Goals

• Explain where it started
• Learn what resources certificates are
• Learn how to request a certificate
• Learn how to create a Route Origin Authorization
• Learn how to integrate ROAs in your workflow
• Making BGP decisions based on the RPKI
• Lots of live demonstrations
Certification
Current Practices in Filtering

• Filtering limited to the edges facing the customer

• Filters on peering and transit sessions are often too complex or take too many resources
  - Do you filter?

• A lot depends on trusting each other
  - Daily examples show this is no longer enough
Limitations of the Routing Registry

• A lot of different registries exist, operated by a number of different parties:
  - Not all of them mirror the other registries
  - How trustworthy is the information they provide?

• The IRR system is far from complete

• Resulting filters are hard to maintain and can take a lot of router memory
Securing BGP Routing

• SIDR working group in the IETF looking for a solution:
  - Is a specific AS authorised to originate an IP prefix?

• Based on open standards:
  - RFC 5280: X.509 Public Key Infrastructure
  - RFC 3779: Extensions for IP addresses and ASNs
The RIPE NCC Involvement in RPKI

• The authority who is the holder of an Internet Number Resource in our region
  - IPv4 and IPv6 address ranges
  - Autonomous System Numbers

• Information is kept in the registry

• Accuracy and completeness are key
Digital Resource Certificates

• Issue digital certificates along with the registration of Internet Resources

• Two main purposes:
  – Make the registry more robust
  – Making Internet Routing more secure

• Added value comes with validation
Using Certificates

• Certification is a free, opt-in service
  – Your choice to request a certificate
    – Linked to your membership
    – Renewed every 12 months

• Certificate does not list any identity information
  – That information is in the RIPE Database

• Digital proof you are the holder of a resource
The PKI System

• The RIRs hold a self-signed root certificate for all the resources that they have in the registry
  - They are the trust anchor for the system

• That root certificate is used to sign a certificate that lists your resources

• You can issue child certificates for those resources to your customers
  - When making assignments or sub allocations
Certificate Authority (CA) Structure

Root CA (RIPE NCC)

Member CA (LIR)

Customer CA
Validation

• All certificates are published in publicly accessible repositories
  - RIPE NCC operates one of them
• You can download all certificates and associated public keys
• Using cryptographic tools to verify yourself that all certificates are valid and linked to the root CA
Which Resources Are Certified?

• Everything for which we are 100% sure who the owner is:
  - Provider Aggregatable (PA) IP addresses
  - Provider Independent (PI) addresses marked as “Infrastructure”

• Other resources will be added over time:
  - PI addresses for which we have a contract
  - ERX resources
Legacy Address Space

• A project has started to bring legacy resources into the registry system

• Makes the registry more robust and complete:
  – Holders are verified to be legit
  – Information published in the RIPE Database
  – Resources can be certified

• Free service for legacy holders
  – Contact legacy@ripe.net for more information
Demo

Setting up certification in the LIR Portal
Enabling Access To RPKI

Edit Alex Band (alexb@ripe.net)

Title

product manager

As an admin, you can grant and revoke access to and from your LIR.

Groups

billing

Certification

general

resources

ticketing

Assign admin privileges to this user

UPDATE USER
Setting Up a Certificate Authority

Certificate Authority Setup

You currently do not have a Certificate Authority for your registry. Would you like to create your Certificate Authority?

RIPE NCC Certification Service Terms and Conditions

Introduction


By clicking on 'I accept. Create my Certificate Authority' below you confirm that you have read, understood and agree to the RIPE NCC Certification Service Terms and Conditions.

I accept. Create my Certificate Authority
Your Resource Certificate

Certified Resources

Certificate Authority Name: CN=nl.ripenc-cs
Certified Resources:
- 193.0.24.0/21
- 2001:67c:64::/48

Resource Certificate

Serial: 231785814
Subject: CN=b2hNZ8lnrMFsXKKWPUwV9nyOxXA
Issuer: CN=u75at9r0D4JbJ3_SFkZX7C5dmg
Not valid before: 2012-04-02T17:28:16.000Z
Not valid after: 2013-07-01T00:00:00.000Z
Resources:
- 193.0.24.0/21
- 2001:67c:64::/48
AIA: ca issuer
SIA: ca repository
manifest

Validation Result: OK
ROA

Route Origination Authorisation
Making a Statement

• You as the certified holder of the IP addresses can decide who should announce these prefixes to the Internet:
  - They can originate from your own ASN
  - Or by a third party on your behalf
  - Maybe a part will be announced by somebody else

• You can use the certificate to “sign” this statement, to prove this is really you
Route Origination Authorisation (ROA)

• Next to the prefix and the ASN which is allowed to announce it, the ROA contains:
  - A minimum prefix length
  - A maximum prefix length
  - An expiry date

• Multiple ROAs can exist for the same prefix

• ROAs can overlap
Publication and Validation

• ROAs are published in the same repositories as the certificates and the keys.

• You can download them and use software to verify all the cryptographic signatures are valid.
  - Was this really the owner of the prefix?

• You will end up with a list of prefixes and the ASN that is expected to originate them.
  - And you can be sure the information comes from the holder of the resources.
Demo

Creating a ROA
My ROA Specifications

A Route Origin Authorisation (ROA) allows anyone on the Internet to validate that you have authorised the announcement of a specific prefix. Once you create a specification, a ROA is automatically published in the RIPE NCC ROA Repository in the form of a cryptographic object. In your ROA specifications, you state which Autonomous Systems are authorised to originate the prefixes you hold. At all times, your ROA specifications should match your intended BGP routing.

You have not entered any ROA Specifications.

Add ROA Specification »

Current BGP announcements

These are the current BGP announcements, as seen by the RIPE NCC Remote Route Collectors, that overlap with your certified resources. Only announcements seen by five or more peers are shown. This data can be up to nine hours old, so recent changes might not be reflected.

<table>
<thead>
<tr>
<th>Origin AS</th>
<th>Prefix</th>
<th>Route Validity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS2121</td>
<td>193.0.24.0/21</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>AS2121</td>
<td>2001:6764::/48</td>
<td>UNKNOWN</td>
</tr>
</tbody>
</table>
Add 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:

- **AS number**: Enter your AS number here.
- **My certified resources**: Search for your certified resources.
- **Drag your resources here**: Drag the resources that you want to add to your ROA.

**AS2121**

- **My ROA for the aggregate**: Enter your ROA for the aggregate.
- **Not valid before** and **and/or after**: Specify the validity dates of your ROA.

**My certified resources**

- **Search**: Use this search function to find your certified resources.
- **193.0.24/21** and **2001:67c:64::/48**: Enter your certified resources here.

**Maximum length**: Click on the maximum length button to adjust the length of your ROA.
Adding a ROA

AS2121

My ROA for the aggregate

193.0.24/21

2001:67c:64::/48

Not valid before

and/or after

2012-07-01 00:00

Add ROA
Your New ROA

ROA Specifications

A Route Origin Authorisation (ROA) allows anyone on the Internet to validate that you have authorised the announcement of a specific prefix. Once you create a specification, a ROA is automatically published in the RIPE NCC ROA Repository in the form of a cryptographic object. In your ROA specifications, you state which Autonomous Systems are authorised to originate the prefixes you hold. At all times, your ROA specifications should match your intended BGP routing.

<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>My ROA for the aggregate</td>
<td>AS2121</td>
<td>193.0.24.0/21 (24)</td>
<td>View »</td>
<td>Edit</td>
<td>Delete</td>
</tr>
</tbody>
</table>

Add ROA Specification »

ROA Object

<table>
<thead>
<tr>
<th>AS Number</th>
<th>Resources</th>
<th>Prefix</th>
<th>Maximum Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS2121</td>
<td>193.0.24.0/21</td>
<td>24</td>
<td></td>
</tr>
</tbody>
</table>

Not valid before 2012-04-02T17:15:28.000Z
Not valid after 2013-07-01T00:00:00.000Z

Download »

Validation Result ✓ OK details »
### The ROA Repository

These are all of the ROA objects that have been created using the RIPE NCC Certification Service. These objects are part of the RIPE NCC Certification Repository and as such are subject to **Terms and Conditions**.

All times displayed are UTC.

<table>
<thead>
<tr>
<th>AS number</th>
<th>Prefixes</th>
<th>Not valid before</th>
<th>Not valid after</th>
<th>Details</th>
<th>Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS2121</td>
<td>193.0.24.0/21</td>
<td>2012-04-02T17:15:28.000Z</td>
<td>2013-07-01T00:00:00.000Z</td>
<td><a href="#">Details</a></td>
<td><a href="#">Download</a></td>
</tr>
<tr>
<td>AS3333</td>
<td>2001:67c:2e8::/48</td>
<td>2012-03-13T16:32:10.000Z</td>
<td>2013-07-01T00:00:00.000Z</td>
<td><a href="#">Details</a></td>
<td><a href="#">Download</a></td>
</tr>
<tr>
<td></td>
<td>84.205.64.0/19</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS12654</td>
<td>93.175.144.0/20</td>
<td>2012-03-13T16:32:10.000Z</td>
<td>2013-07-01T00:00:00.000Z</td>
<td><a href="#">Details</a></td>
<td><a href="#">Download</a></td>
</tr>
<tr>
<td></td>
<td>2001:7fd::/32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2001:7fd::/32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS20647</td>
<td>91.102.8.0/21</td>
<td></td>
<td></td>
<td><a href="#">Details</a></td>
<td><a href="#">Download</a></td>
</tr>
<tr>
<td>AS25152</td>
<td>194.29.224.0/19</td>
<td>2012-04-04T07:31:08.000Z</td>
<td>2013-07-01T00:00:00.000Z</td>
<td><a href="#">Details</a></td>
<td><a href="#">Download</a></td>
</tr>
<tr>
<td>AS34347</td>
<td>2a02:f28::/32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS197000</td>
<td>2001:67c:e0::/48</td>
<td>2012-03-13T16:32:10.000Z</td>
<td>2013-07-01T00:00:00.000Z</td>
<td><a href="#">Details</a></td>
<td><a href="#">Download</a></td>
</tr>
</tbody>
</table>
Validator
ROA Validation

• All the certificates, public keys and ROAs which form the RPKI are available for download

• Software running on your own machine can retrieve and then verify the information
  - Cryptographic tools can check all the signatures

• The result is a list of all valid combinations of ASN and prefix, the “validated cache”
ROA Validation Workflow

Cert's ROAs

Repositories

ARIN
Afrinic
APNIC
Lacnic

RIPE NCC

Validator

Validated cache

Network equipment

RPKI-RTR protocol

Sandbox

Processing

View and modify

view and modify

http
Validation

• Every certificate and ROA is signed using the private key of the issuer

• The public keys in the repository allow you to verify the signature was made using the correct private key

• You can walk the whole RPKI tree structure up to the Root Certificates of the RIRs
Reasons For a ROA To Be Invalid

• The start date is in the future
  - Actually this is flagged as an error

• The end date is in the past
  - It is expired and the ROA will be ignored

• The signing certificate or key pair has expired or has been revoked

• It does not validate back to a configured trust anchor
Modifying the Validated Cache

• The RIPE NCC Validator allows you to manually override the validation process
• Adding an ignore filter will ignore all ROAs for a given prefix
  - The end result is the validation state will be “unknown”
• Creating a whitelist entry for a prefix and ASN will locally create a valid ROA
  - The end result is the validation state becomes “valid”
The Decision Process

• When you receive a BGP announcement from one of your neighbors you can compare this to the validated cache

• There are three possible outcomes:
  - **Unknown**: there is no covering ROA for this prefix
  - **Valid**: a ROA matching the prefix and ASN is found
  - **Invalid**: There is a ROA but it does not match the ASN or the prefix length
Router-RPKI Protocol

• Routers can download the validated cache from the validator and have it available in memory

• The BGP process will check each announcement and label the prefix

• You can instruct your router to look at those labels and make a decision based on it
  - Modify preference values
  - Filter the announcement
  - ...
The Decision is Yours

• The Validator is a tool which can help you making informed decisions about routing

• Using it properly can enhance the security and stability of the Internet

• It is your network and you make the final decision
Exercise/Demo

Using the RIPE NCC Validator
Download the Validator

- [http://www.ripe.net/certification -> tools](http://www.ripe.net/certification -> tools)
  - Requires Java 1.6 and rsync
  - No Installation required
    - Unzip the package
    - Run the program
- Interface available on localhost port 8080
Starting the Validator

```
$ cd Downloads/rpki-validator-app-2.0.4/
$ ./bin/rpki-validator

15:02:25,138 INFO Loading trust anchors...
15:02:25,293 INFO Config file does not exist: File '/Users/mhogewon/Downloads/rpki-validator-app-2.0.4/data/configuration.json' does not exist
15:02:25,482 INFO RTR server listening on 0.0.0.0/0.0.0.0:8282
15:02:25,989 INFO Welcome to the RIPE NCC RPKI Validator, now available on port 8080. Hit CTRL+C to terminate.
15:02:26,143 INFO Retrieving BGP entries from http://www.ris.ripe.net/dumps/riswhoisdump.IPv4.gz
15:02:26,454 INFO Retrieving BGP entries from http://www.ris.ripe.net/dumps/riswhoisdump.IPv6.gz
15:02:27,334 INFO Loaded trust anchor from location rsync://rpki-pilot.arin.net:10873/certrepo/e8/29af2d-319c-428f-b6b0-3528a7d24dcd/1/4789Xt9H2ltHuAXdrQ6GWXWH2Ao.cer
15:02:27,343 INFO Prefetching 'rsync://rpki-pilot.arin.net:10873/certrepo/'
15:02:27,389 INFO Loaded trust anchor from location rsync://rpki.ripe.net/ta/ripe-ncc-ta.cer
15:02:27,390 INFO Prefetching 'rsync://rpki.ripe.net/repository/'
15:02:28,294 INFO Loaded trust anchor from location rsync://rpki.afrinic.net/repository/AfrINIC.cer
15:02:28,295 INFO Prefetching 'rsync://rpki.afrinic.net/member_repository/'
15:02:28,557 INFO Started validating ARIN Test Lab
15:02:29,165 INFO Loaded trust anchor from location rsync://repository.lacnic.n...
The Web Interface

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 all the RIRs who are running such systems now.

If you would like to add or change the Trust Anchors that are used by this validator, please see the README.txt file for details.
## Trust Anchors

![Screenshot of RPKI Validator - Configured Trust Anchors](image)

### Configured Trust Anchors

<table>
<thead>
<tr>
<th>Trust anchor</th>
<th>Processed Items</th>
<th>Expires in</th>
<th>Last updated</th>
<th>Next update in</th>
</tr>
</thead>
<tbody>
<tr>
<td>APNIC RPKI Root</td>
<td>1356</td>
<td>4 years and 2 months</td>
<td>7 minutes ago</td>
<td>3 hours</td>
</tr>
<tr>
<td>ARIN Test Lab</td>
<td>88</td>
<td>1 year and 2 months</td>
<td>8 minutes ago</td>
<td>3 hours</td>
</tr>
<tr>
<td>AfriNIC RPKI Root</td>
<td>81</td>
<td>4 years and 7 months</td>
<td>8 minutes ago</td>
<td>3 hours</td>
</tr>
<tr>
<td>LACNIC RPKI Root</td>
<td>216</td>
<td>10 months and 3 weeks</td>
<td>8 minutes ago</td>
<td>3 hours</td>
</tr>
<tr>
<td>RIPE NCC RPKI Root</td>
<td>3570</td>
<td>4 years and 9 months</td>
<td>7 minutes ago</td>
<td>3 hours</td>
</tr>
</tbody>
</table>

Copyright ©2009-2012 the Réseaux IP Européens Network Coordination Centre RIPE NCC. All rights restricted. Version 2.0.4
Listing All Validated ROAs

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

<table>
<thead>
<tr>
<th>ASN</th>
<th>Prefix</th>
<th>Maximum Length</th>
<th>Trust Anchor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.1.0/24</td>
<td>24</td>
<td>ARIN Test Lab</td>
</tr>
<tr>
<td>1</td>
<td>192.168.1.0/24</td>
<td>24</td>
<td>ARIN Test Lab</td>
</tr>
<tr>
<td>1</td>
<td>61.45.250.0/23</td>
<td>23</td>
<td>APNIC RPKI Root</td>
</tr>
<tr>
<td>1</td>
<td>61.45.250.0/23</td>
<td>23</td>
<td>APNIC RPKI Root</td>
</tr>
<tr>
<td>21</td>
<td>10.4.0.0/16</td>
<td>16</td>
<td>ARIN Test Lab</td>
</tr>
<tr>
<td>22</td>
<td>10.255.1.0/24</td>
<td>24</td>
<td>ARIN Test Lab</td>
</tr>
<tr>
<td>42</td>
<td>2001:678:3::/48</td>
<td>48</td>
<td>RIPE NCC RPKI Root</td>
</tr>
<tr>
<td>42</td>
<td>194.0.17.0/24</td>
<td>24</td>
<td>RIPE NCC RPKI Root</td>
</tr>
<tr>
<td>174</td>
<td>89.207.56.0/21</td>
<td>21</td>
<td>RIPE NCC RPKI Root</td>
</tr>
</tbody>
</table>
Add an Ignore Filter

Insert the prefix and click “add”

The overview shows if there is a match
Creating a Whitelist

Add the origin, prefix and maximum length

This locally creates a valid (but fake) ROA
BGP Preview

• The validator downloads a copy of the RIS
  - Allows you to get a hint of what would happen
  - RIS view might be different from your routing table
BGP Preview Detail

<table>
<thead>
<tr>
<th>ASN</th>
<th>Prefix</th>
<th>Length</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>2001:468:904::/48</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>2001:468:c01::/48</td>
<td></td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>2001:468:1900::/40</td>
<td></td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>2001:468:1500::/40</td>
<td></td>
<td></td>
</tr>
<tr>
<td>102</td>
<td>2001:468:c13::/48</td>
<td></td>
<td>INVALID</td>
</tr>
<tr>
<td>719</td>
<td>193.209.25.0/24</td>
<td></td>
<td>INVALID</td>
</tr>
<tr>
<td>1312</td>
<td>2001:468:c80::/48</td>
<td></td>
<td>INVALID</td>
</tr>
<tr>
<td>1312</td>
<td>2001:468:ce0::/44</td>
<td></td>
<td>INVALID</td>
</tr>
<tr>
<td>1351</td>
<td>2001:468:606::/48</td>
<td></td>
<td>INVALID</td>
</tr>
<tr>
<td>1406</td>
<td>2001:470:e::/48</td>
<td></td>
<td>INVALID</td>
</tr>
</tbody>
</table>
Exporting the Validated Cache

- **Router sessions**
  - Validator listens on 8282 for RPKI-RTR Protocol
  - Routers can connect and download the cache

- **Export function**
  - Allows you to download a CSV with the cache
  - Can be integrated with your internal workflow
  - Use for statistics or spotting anomalies
Router Integration
Open Standards

• The RPKI-RTR Protocol is an IETF standard

• All router vendors can implement it
  - Cisco has beta images available
  - Juniper expects it to be in 12.2 (Q312)
  - Quagga has support for it

• Ask your favorite sales person for more information
  - And tell them you like this
Public Testbeds

- A few people allow access to routers that run RPKI and allow you to have a look at it

- RIPE NCC has a Cisco:
  - Telnet to rpki-rtr.ripe.net
  - User: ripe, no password

- Eurotransit has a Juniper:
  - Telnet to 193.34.50.25 or 193.34.50.26
  - Username: rpki, password: testbed

Non Hosted

Doing it all yourself
Using the RIPE NCC Platform

• Using the hosted system is an easy way to deploy RPKI without high investments
  - Easy to setup a certificate authority and ROAs
  - Key and certificate rollovers are taken care of
  - RIPE NCC system is certified and audited

• Drawback is the RIPE NCC needs to have both your public and private key
  - Needed to create ROAs and certificates
  - Some people say this is less secure
Do It Yourself

• Everything is based on open standards

• You can take matters in your own hand:
  – Setup and run your own Certificate Authority
  – Create the ROAs on your system
  – Optionally have your own publication point

• Communication channel with the RIPE NCC allows you to get your certificate signed by us
  – This is known as the “up down protocol”
Third Party Tools

• RPKI Engine 1.0
  - http://www.hactrn.net/rpki-dox/
  - Includes rcynic validation tool

• RPSTIR (BBN Third Party Tool)
  - http://rpstir.sourceforge.net/

• RTRlib - The RPKI RTR Client C Library
  - http://rpki.realmv6.org/
Roadmap

• Support for non-hosted is still under development by the RIPE NCC
  - Expected release will be third quarter 2012

• We can give you access to beta test
  - Mail certification@ripe.net if you are interested

• More information will be published on the certification website
  - [http://www.ripe.net/certification](http://www.ripe.net/certification)
Questions?
Follow Us

@TrainingRIPENCC
#RPKI
The End!