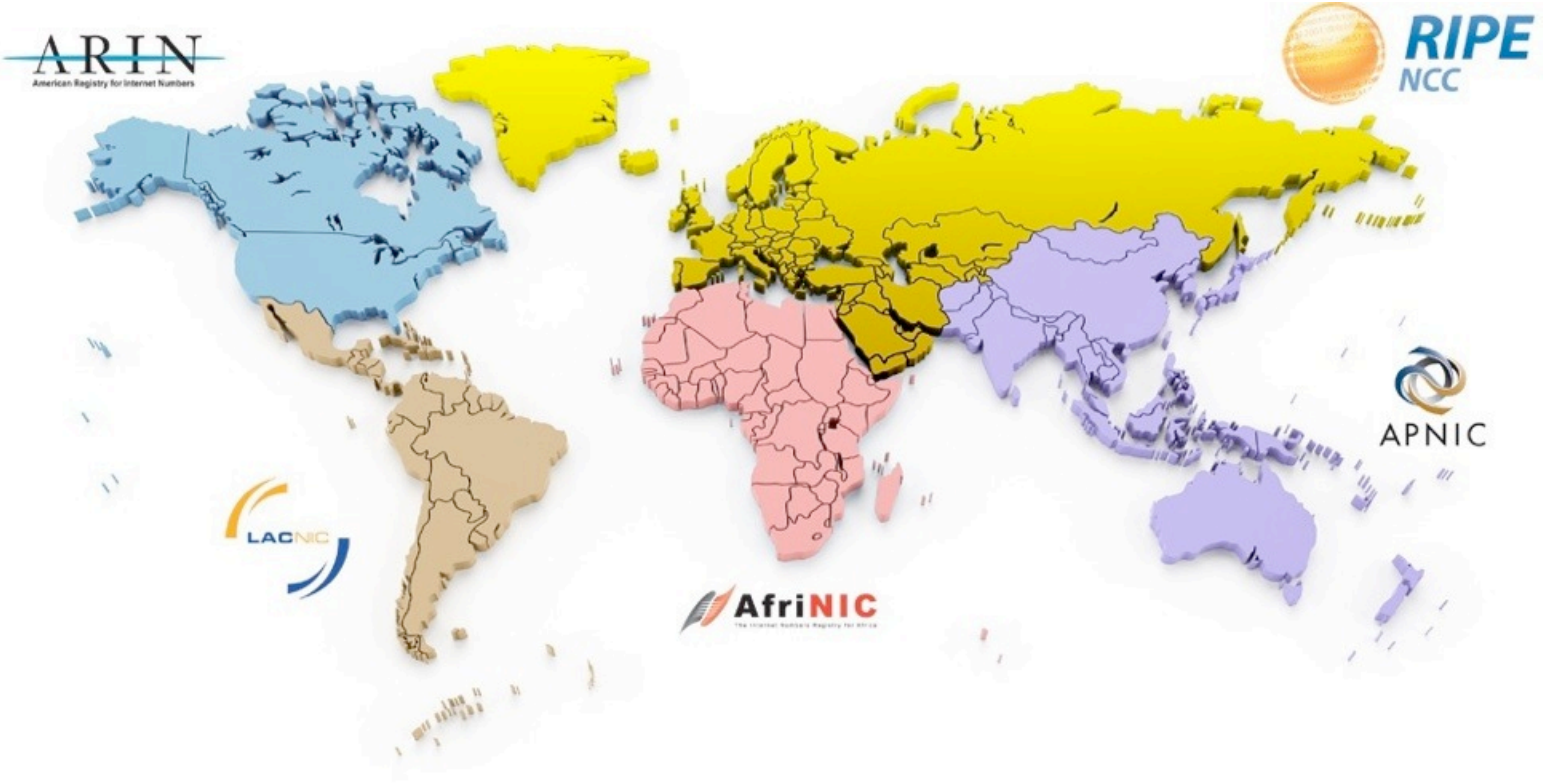
Resource Certification

Alex Band – Product Manager
ENOG, Moscow

The RIPE NCC


ARIN
American Registry for Internet Numbers
RIPE NCC
APNIC
LACNIC
AfriNIC
The Internet Numbers Registry for Africa

The RIPE NCC

- 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

Internet Routing Today

- Routing is non-hierarchical, open and free
- Freedom comes at a price:
  - You can announce any address block on your router
  - Accidental errors happen frequently, impact is high
    - Entire networks become unavailable
  - Malicious attacks are relatively easy
    - Mitigation requires intervention from operators
- IPv4 address depletion may intensify issue

What is “Internet Routing Registry”

- Distributed databases with public routing policy information, mirroring each other: irr.net
    - APNIC, RADB, Level3, SAVVIS...
- RIPE NCC operates “RIPE Routing Registry”
- Big operators make use of it
    - AS286 (KPN), AS5400 (BT), AS1299 (Telia), AS8918 (Carrier1), AS2764 (Connect), AS3561 (Savvis), AS3356 (Level 3)...

RIPE Database

- Public Internet resources database

- All your objects are already there:
  - Address space: inetnum & inet6num
  - AS Number: aut-num
  - Contact details: person, role, organisation,
  - Strong protection: maintainer (key-cert, irt)

Resource Certificates – The Goal

- Issue digital certificates along with the allocation of Internet Resources

- Two main purposes:
  - Make Internet routing more secure
  - Make the Registry more robust

- Validation is the added value

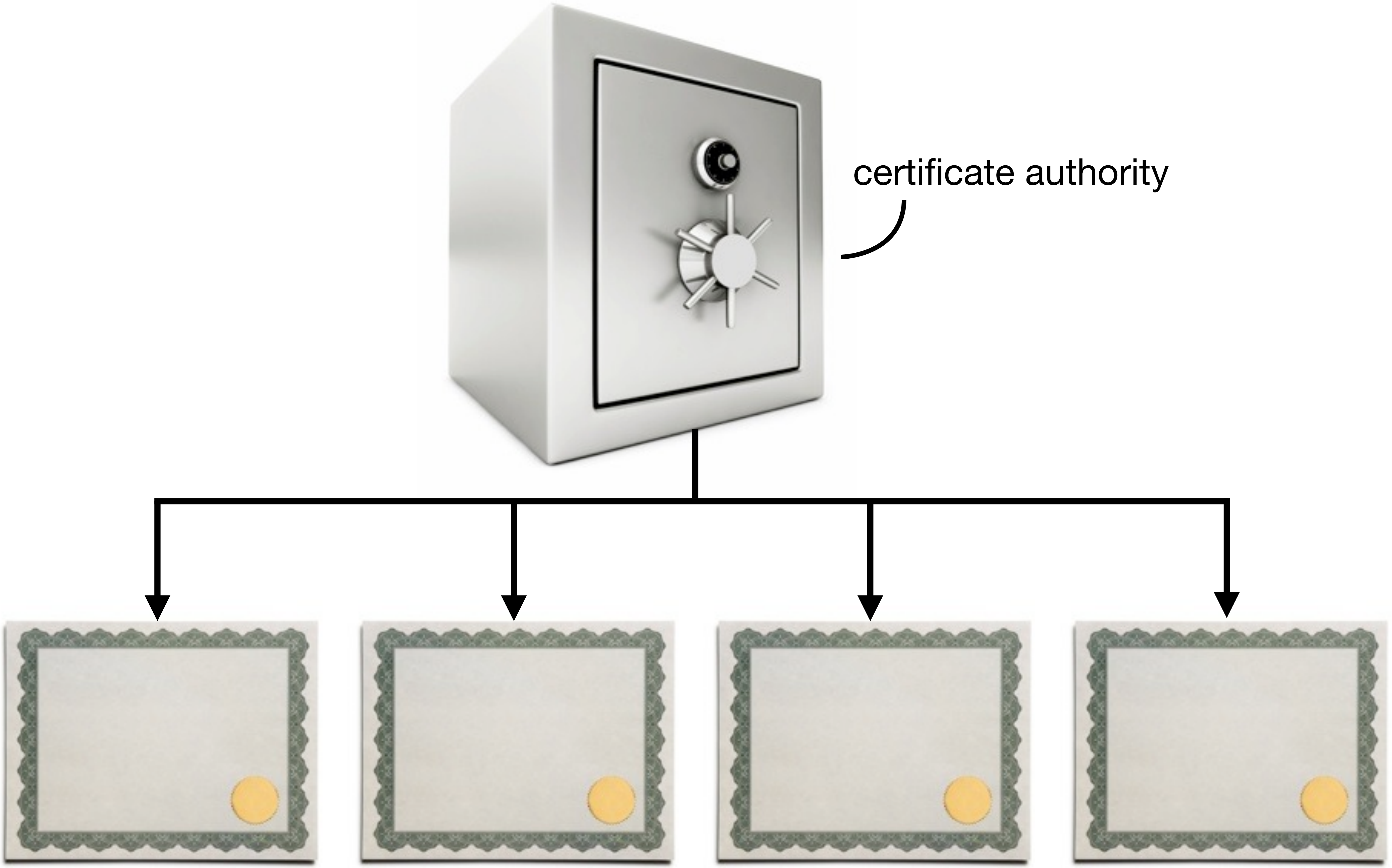
Digital Resource Certificates

- 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

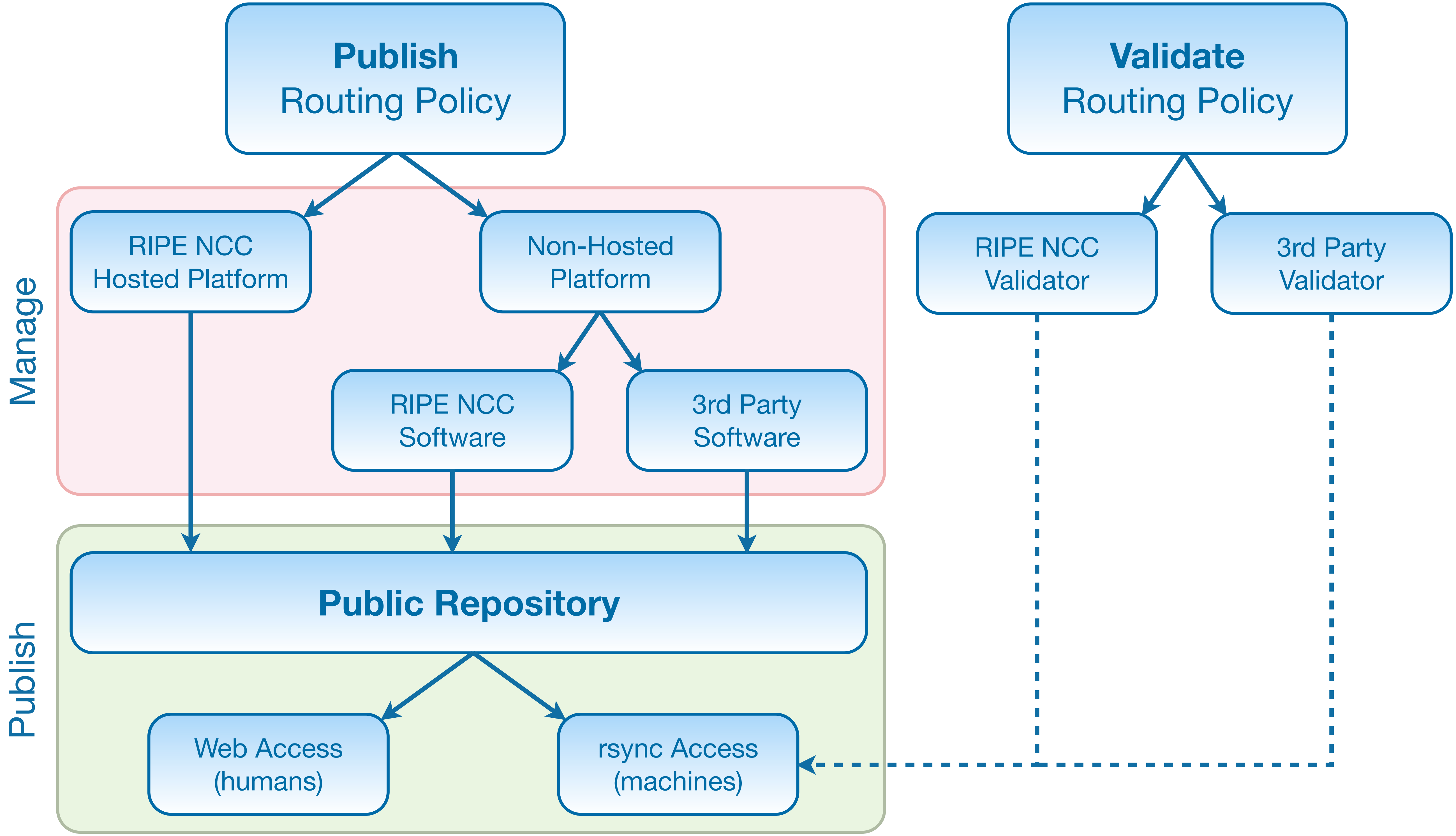
Digital Resource Certificates

- 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



Using Certification to Secure Internet Routing



Our Mission

- Quality
  - Reliability and security of the platform are key
  - Received highest possible rating in independent audit

TÜViT®
2011 Trusted Product
Voluntary Validation
© 2011 TÜViT GmbH - Member of TÜV NORD Group

- Usability
  - 1-Click set-up of Certificate Authority
  - Easy drag and drop creation of ROAs
  - All crypto operations handled by 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)

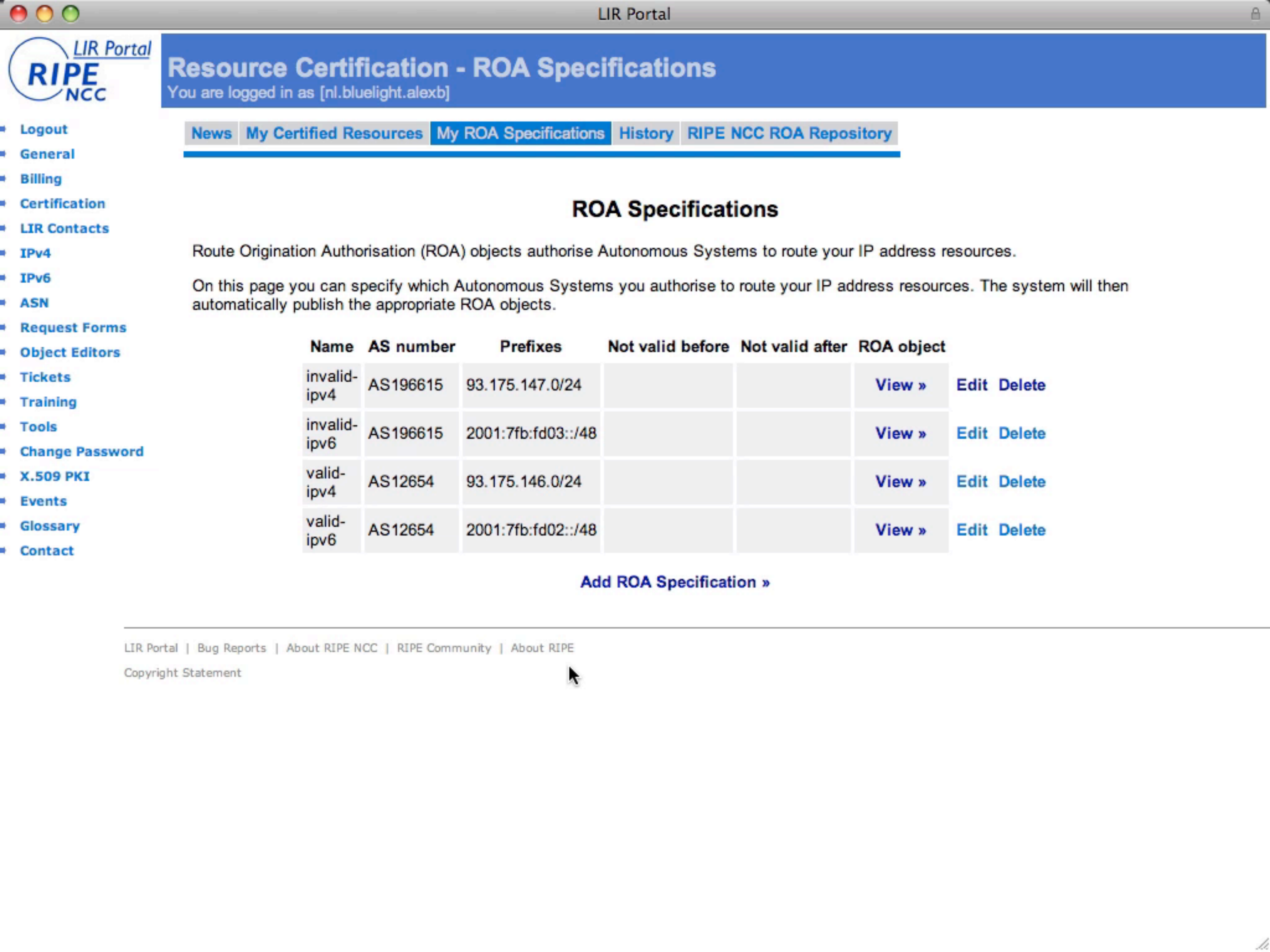
“I authorise this Autonomous System
to originate these IP prefixes”

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

ROA Considerations

- ROAs have a ‘maximum length’ option
  - Authorises AS to deaggregate to the point you specify
  - When not set, AS may only announce the whole prefix
    - A more specific announcement will be invalid
- Before issuing a ROA for an address block
  - Ensure that any sub-allocations announced by others (e.g. customers) have ROAs in play
  - Otherwise, the announcements of sub-allocations with no ROAs will be invalid

ROA Creation Demo



Resource Certification - ROA Specifications

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

ROA Specifications

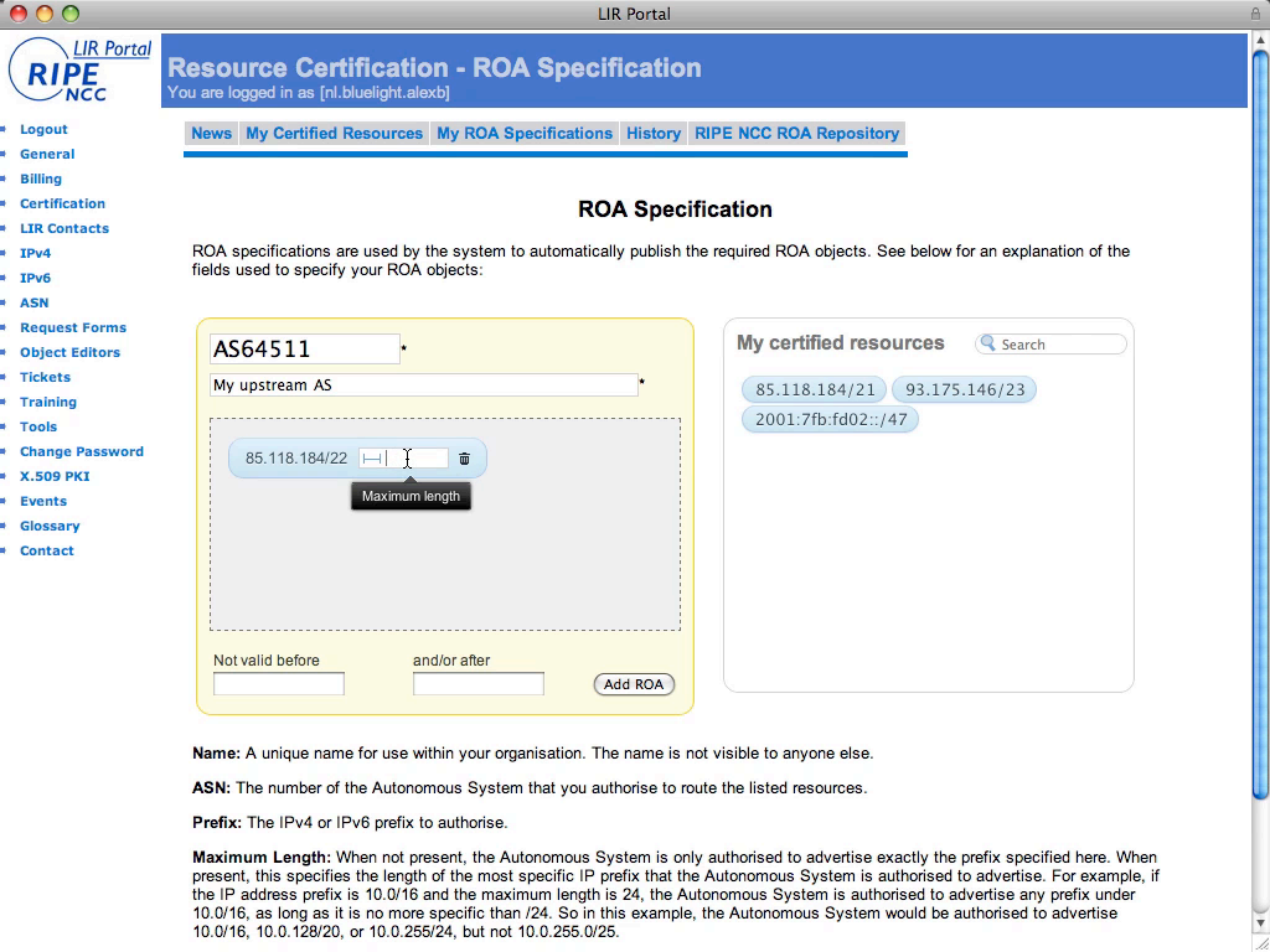
Route Origination Authorisation (ROA) objects authorise Autonomous Systems to route your IP address resources.

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

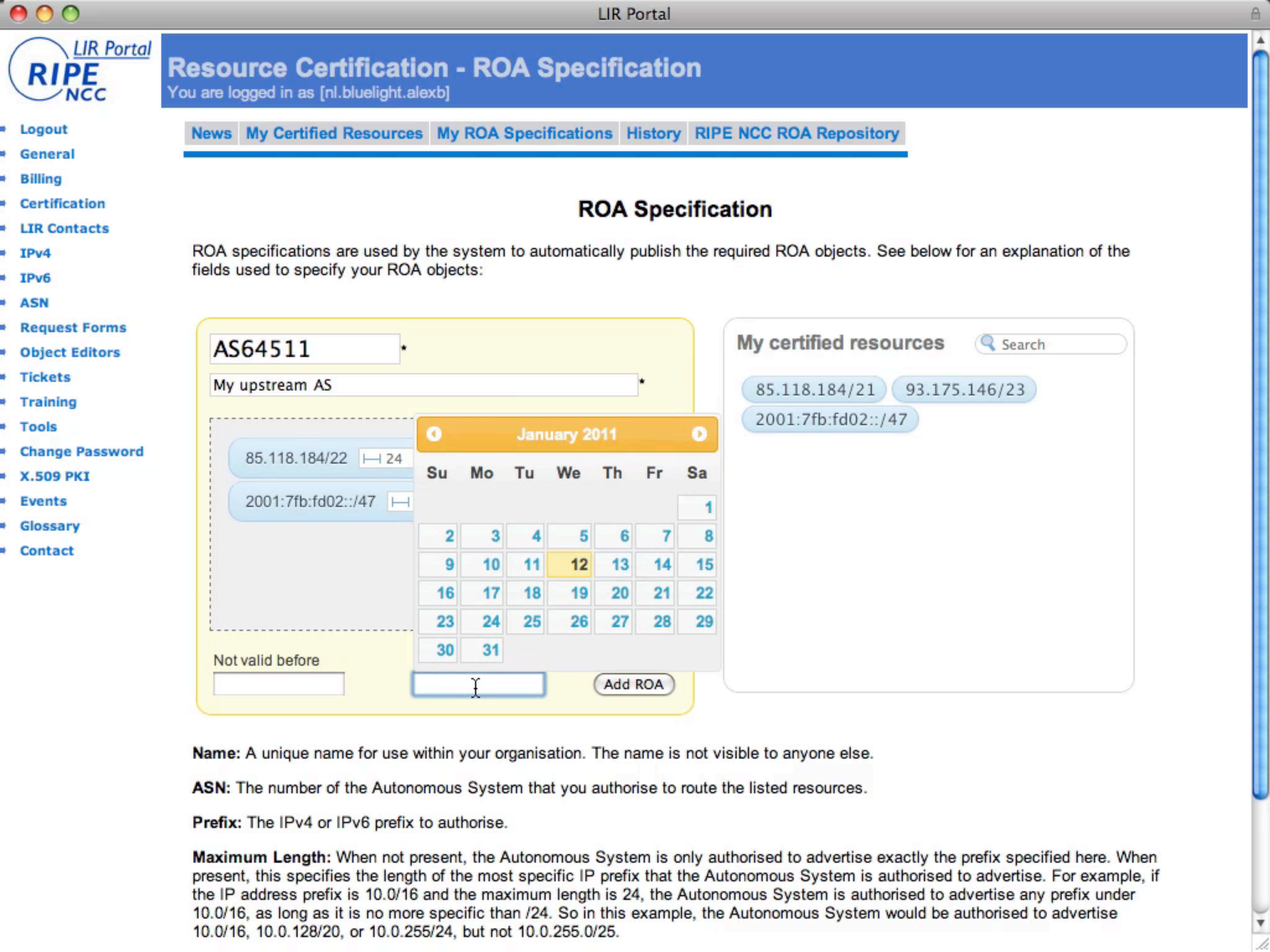
2001:7fb:fd02::/47

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

January 2011

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

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.

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

Software Validation of Certificates and ROAs

- Three software tools available
  - RIPE NCC Validator
    - Easy to set-up and use, limited feature set
  - rcynic
  - BBN Relying Party Software
    - Complex set-up, but more options and flexibility

- http://ripe.net/certification/validation

BGPmon ROA validation service

- Relies heavily on RIPE NCC Validator

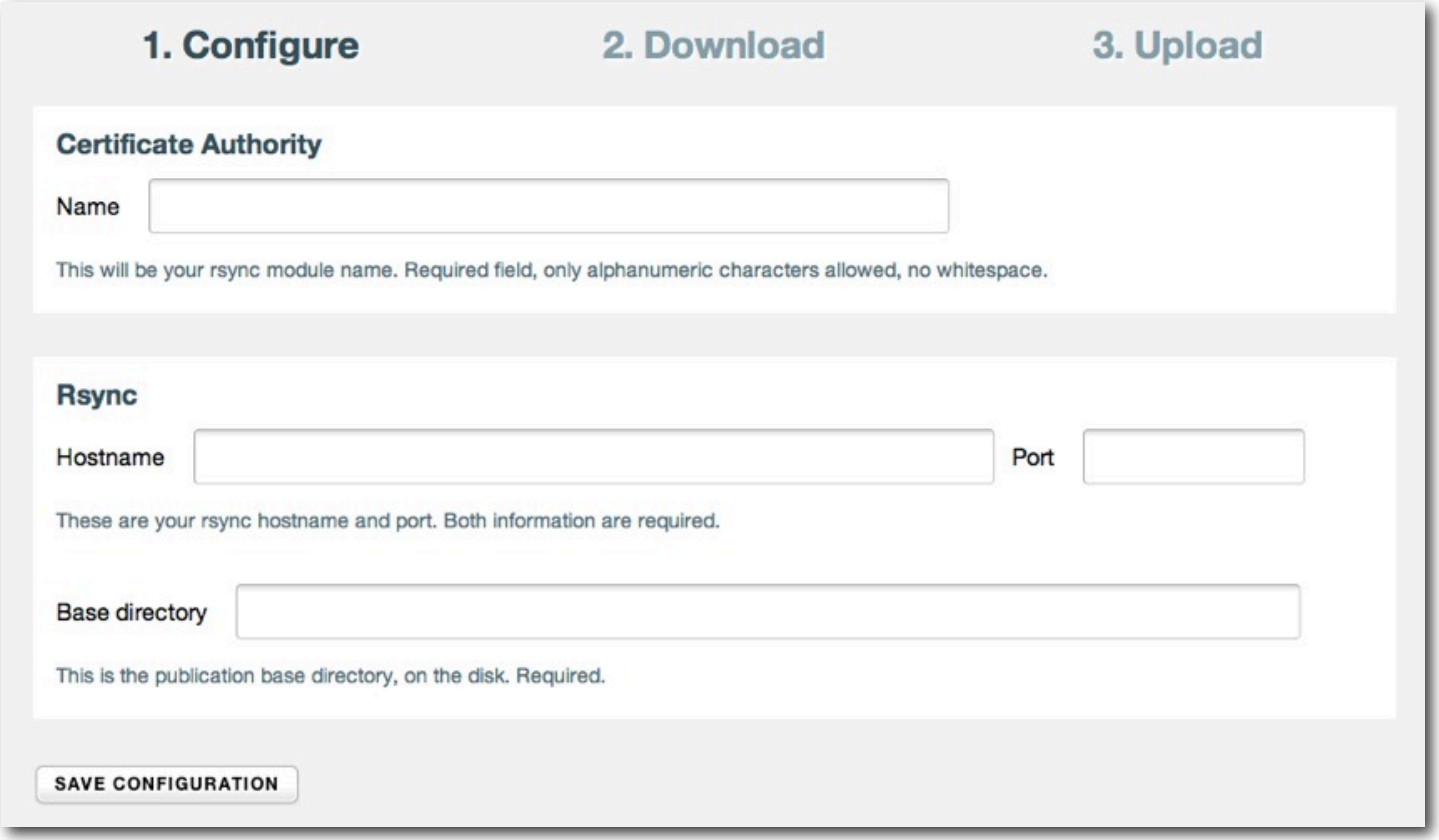
```
$ whois -h whois.bgpmon.net 80.242.128.0
Prefix:              80.242.128.0/19
Prefix description:  MAIN-Route for our allocation 80-242-128-0---slash19
Country code:        DE
Origin AS:           21501
Origin AS Name:      MAINLAB-AS Autonomous System Mainlab GmbH, Germany
RPKI status:         ROA validation successful


$ whois -h whois.bgpmon.net " --roa 21501 80.242.128.0/19"
0 - Valid
------------------------
ROA Details
------------------------
Origin ASN:       AS21501
Not valid Before: 2011-02-02 00:05:57
Not valid After:  2012-07-01 00:00:00
Trust Anchor:     rpki.ripe.net
Prefixes:         46.22.32.0/20
                  80.242.128.0/19
                  89.19.224.0/19
                  2001:830::/32
```

Q1/Q2: Support for Non-Hosted System

- Build secure authentication for LIRs
- Implement the up/down protocol
  - Allows to run your own Certificate Authority
    - Requirement for ARIN to launch
- Test interoperability with 3rd party solutions
- Release RIPE NCC client software
  - Pilot program: contact us if you want to participate
  - Open source, BSD license

Non-Hosted Software Demo

Basic Configuration



1. Configure

2. Download

3. Upload

Certificate Authority

Name

This will be your rsync module name. Required field, only alphanumeric characters allowed, no whitespace.

Rsync

Hostname

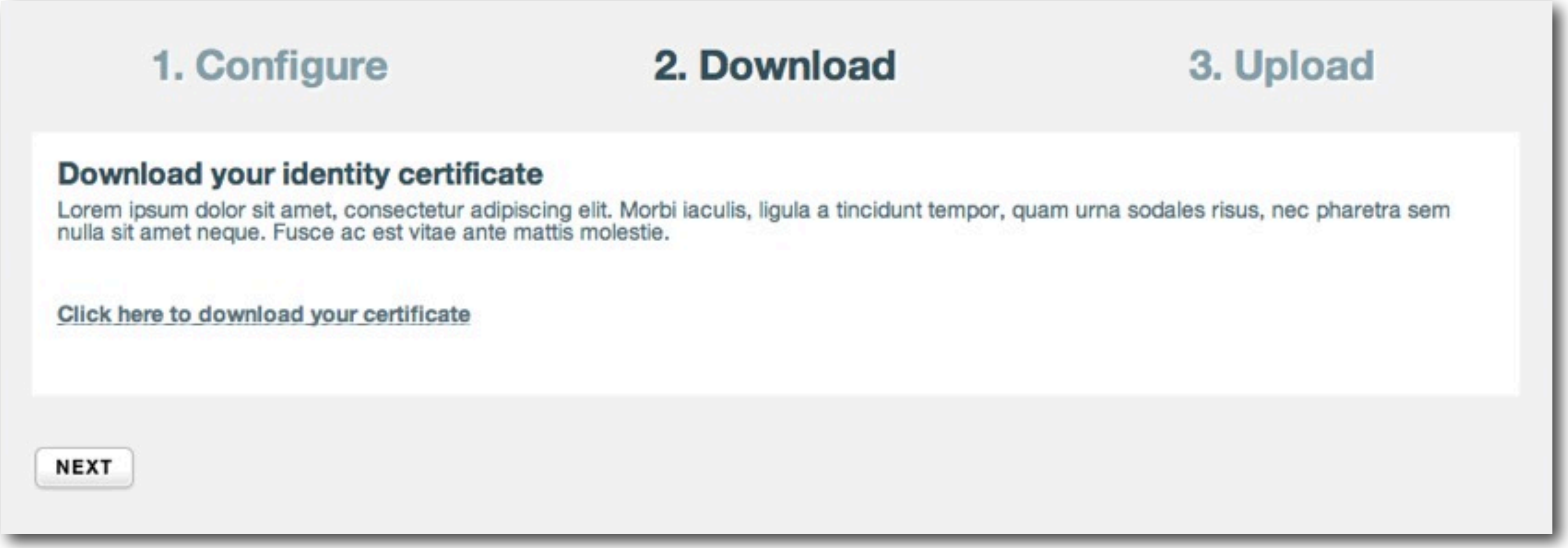
Port

These are your rsync hostname and port. Both information are required.

Base directory

This is the publication base directory, on the disk. Required.

Download Identity Certificate

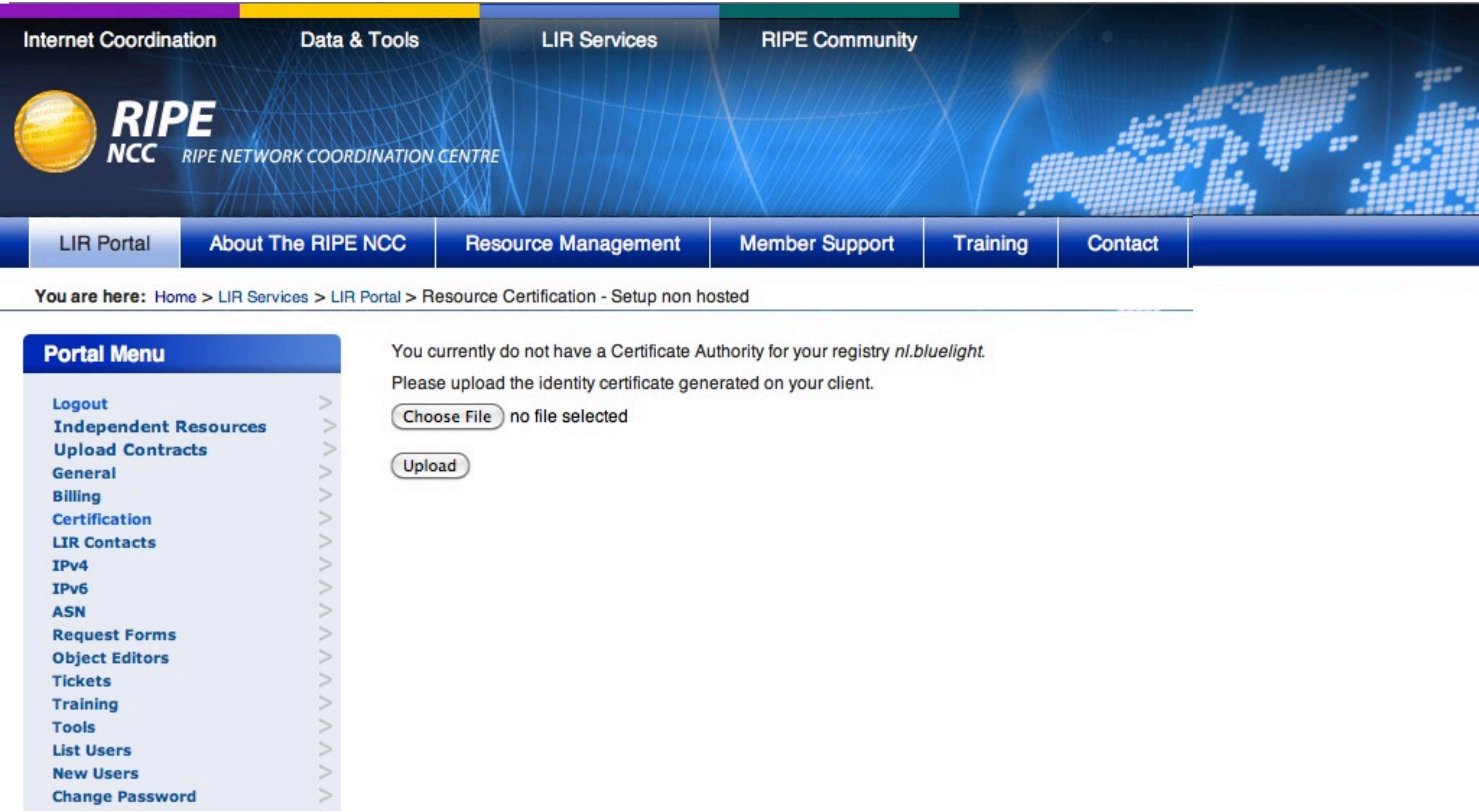


Download your identity certificate

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi iaculis, ligula a tincidunt tempor, quam urna sodales risus, nec pharetra sem nulla sit amet neque. Fusce ac est vitae ante mattis molestie.

Click here to download your certificate

Upload Client Identity Certificate to Portal



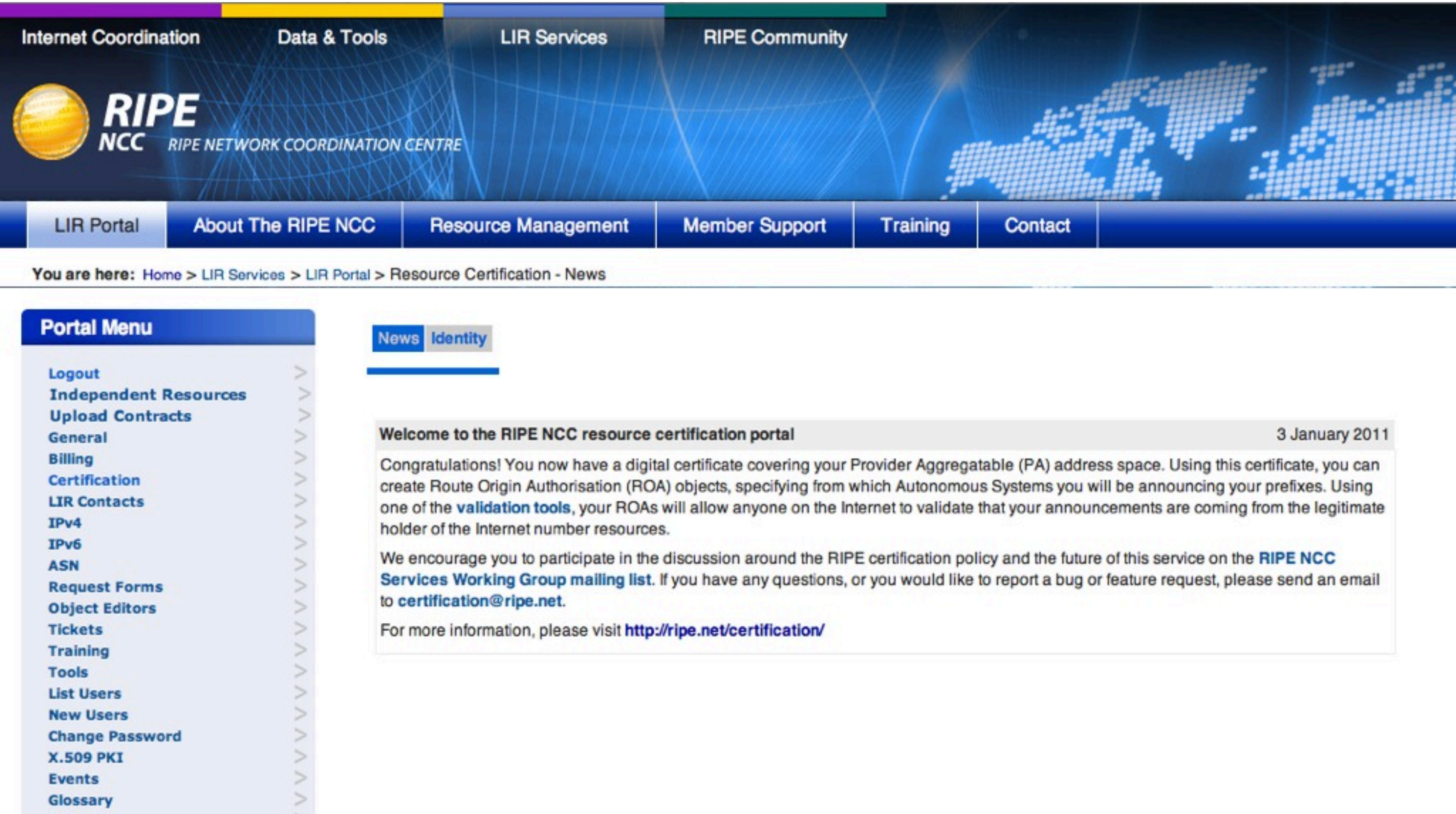
You are here: Home > LIR Services > LIR Portal > Resource Certification - Setup non hosted

You currently do not have a Certificate Authority for your registry *nl.bluelight*.

Please upload the identity certificate generated on your client.

no file selected

Upload succeeded...



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

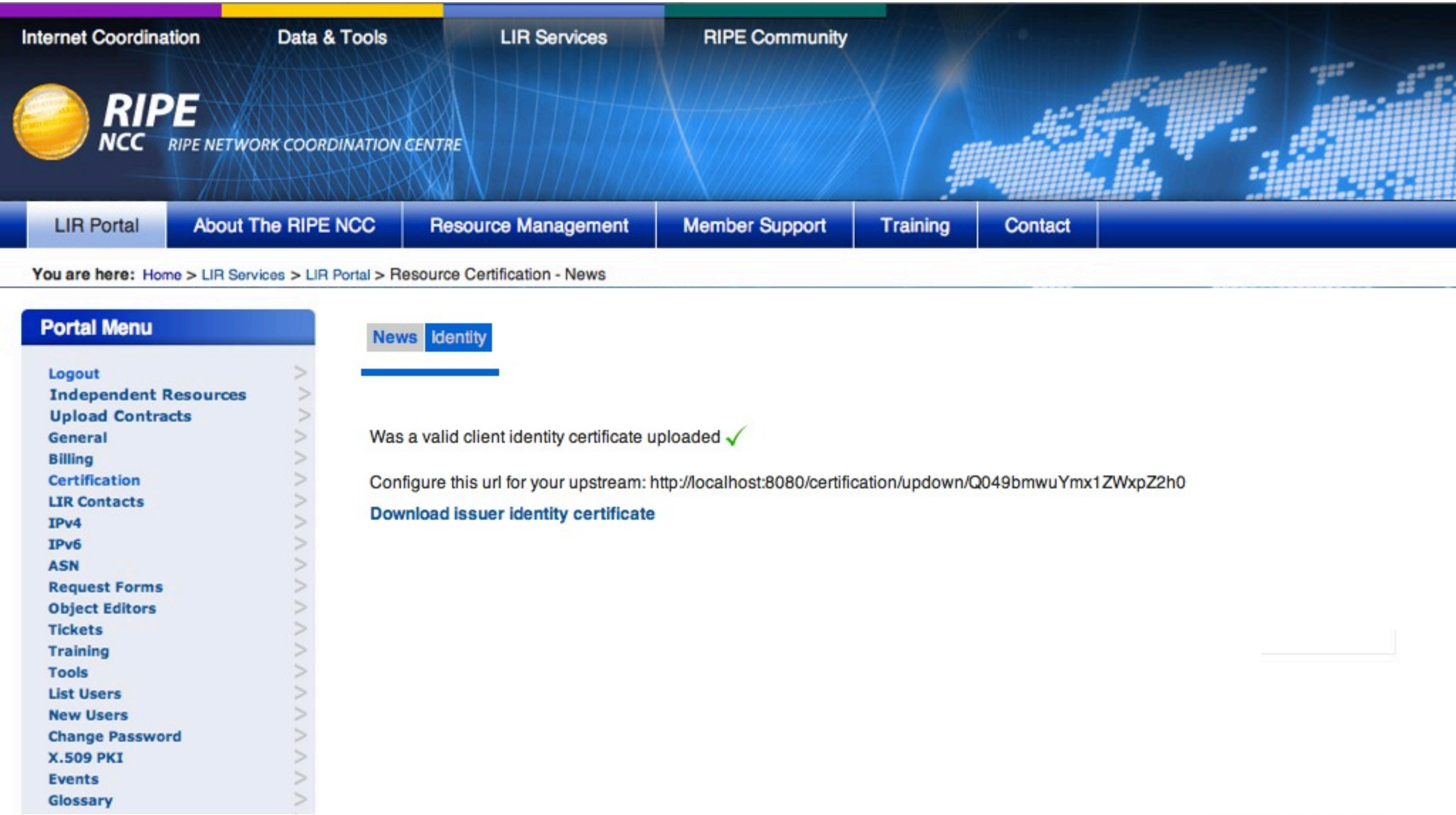
Welcome to the RIPE NCC resource certification portal 3 January 2011

Congratulations! You now have a digital certificate covering your Provider Aggregatable (PA) address space. Using this certificate, you can create Route Origin Authorisation (ROA) objects, specifying from which Autonomous Systems you will be announcing your prefixes. Using one of the **validation tools**, your ROAs will allow anyone on the Internet to validate that your announcements are coming from the legitimate holder of the Internet number resources.

We encourage you to participate in the discussion around the RIPE certification policy and the future of this service on the **RIPE NCC Services Working Group mailing list**. If you have any questions, or you would like to report a bug or feature request, please send an email to **certification@ripe.net**.

For more information, please visit **http://ripe.net/certification/**

Download Issuer Identity Certificate

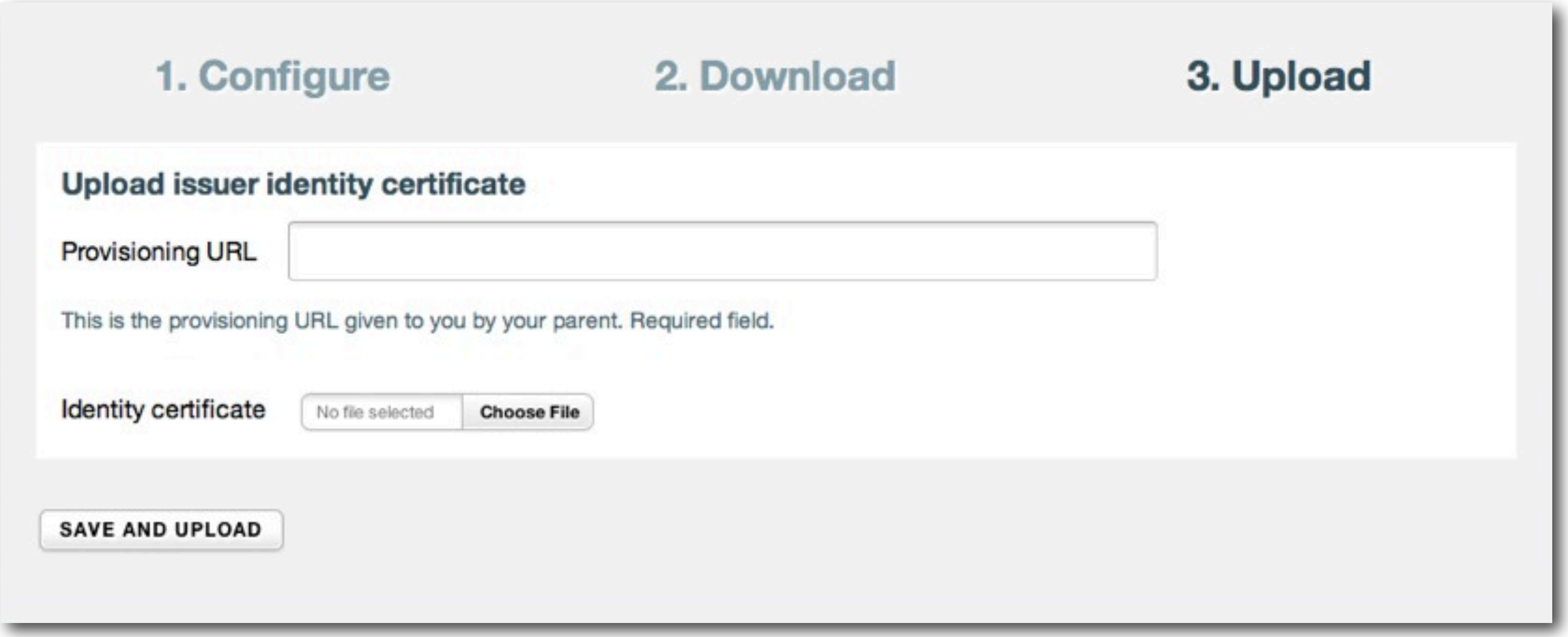


Was a valid client identity certificate uploaded ✓

Configure this url for your upstream: http://localhost:8080/certification/updown/Q049bmwuYmx1ZWxpZ2h0

Download issuer identity certificate

Upload Issuer Identity Certificate



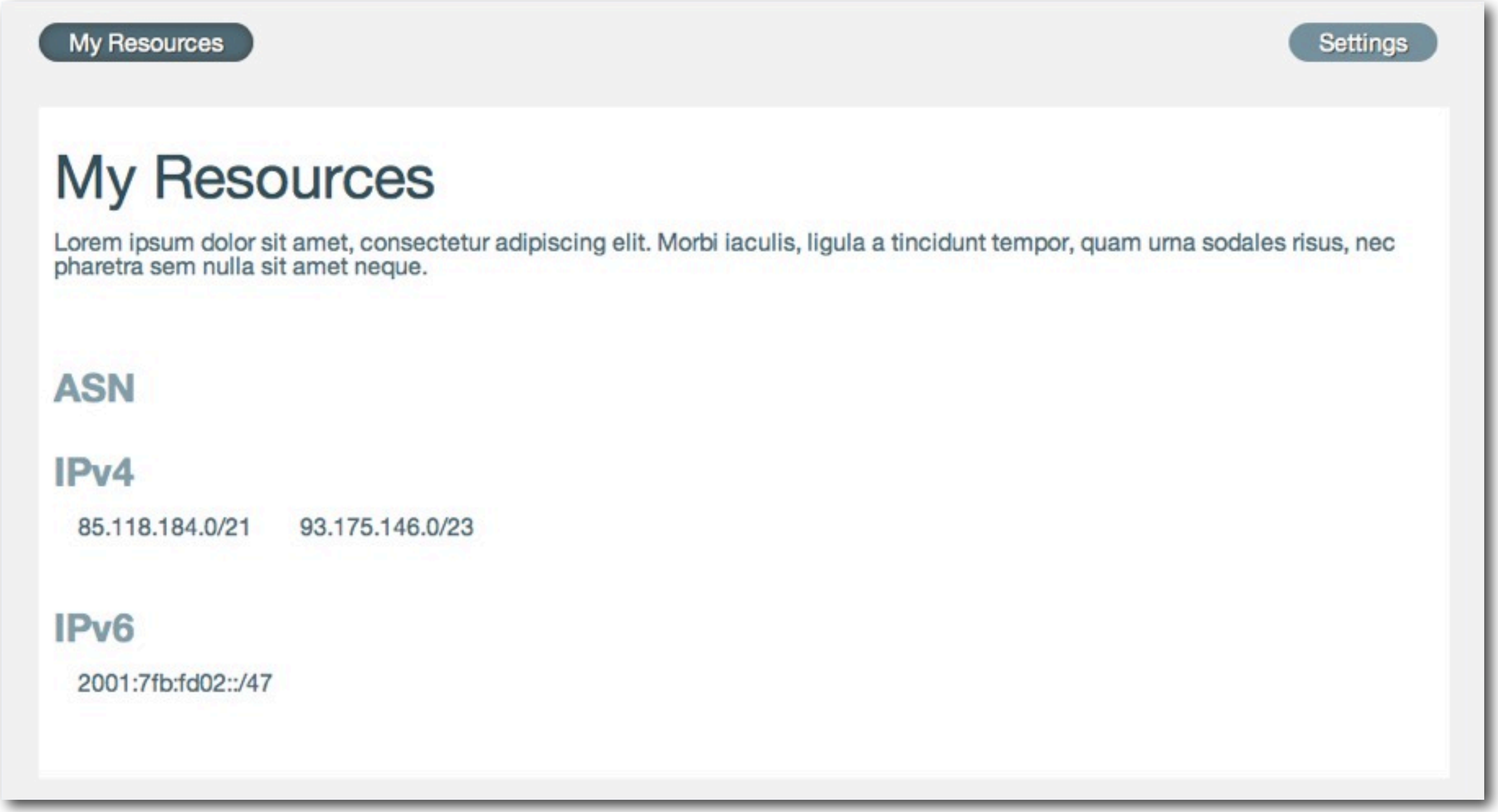
Upload issuer identity certificate

Provisioning URL

This is the provisioning URL given to you by your parent. Required field.

Identity certificate: No file selected

Only resources listed for your registry...



My Resources

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi iaculis, ligula a tincidunt tempor, quam urna sodales risus, nec pharetra sem nulla sit amet neque.

ASN

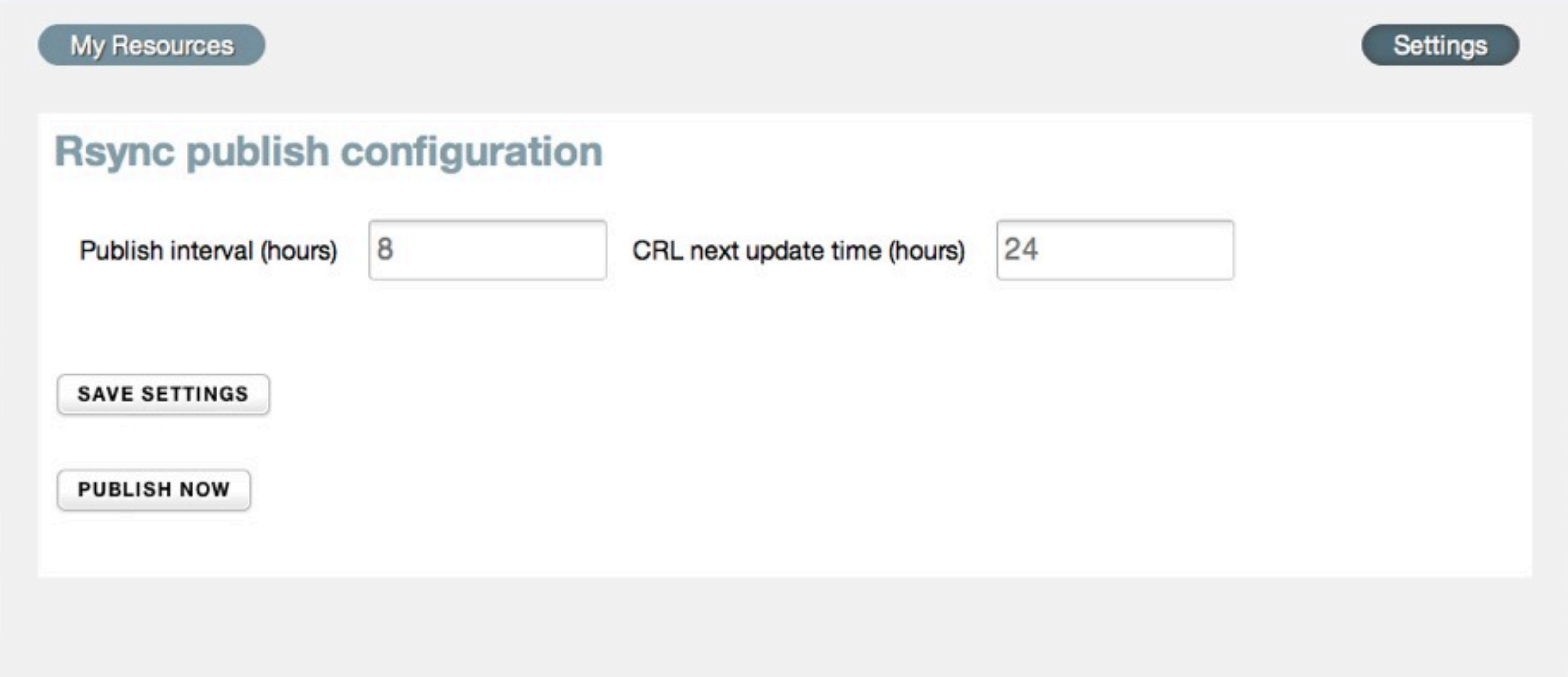
IPv4

85.118.184.0/21   93.175.146.0/23

IPv6

2001:7fb:fd02::/47

Configure Settings



Rsync publish configuration

Publish interval (hours): 8

CRL next update time (hours): 24

Q2: Data Quality and Integrity

- Use RIS Route Collectors to support Certification
  - Suggest ROAs based on real-world routing
  - Trigger alert to creator of ROA when:
    - More specific prefix announced from authorised AS
    - More specific prefix announced from different AS
    - Prefix for which a ROA exists is no longer announced

Q2/Q3: Validation, Toolset

- Expand current Validator
  - Background caching
  - Web-based User Interface
  - Scripting support (Perl, Python, etc.)
  - Expose API
  - RPKI-Router Support...

Open source, BSD License!

Q2/Q3: Validation, Hardware Router Support

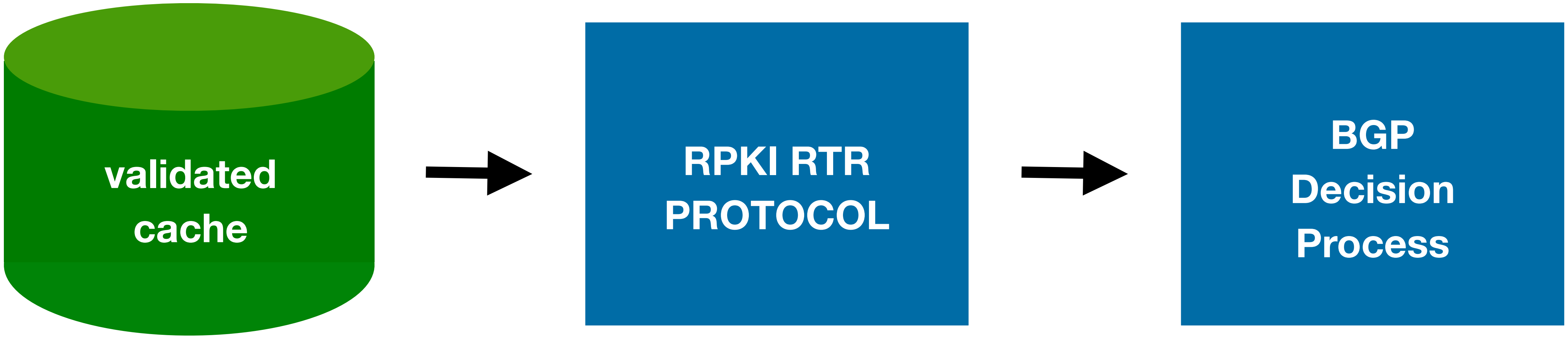
- Based on open IETF Standards: RPKI-RTR
  - Scheduled on Cisco roadmap for Q4, 2011
  - Juniper actively pursuing support as well

- RIPE NCC is actively working with Cisco to provide comprehensive open source toolset

Hardware Validation: RPKI-RTR Protocol

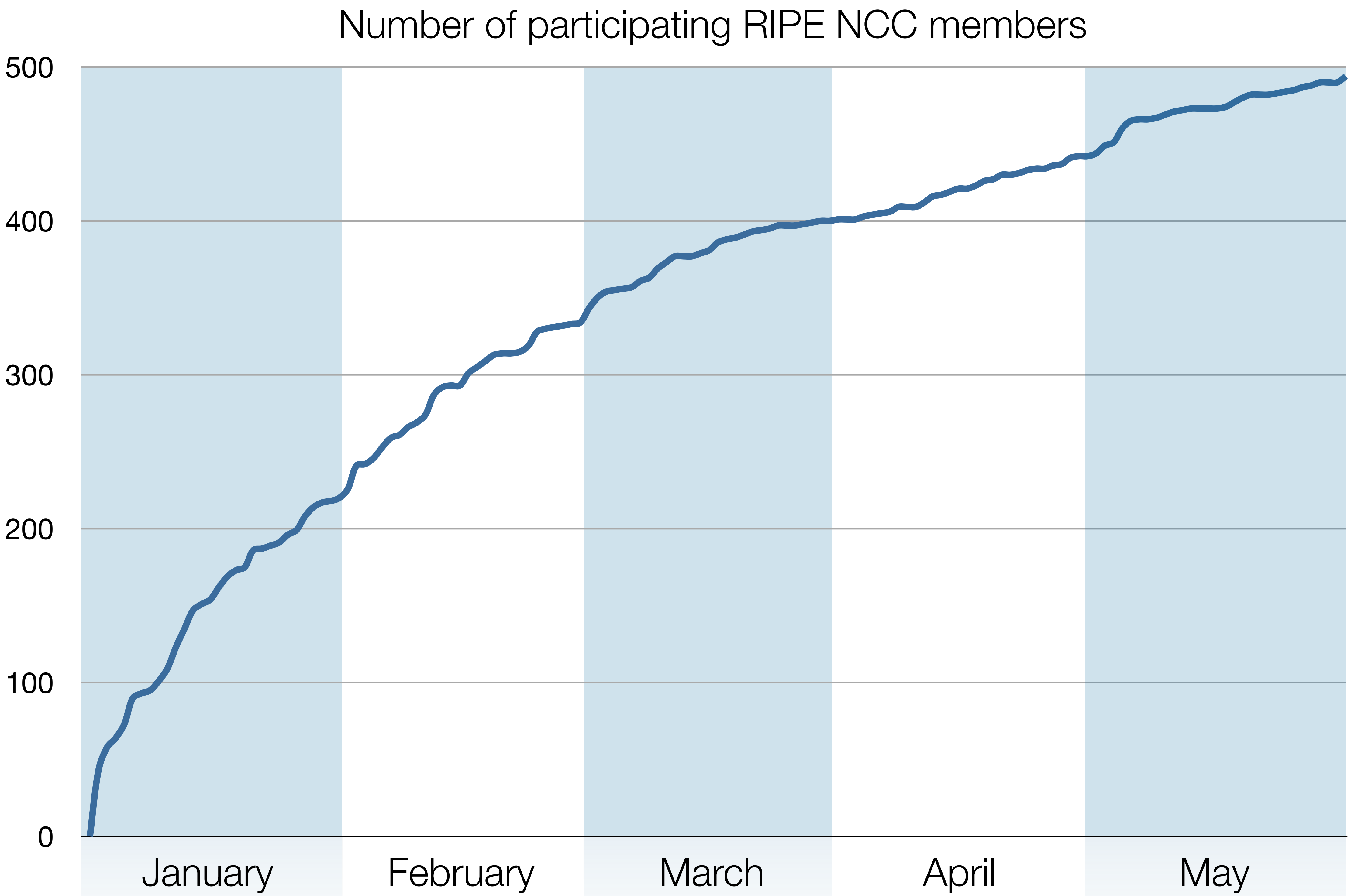
- Routers won’t do actual validation
  - takes to many resources
  - talks to remote validator instead
  - asks if certain announcement is authorised
- Validator answers authorisation question with:
  - Code 0: ROA found, validation succeeded
  - Code 1: No ROA found (resource not yet signed)
  - Code 2: ROA found, but validation failed

Hardware Validation: RPKI-RTR Protocol



```
route-map validity-0
  match rpki-invalid
  drop
route-map validity-1
  match rpki-not-found
  set localpref 50

// valid defaults to 100
```

Adoption


Number of participating RIPE NCC members
500
400
300
200
100
0
January
February
March
April
May

Adoption

france telecom

BT

Sunrise

janet

swisscom

012 smile

Telefonica

Limelight NETWORKS

du

وتحيا بها الحياة

add life to life

Telepac

A Internet profissional

T Deutsche Telekom

elisa

СЕВЕРО-ЗАПАДНЫЙ ТЕЛЕКОМ

TELE2 Sweden

RESILANS AB

sonera

belgacom

and 425 others...

Address Space Covered by ROAs

The equivalent of:

168,000 /24 IPv4 prefixes

8,400 /32 IPv6 prefixes

The Politics of Being a Certificate Authority

- If you issue certificates, they can also be revoked!

- Governments could mandate the use of resource certificates
  - As well as requiring to respect their status

- Law enforcement could try to use the system to take (foreign) ISPs offline

The Legal Analysis

- The RIPE NCC is an association under Dutch law
  - therefore subject to the Dutch legislation

- There is no specific Dutch legislation:
  - to order the deregistration of Internet resources
  - change the registration details of Internet resources
  - to revoke certificates over Internet resources

But... but...

“Laws can change!”

The Reality Today

- Anyone is free to request a certificate
- Anyone is free to specify their routing policy
- Anyone is free to base any decision on the data

Resource Certification drives routing preferences

Information and Announcements

http://ripe.net/certification

Questions?

✉ alexb@ripe.net

alexander_band

in linkedin.com/in/alexanderband

RIPE NCC