ARIN Provisioning in RPKI

Mark Kosters
ARIN CTO
Possible Data Flow for Operations

- RPKI provisioning -> Repository
- Repository aggregator -> Validator
- Validated entries -> Route checking
- Route checking results -> Local routing decisions (based on local policy)

- We will focus on provisioning
How you can use ARIN’s RPKI System?

• Hosted
• Hosted using ARIN’s RESTful service
• Delegated using Up/Down Protocol
Hosted RPKI

• Pros
  – Easier to use
  – ARIN managed

• Cons
  – No current support for downstream customers to manage their own space (yet)
  – Tedious through the IU if you have a large network
  – We hold your private key
Hosted RPKI with RESTful Interface

• Pros
  – Easier to use
  – ARIN managed
  – Programmatic interface for large networks

• Cons
  – No current support for downstream customers to manage their own space (yet)
  – We hold your private key
Delegated RPKI with Up/Down

• Pros
  – You safeguard your own private key
  – Follows the IETF up/down protocol

• Cons
  – Hard to setup
  – Need to operate your own RPKI environment
Hosted RPKI in ARIN Online

To participate in Hosted RPKI you will need to do the following:

1. Generate a ROA Request Generation Key Pair.
2. Select Hosted.
3. Read and agree to the RPKI Terms of Service.
4. Enter your ROA Request Generation Public Key into the field provided.
5. Click Submit.
Hosted RPKI in ARIN Online

Organization Hosted RPKI Terms of Service

AGREEMENT

☐ I agree to the ARIN Hosted RPKI Terms of Service

You must accept the Hosted RPKI Terms of Service in order to proceed.
Access a printable .pdf version of the Hosted RPKI Terms of Service.

Enter your initials

Continue

TERMS OF SERVICE

AMERICAN REGISTRY FOR INTERNET NUMBERS, LTD.
RPKI TERMS OF SERVICE AGREEMENT

YOU MUST READ AND ACCEPT THIS RPKI TERMS OF SERVICE AGREEMENT (THIS "AGREEMENT") BEFORE ACCESSING OR USING ANY RPKI SERVICES (AS DEFINED BELOW). IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT ACCESS OR USE ANY RPKI SERVICES.
Hosted RPKI in ARIN Online

Enter your ROA Request Generation Public Key below.

ROA Request Generation Public Key:

Learn more about the ROA Request Generation Key Pair. Or, just how to create one and extract the public key.

-----BEGIN PUBLIC KEY-----
MiIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvtR8hYh/4LE0yK
hWcHL/6bJd9a2dCTw6MUS6tVam1qgdY3mMP6j8/wA/mTFO0u+4t0gUJ0
q9s6qxi2FnRn6CJfitKAr3f/9rTYP99YJiJ6bVKjJd6SOS1yUW/SdR2hYh/4LE0yK
MPr3zAuDS2QO67786Y/kpUEoCzwzG:+GM4kJLQo9/sP6yFgV1Hgux5pCMzSQu/F/nP
son5vOLkWtkuFNgm9pXRLfEdBR6MCY7eKaTeYM6EE7rUCY69SUq+SFmuwYFsg
7YNzRAErF9THlpEWqOaOxaSu/4nwLVJ2ceexsT6k4hsEWPadxJ0P3EDFHb/8/os
fwIDAQAB
-----END PUBLIC KEY-----
Hosted RPKI in ARIN Online

Hosted Certificates

Information
Each resource certificate entry displays the number of Route Origin Authorizations (ROAs), IP addresses or ranges, and Autonomous System Numbers (ASNs) covered by that certificate, and the date of the certificate’s last update. For a listing of data elements for a given resource certificate, select Details.

For more information about resource certificates, visit ARIN’s RPKI section.

ARIN

Updated: 03-20-2013

ROAs: 0  Nets: 20  ASNs: 10

Create Roa  View Resources  View Roas  View Details
Hosted RPKI in ARIN Online

Create a Route Origin Authorization (ROA) Request for SAMPLE-ORG

There are two ways to create and submit a ROA Request to ARIN:

Browser Signed ROA Request: Complete the required fields below and digitally sign the ROA Request using the private key that corresponds with the public key you registered with ARIN.

Signed ROA Request: You must construct a precisely formatted text block containing your ROA Request information, and sign it using the private key that corresponds with the public key you registered with ARIN.

- ROA Name:
- Origin AS:
- Start Date: 03-20-2013
- End Date: 03-20-2023
- Prefix: Max Length
- Private Key: Choose file, No file chosen, Key Not Loaded

* denotes optional field.
Hosted RPKI in ARIN Online

Create a Route Origin Authorization (ROA) Request for SAMPLE-ORG

There are two ways to create and submit a ROA Request to ARIN:

**Browser Signed ROA Request:** Complete the required fields below and digitally sign the ROA Request using the private key that corresponds with the public key you registered with ARIN.

**Signed ROA Request:** You must construct a precisely formatted text block containing your ROA Request information, and sign it using the private key that corresponds with the public key you registered with ARIN.
Hosted RPKI in ARIN Online

**SUBMIT SIGNED ROUTE ORIGIN AUTHORIZATION**

This information will not be saved until you click the **Submit** button below. Note that the signature is used by ARIN to ensure that the ROA Request was signed with your private key. Please verify that the information below is correct. Click **Submit** to send the request, or click **Back** to make changes.

- **ROA Name:** Test-ROA
- **Origin AS:** 23456
- **Validity Period:** 03-20-2013 to 03-20-2023
- **Resources:** 70.182.32.0/24 max length 24
- **Signature:**
  
  hjnse52POzaVFupNDqYXZVylmr78wSd4A1XEMUpj4vVmpJWWh
  nKoZRupDvB2OBtwcJJEyx4KUWPgLH18VItdCYrcyZGRxJKdTe
  qc8c0FT2QdljuD+GmUfVtvnSD26VzdYUrXM6WniTVwL96UV6sK
  bjGTx40GqD52tdJq66120pC8kY+YEIsGauVyy2hntAPI5r1Z
  GY42Fb9c1CEoEBGmt/FWy+CX6UmKsxJBLQ0NGR2XUeGKZyc2k5
  gKiSCog976Vntt88/2jOm1GkYQ0vkb6uyyy+yYUKrCc+GyNqP
  YyPAvQAq61jY1DXMhDTSjWdQRI2dNQBzMmoD0gm9A==
Your ROA request is automatically processed and the ROA is placed in ARIN’s repository, accompanied by its certificate and a manifest. Users of the repository can now validate the ROA using RPKI validators.
Delegated with Up/Down

Up/Down RPKI
To participate in Up/Down Delegated RPKI you will need to do the following:

2. Select Up/Down.
3. Read and agree to the RPKI Terms of Service.
4. Submit your UpDown Identity.xml.
5. Click Submit.

Up/Down
Delegated with Up/Down
Delegated with Up/Down
Delegated with Up/Down

- You have to do all the ROA creation
- Need to setup a CA
- Have a highly available repository
- Create a CPS
Updates within RPKI outside of ARIN

- The four other RIRs are in production with Hosted CA services
- ARIN and APNIC have delegated working for the public
- Major routing vendor support
- Public domain routing code support through Quagga and BIRD
ARIN Status

• Hosted CA deployed 15 Sept 2012
• Web Delegated CA deployed 16 Feb 2013 (deprecated from lack of use)
• Delegated using “Up/Down” protocol deployed 7 Sept 2013
• RESTful interface deployed 1 Feb 2014
## RPKI Usage

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certified Orgs</strong></td>
<td>47</td>
<td>68</td>
<td>108</td>
<td>153</td>
<td>187</td>
<td>220</td>
<td>250</td>
<td></td>
</tr>
<tr>
<td><strong>ROAs</strong></td>
<td>19</td>
<td>60</td>
<td>106</td>
<td>162</td>
<td>239</td>
<td>308</td>
<td>338</td>
<td>370</td>
</tr>
<tr>
<td><strong>Covered Resources</strong></td>
<td>30</td>
<td>82</td>
<td>147</td>
<td>258</td>
<td>332</td>
<td>430</td>
<td>482</td>
<td>528</td>
</tr>
<tr>
<td><strong>Up/Down Delegated</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>