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

certificate authority
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
## 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>AS number</th>
<th>Prefixes</th>
<th>Not valid before</th>
<th>Not valid after</th>
<th>ROA object</th>
</tr>
</thead>
<tbody>
<tr>
<td>invalid-ipv4</td>
<td>AS196615</td>
<td>93.175.147.0/24</td>
<td></td>
<td></td>
<td><a href="#">View</a></td>
</tr>
<tr>
<td>invalid-ipv6</td>
<td>AS196615</td>
<td>2001:7fb:fd03::/48</td>
<td></td>
<td></td>
<td><a href="#">View</a></td>
</tr>
<tr>
<td>valid-ipv4</td>
<td>AS12654</td>
<td>93.175.146.0/24</td>
<td></td>
<td></td>
<td><a href="#">View</a></td>
</tr>
<tr>
<td>valid-ipv6</td>
<td>AS12654</td>
<td>2001:7fb:fd02::/48</td>
<td></td>
<td></td>
<td><a href="#">View</a></td>
</tr>
</tbody>
</table>

[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:

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:

**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
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

- Adoption chart showing the increase in the number of participating RIPE NCC members over time from January to October. The number of members grows steadily from a low in January to a high in October.

Monday, October 31, 2011
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

Welcome to the Local Certification Service

It takes just a couple of minutes to set up your Certificate Authority. At the end of this process you will have a resource certificate listing the Internet Number Resources that your LIR holds.

There are two requirements to complete this process:

1. Resource Certification needs to be enabled for your user account in the RIPE NCC LIR Portal. Please ask your LIR Portal Administrator to follow these steps to set this up for you.
2. rsync needs to be running on your system. It will be used to make the repository where your resource certificate is published available to others. Please see the README file for details. It is a good idea to set up rsyncd first and start it using the supplied scripts. This will give you all the information you need below.

To get started, enter the required information below.

Rsync

Hostname: lca.example.net
Port: 10873
Module: lca

All fields are required. Use port 873 for rsync default. Only alphanumeric characters are allowed. No whitespace.

So the public uri for the base of your repository is: rsync://lca.example.net:10873/lca

Base directory: /Users/johndoe/rpki-lca/repository

This is the base directory on disk. Please use the directory that rsyncd_ctl.sh reported here. If you don’t understand this sentence read this text.

SAVE 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
Quick overview of BGP Origin validation

Trust Anchors  ROAs  Ignore Filters  Whitelist  Router

Trust Anchors are the entry points used for validation in any Public Key Infrastructure (PKI) system. This validator is intended for the validation of Resource PKI (RPKI) systems. It is pre-configured with Trust Anchors for four RIRs who are running such systems now.

Copyright © 2009, 2010, 2011 the Réseaux IP Européens Network Coordination Centre RIPE NCC. All rights restricted.
RIPE NCC RPKI-RTR Validator

Validated ROAs

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

Download validated ROAs as CSV

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