

Resource Certification

Alex Band, Product Manager
DENIC Technical Meeting



Internet Routing

- Routing is non-hierarchical, open and free
- Freedom comes at a price:
 - You can announce any address block on your router
 - Route leaking happens frequently, impact is high
 - Entire networks become unavailable
 - Route hijacking is easy, as long as peers don't filter
- IPv4 address depletion may intensify issue

Digital Resource Certificates

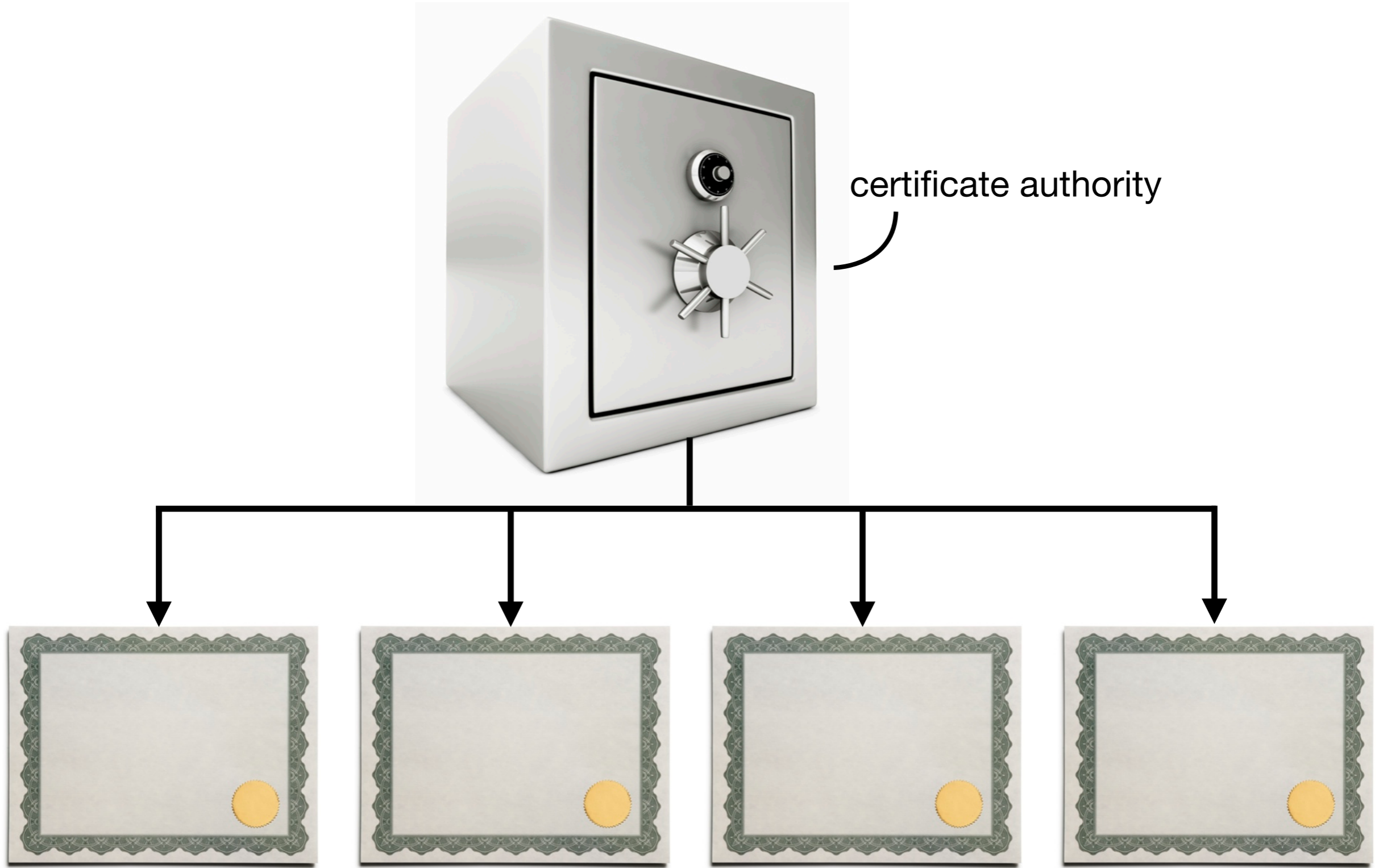
- Based on open IETF standards (sidr)
 - RFC 5280: X.509 PKI Certificates
 - RFC 3779: Extensions for IP Addresses and ASNs
- Issued by the RIRs
- States that an Internet number resource has been registered by the RIPE NCC
- Do not list any identity information
 - All resource information can be found in the registry

What Certification offers

- Proof of holdership
- Secure Inter-Domain Routing
 - Route Origin Authorisation
 - Prefer certified routing
- Resource transfers
- Validation is the added value!

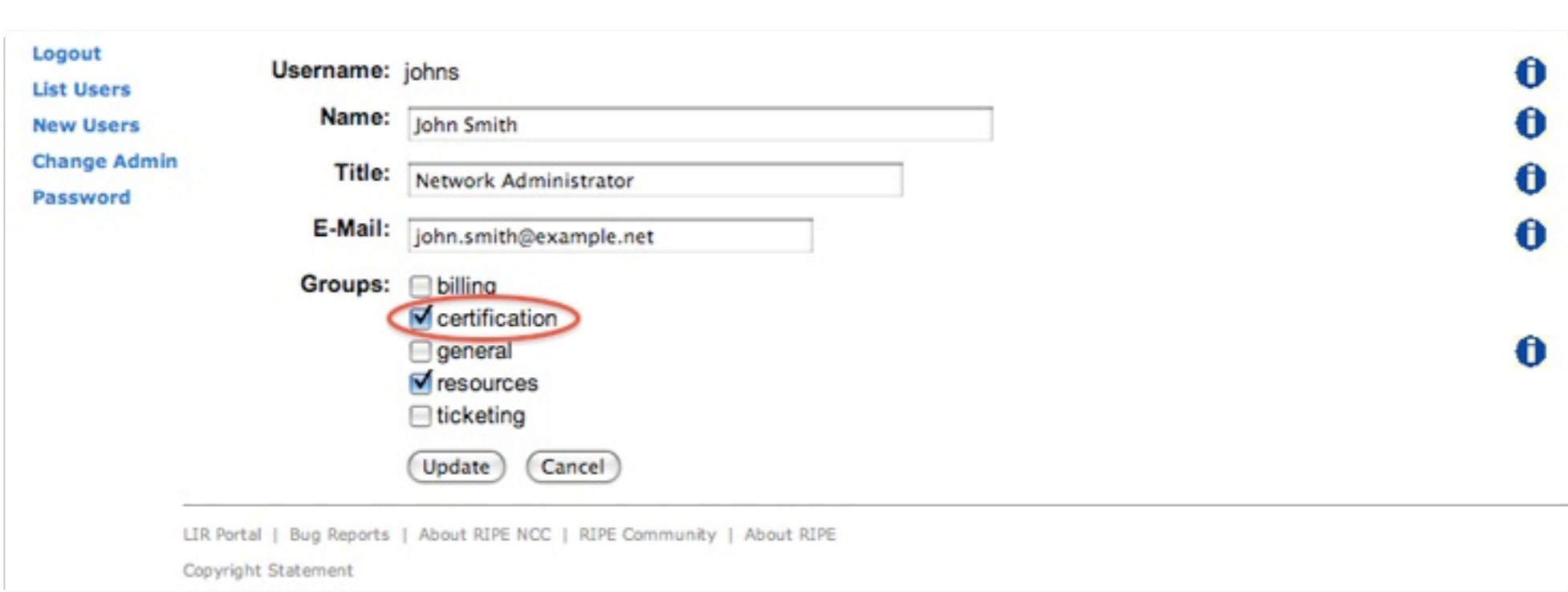


The system



The system (2)

- Accessible through the LIR Portal
- Administrator grants access to users



Logout
List Users
New Users
Change Admin
Password

Username: johns

Name: John Smith

Title: Network Administrator

E-Mail: john.smith@example.net

Groups:

- billing
- certification
- general
- resources
- ticketing

Update Cancel

LIR Portal | Bug Reports | About RIPE NCC | RIPE Community | About RIPE
Copyright Statement

Proof of holdership



Certificate validity

- Certificate is linked to the registration status
- Valid for 18 months after generating
- Automatically renewed after 12 months



Route Origin Authorisation (ROA)



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

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 »](#)

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:

Maximum length

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.

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:

My certified resources

85.118.184/21

93.175.146/23

2001:7fb:fd02::/47

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					

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

- Validators access publicly accessible repository
- Three software tools available
 1. RIPE NCC Validator
 - Easy to set-up and use, limited feature set
 2. rcynic
 3. 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 200.7.86.0
```

```
Prefix:                195.157.0.0/16
Prefix description:    Netscalibur UK Ltd
Country code:         GB
Origin AS:            8426
Origin AS Name:       CLARANET-AS ClaraNET
RPKI status:          ROA validation successful
```

```
$ whois -h whois.bgpmon.net " --roa 8426 195.157.0.0/16"
```

```
0 - valid
```

```
-----
ROA Details
-----
```

```
Origin ASN:           AS8426
Not valid Before:     2011-01-01 13:56:21
Not valid After:      2012-07-01 00:00:00
Trust Anchor:         rpki.ripe.net
Prefixes:             213.165.128.0/19
                    195.157.0.0/16
                    194.112.32.0/19
```


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
```

Hardware Validation: RPKI-RTR Protocol



- Cisco roadmap has router validation for RLS12 / IOS-XR in 2011
- Juniper is actively working on validation as well

Where are we now?

After 1 Month

234 LIRs are using the service
and created 173 ROAs
covering 469 prefixes

40159 /24 IPv4 prefixes

7340035 /48 IPv6 prefixes

The road ahead

- Enhance RIPE NCC Validator
- Up / Down protocol
 - Run your own Certificate Authority
 - Allow PI holders to manage ROAs
 - Transfers between RIRs
 - ERX space
- ROA tools
 - Import using combination of IRR + BGP + Human
 - Receive alert if ROA does not match BGP

For information and announcements:
<http://ripe.net/certification>



Questions?

