



RIPE NCC Certification Software

Tim Bruijnzeels
Senior Software Engineer RIPE NCC

Resource Certificate

- ✓ Public Key
- ✓ Resources
- ✓ Signature



➔ *NO IDENTITY!*

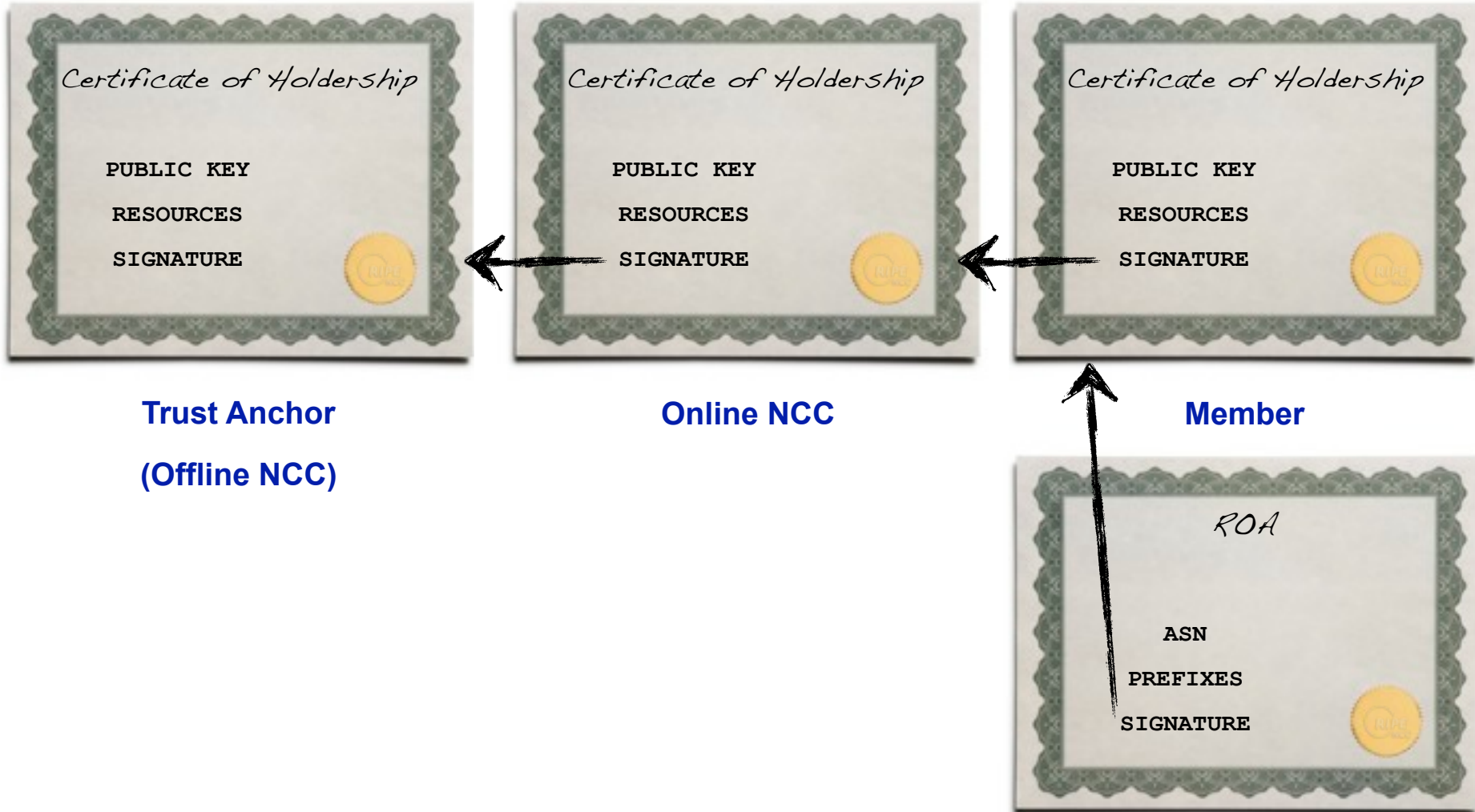
Route Origin Authorisation

- ✓ AS Number
- ✓ IP Prefixes
- ✓ Signature



➔ *NO IDENTITY!*

The Resource PKI





Hosted Member CA

- ➔ Simplify ROA management for members
- ➔ Available for all members
- ➔ Opt-in
- ➔ PA only, for now...


Hosted Member CA


LIR Portal
RIPE NCC


Edit LIR User
You are logged in as [nl.bluelight.admin]


[Home](#) » [Edit LIR User](#)


[Add a user from a different LIR.](#)

Username: timbru 

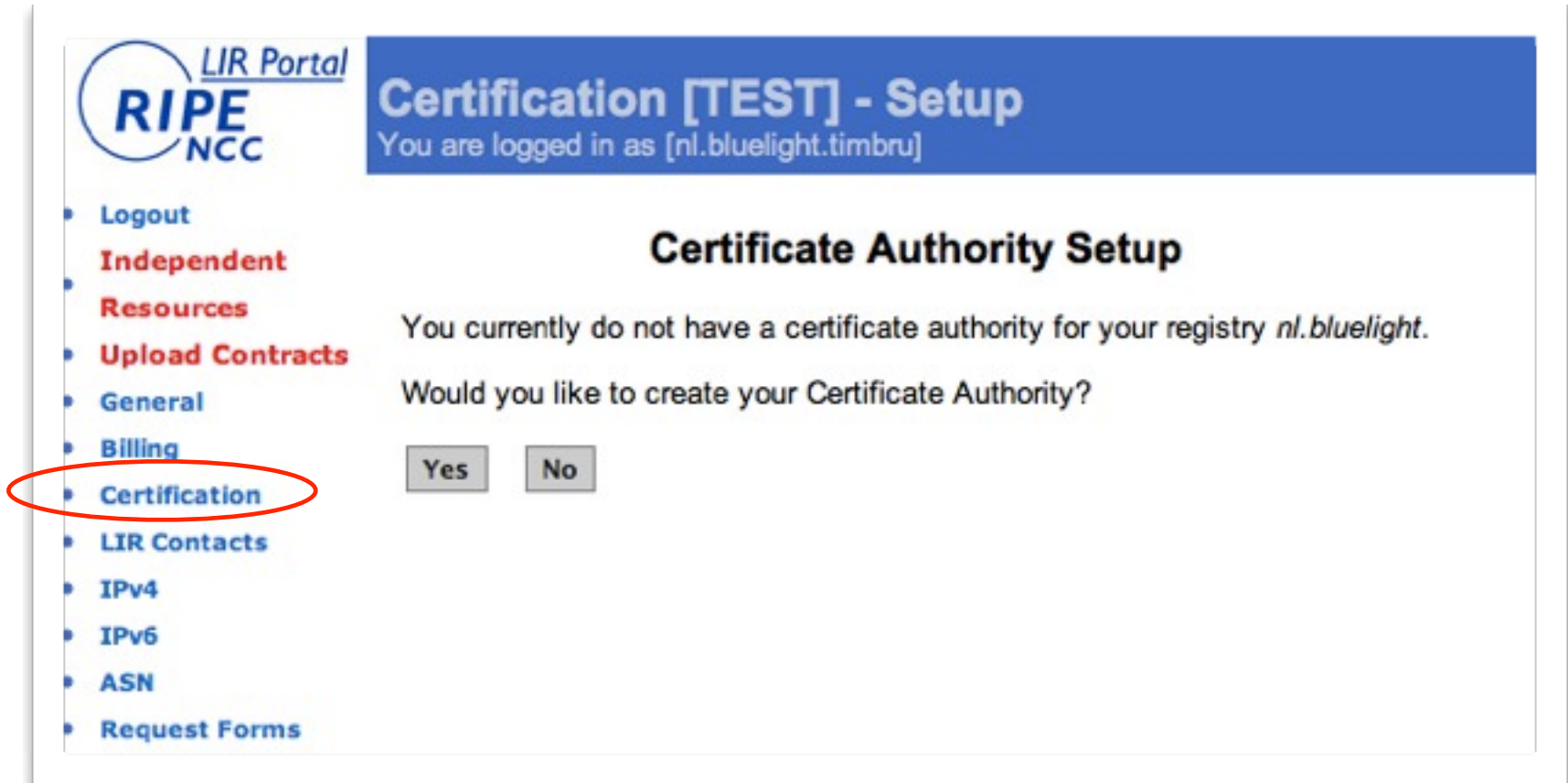
Name: 

Title: 

E-Mail: 

Groups: billing 
 certification
 general
 resources
 ticketing

Hosted Member CA

A screenshot of the RIPE NCC LIR Portal interface. The page title is "Certification [TEST] - Setup" and it shows the user is logged in as [nl.bluelight.timbru]. The main heading is "Certificate Authority Setup". The text states: "You currently do not have a certificate authority for your registry nl.bluelight. Would you like to create your Certificate Authority?" Below this text are two buttons: "Yes" and "No". On the left side, there is a navigation menu with several items: "Logout", "Independent Resources", "Upload Contracts", "General", "Billing", "Certification", "LIR Contacts", "IPv4", "IPv6", "ASN", and "Request Forms". The "Certification" item in the menu is circled in red.

LIR Portal
RIPE
NCC

Certification [TEST] - Setup

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

Certificate Authority Setup

You currently do not have a certificate authority for your registry *nl.bluelight*.

Would you like to create your Certificate Authority?

- Logout
- **Independent Resources**
- **Upload Contracts**
- General
- Billing
- **Certification**
- LIR Contacts
- IPv4
- IPv6
- ASN
- Request Forms



Hosted Member CA

Certification [TEST] - Certified Resources

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

[Welcome](#) [My Certified Resources](#) [My ROA Specifications](#) [History](#) [RIPE NCC ROA Repository](#)

Certified Resources

Certificate Authority Name	CN=nl.bluelight
Certified Resources	10.0.0.0/24

[View Certificate »](#)

Use [My ROA Specifications](#) to authorise an Autonomous System to announce your certified resources.



Hosted Member CA

Certification [TEST] - View Resource Certificate

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

[Welcome](#)
[My Certified Resources](#)
[My ROA Specifications](#)
[History](#)
[RIPE NCC ROA Repository](#)

Resource Certificate

[Download »](#)

Serial	2
Subject	CN=k47gWY4FXqjwyEKpczt4aMcgBcQ
Issuer	CN=x5c1-q3dTMuL7LMzzVX0r6zWjEk
Not valid before	2010-8-19 13:29
Not valid after	2011-7-1 0:00
Resources	10.0.0.0/24
AIA	ca issuer
SIA	ca repository
	manifest
Status	✓ OK Validation details »



Hosted Member CA

Certification [TEST] - ROA Specifications

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

[Welcome](#)[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 resources. Using your ROA specifications, the system will automatically publish the necessary ROA objects.

You have not entered any ROA Specifications.

[Add ROA Specification »](#)

Hosted Member CA

Certification [TEST] - ROA Specification

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

[Welcome](#)
[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. The ROA objects are signed with your current key to allow validation. See below for an explanation of the fields used to specify your ROA objects:

Name *	<input type="text" value="Example"/>			
ASN *	<input type="text" value="AS64512"/>			
Resources	Prefix *	Maximum Length		
	<input type="text" value="10.0.0.0/24"/>	<input type="text"/>	<input type="button" value="Remove"/>	
			<input type="button" value="Add row"/>	
Not valid Before	<input type="text"/>			
After	<input type="text"/>			
		<input type="button" value="Save"/>	<input type="button" value="Cancel"/>	



Hosted Member CA

Certification [TEST] - ROA Specifications

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

[Welcome](#) [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 resources. Using your ROA specifications, the system will automatically publish the necessary ROA objects.

Name	AS number	Prefixes	Not valid before	Not valid after	ROA object
Example	AS64512	10.0.0.0/24			View » Edit Delete

[Add ROA Specification »](#)



Hosted Member CA

Certification [TEST] - ROA Object

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

[Welcome](#)
[My Certified Resources](#)
[My ROA Specifications](#)
[History](#)
[RIPE NCC ROA Repository](#)

ROA Object

[Download »](#)

AS Number	AS64512	
Resources	Prefix	Maximum Length
	10.0.0.0/24	
Not valid before	2010-8-19 13:29	
Not valid after	2011-7-1 0:00	
Status	✓ OK	Validation details »
	View certificate details	



Hosted Member CA

Certification [TEST] - Certificate Authority History

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

[Welcome](#) [My Certified Resources](#) [My ROA Specifications](#) [History](#) [RIPE NCC ROA Repository](#)

Command History

Time	User	Command	
2010-8-19 13:04	nl.bluelight.timbru	Create ROA specification 'Example'.	Details »
2010-8-19 11:49	system	Create and activate Member Certificate Authority 'CN=nl.bluelight'.	Details »



Hosted Member CA

Certification [TEST] - RIPE NCC ROA Repository

You are logged in as [nl.bluelight.timbru] and you are editing registry nl.bluelight

[Welcome](#) [My Certified Resources](#) [My ROA Specifications](#) [History](#) [RIPE NCC ROA Repository](#)

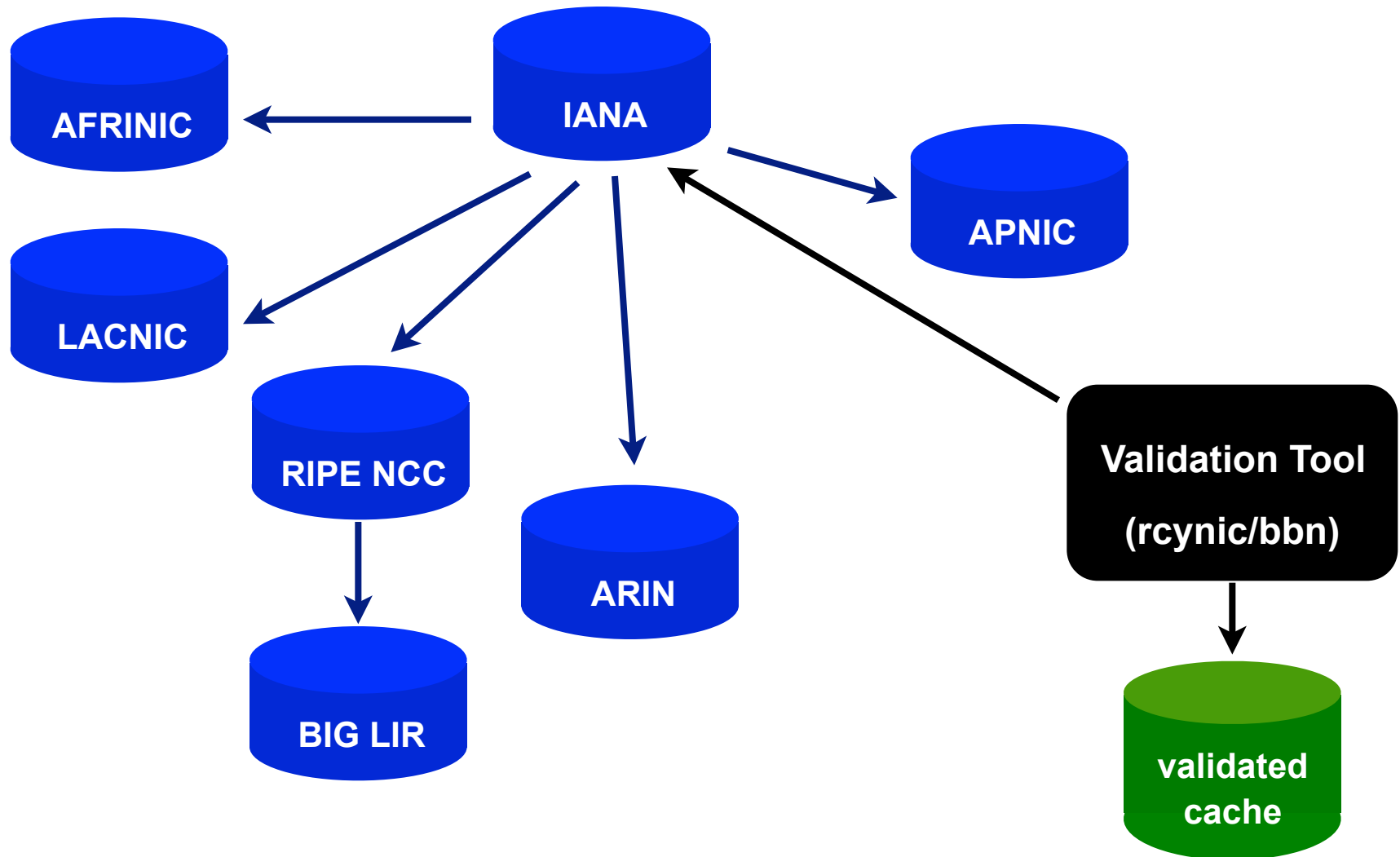
RIPE NCC ROA Repository

This page shows all ROA objects that have been made using the RIPE NCC certification system.

All times displayed are UTC.

AS number	Prefixes	Not valid before	Not valid after	
AS3333	85.118.184.0/21	2010-7-21 9:55	2011-7-1 0:00	Details » Download »
AS12657	212.72.64.0/19	2010-7-22 8:41	2011-7-1 0:00	Details » Download »
AS12657	213.131.192.0/19	2010-7-22 8:41	2011-7-1 0:00	Details » Download »
AS12657	2001:1578::/32	2010-7-22 8:41	2011-7-1 0:00	Details » Download »
AS12817	2001:1578:0200::/40	2010-7-22 8:41	2011-7-1 0:00	Details » Download »
AS29317	212.102.160.0/19	2010-7-22 8:41	2011-7-1 0:00	Details » Download »
AS29317	2001:1578:0100::/40	2010-7-22 8:41	2011-7-1 0:00	Details » Download »
AS43939	91.145.128.0/18	2010-8-11 9:42	2011-7-1 0:00	Details » Download »

RPKI Validation: Distributed Repositories





RPKI Validation: RPKI-RTR protocol



RPKI Validation: RPKI-RTR protocol

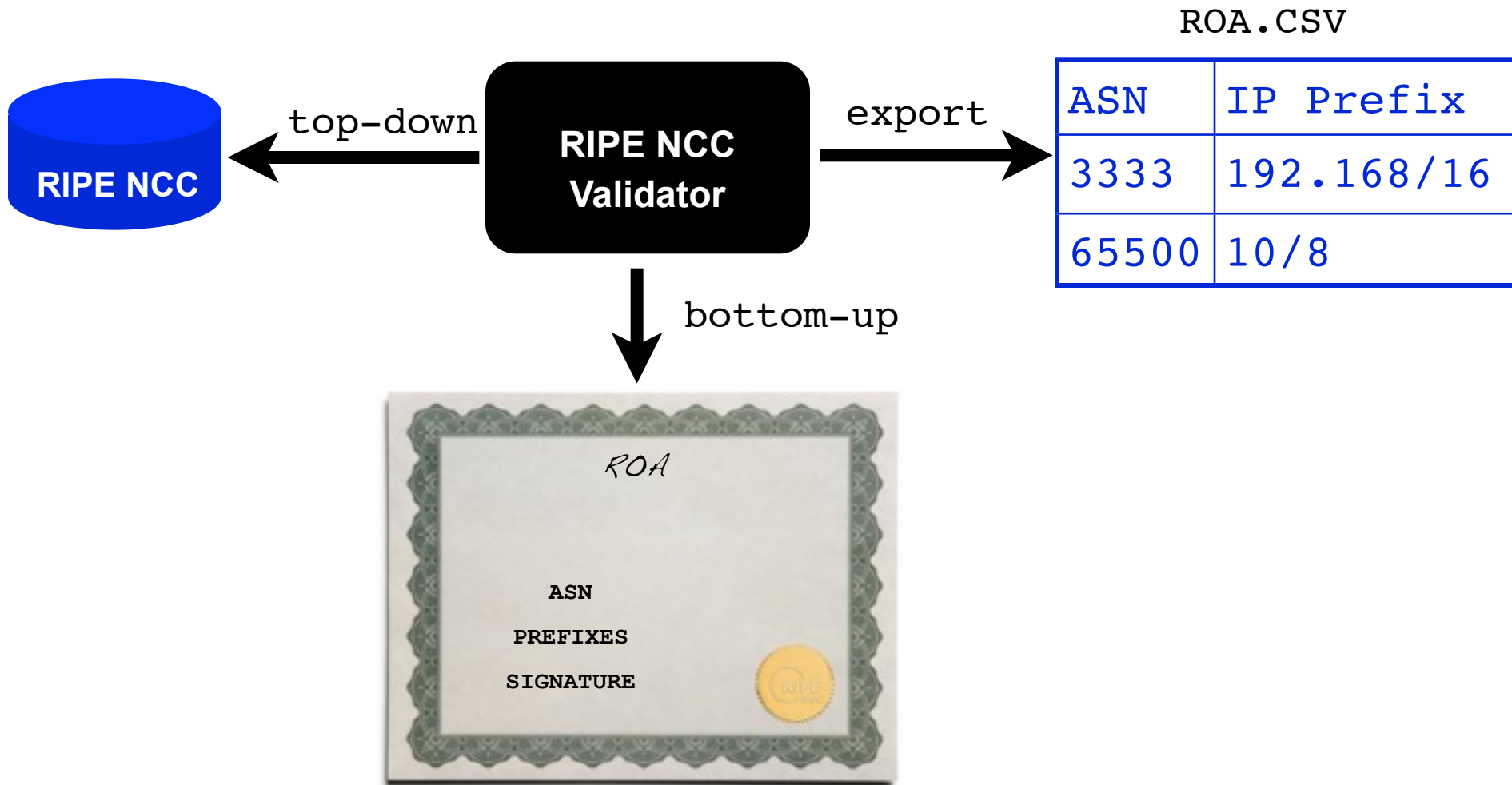


```
route-map validity-0
  match rpki-invalid
  drop
route-map validity-1
  match rpki-not-found
  set localpref 50

// valid defaults to 100
```



RPKI Validation: RIPE NCC Validator





RPKI Validation: RIPE NCC Validator

<http://labs.ripe.net/Members/agowland/ripe-ncc-validator-for-resource-certification>

ripenncc-rpki-validator.zip

```
../ripenncc-rpki-validator $ find .  
./bin  
./bin/certification-validator  
./jar  
./jar/certification-validator-1.17-jar-with-dependencies.jar  
./README.txt
```



RPKI Validation: RIPE NCC Validator

download TA

```
rsync rsync://certrepo.ripe.net/rta/CN=RTA,O=RIPE  
%20NCC,C=NL.cer ./rta.cer
```

top-down validation

```
.../ripenncc-rpki-validator $ bin/certification-validator \  
    --top-down -t ./rta.cer -o out --roa-export roas.csv  
  
15:55:49,927 INFO rsync://certrepo.ripe.net/rta/CN=RTA,O=RIPE  
%20NCC,C=NL.crl is VALID  
  
15:55:49,932 INFO rsync://certrepo.ripe.net/rta/CN=RTA,O=RIPE  
%20NCC,C=NL.mnf is VALID  
  
.....
```



RPKI Validation: RIPE NCC Validator

roas.csv

URI	ASN	IP Prefix	...
rsync://..	AS3333	85.118.184.0/21	
rsync://..	AS12657	2001:1578::/32	
rsync://..	AS29317	212.102.160.0/19	
...			



RPKI Validation: RIPE NCC Validator

bottom-up validation

```
.../ripenncc-rpki-validator $ bin/certification-validator \  
    -t ./rta.cer -f bl.roa --print  
  
16:47:56,381 INFO  rsync://certrepo.ripe.net/rta/CN=RTA,O=RIPE  
%20NCC,C=NL.cer is VALID  
  
....  
  
16:47:58,357 INFO  file:/Users/tim/Desktop/Brisbane/ripenncc-rpki-  
validator/bl.roa is VALID  
  
Signing time: 2010-08-19T09:28:53.000Z  
  
ASN: AS3333  
  
Prefixes:  
  
    85.118.184.0/21
```



RIPE NCC Validator

- ➔ Initially developed to test server implementation
- ➔ Command line tool released to support ad-hoc validation and ROA exports right now
- ➔ Can be extended if community wants:
 - ➔ usability
 - ➔ caching / distributed repositories
 - ➔ RPKI-RTR
- ➔ Open Source Release planned

Questions?

