/in/alexanderband

RIPE NCC