Certification in the real world

Alex Band – Product Manager
RIPE 62 – Routing WG

The Certification System Today

- 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 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

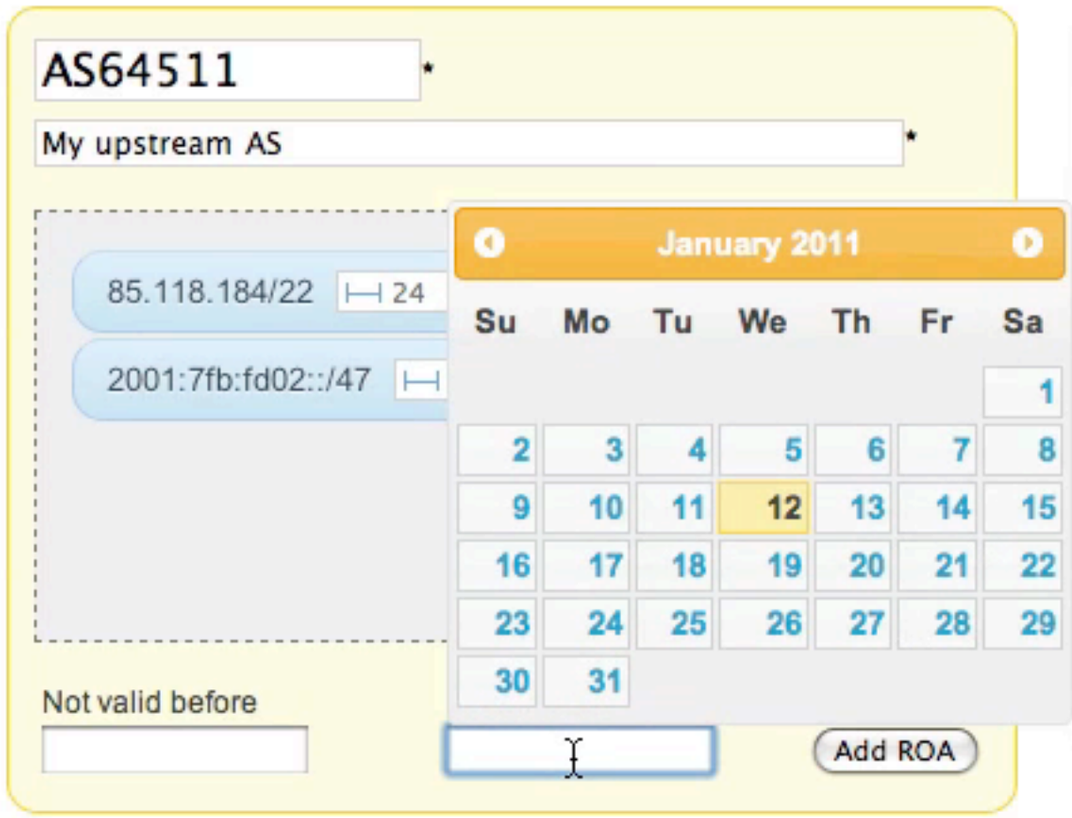
You are logged in as [nl.bluelight.alexb]

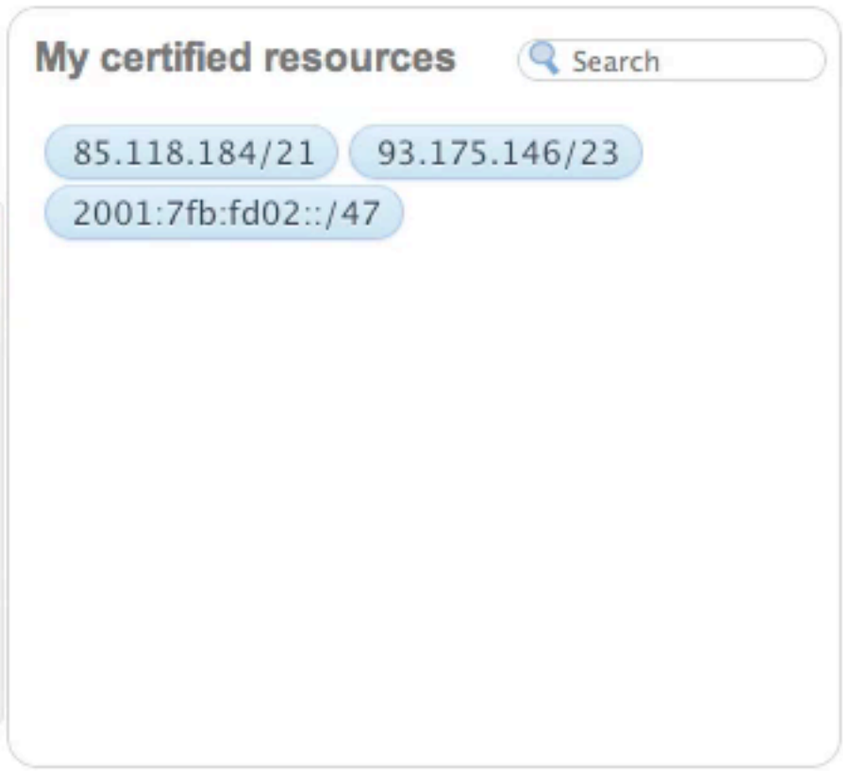
- Logout
- General
- Billing
- Certification
- LIR Contacts
- IPv4
- IPv6
- ASN
- Request Forms
- Object Editors
- Tickets
- Training
- Tools
- Change Password
- X.509 PKI
- Events
- Glossary
- Contact

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.

Address Space Covered by ROAs

The equivalent of:

168,000 /24 IPv4 prefixes

8,400 /32 IPv6 prefixes

Data in the ROA Repository

- Varying degrees of detail in routing policy
  - Only ROAs for some of their prefixes
  - Only ROAs for their own AS
    - Invalidating announcements by other (legitimate) ASs
- Varying usage of Maximum Length option
  - Some want to allow the freedom to deaggregate
  - Some want to be a strict as possible
  - Some misunderstand the purpose

The Implementation of Maximum Length

- RIPE NCC has an optional blank field
- LACNIC has a mandatory blank field
- APNIC, AfriNIC allow maximum deaggregation
  - Default /32 for IPv4
  - Default /128 for IPv6

What's the sensible default?

Knowing The Effect of Your Choices

- Use RIS Route Collectors to support Certification
  - 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
- Suggest ROAs based on real-world routing

Support for Non-Hosted System

- Implement the up/down protocol
  - Allows to run your own Certificate Authority
    - Requirement for ARIN to launch
- Release RIPE NCC client software
  - Pilot program: contact us if you want to participate
  - Open source, BSD license

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

Information and Announcements

http://ripe.net/certification

Questions?