Agenda

• Resource Public Key Infrastructure (RPKI)
• Route Origin Authorizations (ROAs)
• Certificate Authorities (CAs)
• ARIN Online Overview
• Operational Test and Evaluation Environment (OT&E) Walk-through
  – Account Creation
  – Key Pair Generation
  – ROA requests
What is RPKI?

- A robust security framework for verifying the association between resource holders and their Internet resources
- “Resource Holders”
  - Regional Internet Registries (RIR)
  - Local Internet Registries (LIRs)
  - Internet Service Providers (ISPs)
  - End-user organizations (no acronym)
What is RPKI?

• A robust security framework for verifying the association between resource holders and their Internet resources

• “Resource Holders”
  – Regional Internet Registries (RIR)
  – Local Internet Registries (LIRs)
  – Internet Service Providers (ISPs)
  – End-user organizations (no acronym)
Key Elements of RPKI

- **Resource Certificates**
  - verifiable digital statement that an Internet number resource has been registered by that RIR

- **Route Origin Authorizations (ROAs)**
  - cryptographically signed object that states which Autonomous System (AS) is authorized to originate a particular prefix or set of prefixes
Certificate Authorities (CAs)

• A CA is any entity that issues digital certificates
• Hosted RPKI
  – ARIN is the CA
• Delegated RPKI
  – Direct resource holders act as a CA for their customers
Hosted RPKI Requirements

1. IPv4 or IPv6 resources obtained directly from ARIN

2. A signed RSA or LRSA covering the resources you wish to certify

3. An ARIN Online account linked to an admin, tech, or abuse Point of Contact (POC) with authority to manage the resources you wish to certify
Before signing up, you must have:

- IPv4 or IPv6 resources obtained directly from ARIN
- A signed RSA or LRSA covering the resources you wish to certify
- An ARIN Online account linked to an admin or tech Point of Contact (POC) with authority to manage the resources you wish to certify
- An Up/Down identity
Delegated RPKI Requirements

• Once you become a participant, you must:
  – Exchange your public key associated with your Delegated RPKI private key with ARIN via ARIN Online
  – Create an infrastructure in which to host a CA, both hardware- and software-wise
  – Perform all work required for maintaining a CA and publishing a Certificate Practice Statement
  – Create an RPKI repository in which to host:
    • Resource certificates
    • ROAs
    • Manifest
    • Certificate Revocation List
A Note about Early Registration Transfer (ERX)

- ERX resources: Resources allocated before the Regional Internet Registries (RIRs) came about
- Many of these are still managed by ARIN
- Some ERX resources may not be eligible for RPKI until ARIN coordinates further with other RIRs
ARIN’s Certificate Authority

- ARIN’s CA Contains:
  - Resource certificates
  - ROAs
  - Manifest
  - Certificate Revocation List
ARIN Online Account Creation

1. Go to www.arin.net and select “new user?”
2. Complete this form

Account Setup

Every individual who manages organization or resource records should create an ARIN Online account using an individual e-mail address. Unlike POC records, ARIN Online accounts cannot use role e-mail addresses, nor should they be shared, or transferred to another person. Individuals can take ARIN Online accounts with them if they move or change jobs because accounts can be unlinked from POC, organization and resource records.

Please register your account by completing the form below.

USERNAME & PASSWORD

Username requirements: minimum of 6 characters
Password requirements: minimum of 8 characters; must contain at least 3 of the following 4 items:
1. Any uppercase letter (A,B,C,...)
2. Any lowercase letter (a,b,c,...)
3. Any number (1, 2, 3,...)
4. Any special character from the following set: / ! @ # $ % ^ & _ - + = , . < >

Other characters are permissible.
Username and password are case sensitive.

*E-mail:

*Username:

*Password:

*Confirm Password:

CONTINUE
3. Challenge Question/Math Problem

Account Setup

**CHALLENGE QUESTIONS**

Select your challenge questions from the drop-down lists and provide an answer. If you forget your username, you will be prompted to re-answer these questions to verify your identity.

* denotes required field

* Challenge Question 1: Please select a challenge question.
* Challenge Answer 1:
* Challenge Question 2: Please select a challenge question.
* Challenge Answer 2:

**SECURITY**

* What is 1 + 2?:

The mathematical equation enables us to distinguish if you are a human or a malicious bot.

CONTINUE
ARIN Online
Account Creation

4. Check your email!

```
American Registry for Internet Numbers
To:
Confirm ARIN Web Account Registration

We received a request to create an ARIN Web account for
To confirm your account, please click the URL below:

https://www.arin.net/public/confirmRegistration.xhtml?confirmationCode=963598f2-7776-4929-bff3-a2ab7f85800d

You must confirm your account to be able to log in.
You must confirm your account within 24 hours of this message being sent
or you will need to register again.

If clicking the above URL doesn’t work, copy and paste it into your browser.

If you did not request an ARIN Web account,
please contact us at hostmaster@arin.net or +1.703.227.0660.

Sincerely,

ARIN Registration Services Department
```
ARIN Online
Account Creation

4. Check your email!

ACCOUNT REGISTRATION

ACCOUNT CONFIRMED

Your ARIN Web account has been confirmed. Log in using the username and password you created when you registered.
Participating in RPKI

1. Log into ARIN Online
Participating in RPKI

2. Select ORGANIZATION DATA
3. Select an Organization Identifier (Org ID)
Participating in RPKI

4. Select Manage RPKI
5. Select “Hosted”

**Hosted RPKI**

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.
Participating in RPKI

6. Agree to the RPKI Terms of Use

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.

1. INTRODUCTION

a. American Registry for Internet Numbers, Ltd. (“ARIN”), a Virginia nonprofit corporation, is a Regional Internet Registry serving the United States, Canada, and specific designated islands in the Caribbean Sea and North Atlantic Ocean (collectively, the “ARIN Service Region”), and is responsible for the registration, administration, and stewardship of Internet number resources in the ARIN Service Region. ARIN has developed a Resource Public Key Infrastructure (“RPKI”), which may also be referred to as “Resource Certification.” RPKI is an emerging security framework to assist verifying the association between organizations and their Internet number resources. A further description of the Resource Certification can be found on ARIN’s Website located at https://www.arin.net (the “Website”), provided that such description is for informational purposes only and shall not form part of this Agreement.

b. The Resource Certification made available to You and the related services provided by ARIN under this Agreement (collectively, the “RPKI Services”) are subject to the terms and conditions of this Agreement, ARIN’s Certification Practice Statement for Resource Certification (“CPS”), and other policies and procedures that ARIN may adopt from time to time applicable to RPKI or any RPKI Services (the “RPKI Policies”) that are or will be published by ARIN on ARIN’s Website. This Agreement, along with the RPKI Policies, constitutes the entire agreement between You and ARIN regarding the RPKI Services and supersedes all prior agreements, understandings, and communications between You and ARIN relating to the RPKI Services.

2. USE OF RPKI SERVICES

a. You agree to use the RPKI Services in accordance with the terms of this Agreement, the RPKI Policies, and in a manner consistent with the intended use of the RPKI Services. You further agree to use the RPKI Services in a manner that is not fraudulent or otherwise illegal, and that does not violate any applicable laws or regulations.

3. CONFIDENTIALITY

a. You agree to maintain the confidentiality of any confidential information disclosed to You by ARIN or any third party in connection with the RPKI Services, and to use such information only for the purposes authorized by this Agreement.

4. NO PATIENT PRIVACY RIGHTS

a. You understand and agree that the RPKI Services do not provide any medical or other professional advice, diagnosis, consultation, treatment, or therapy. The RPKI Services do not replace the need for professional medical or other professional advice, diagnosis, consultation, treatment, or therapy.

5. LIMITATION OF LIABILITY

a. ARIN shall have no liability for any damage, loss, or expense incurred by You as a result of the use or inability to use the RPKI Services, or as a result of any error, omission, interruption, deletion, defect, delay in operation or transmission, communications line failure, or any other cause beyond ARIN’s control.

6. TERMINATION

a. ARIN may terminate this Agreement at any time for any reason, without notice.

7. GOVERNING LAW

a. This Agreement shall be governed by and construed in accordance with the laws of the State of Virginia, without giving effect to any choice or conflict of law provision or rule.

8. DISPUTES

a. Any dispute arising out of or in connection with this Agreement or the RPKI Services shall be resolved by arbitration in accordance with the rules of the American Arbitration Association.

9. ADDITIONAL TERMS

a. This Agreement shall be deemed to include any other terms that may be applicable to the RPKI Services, as determined by ARIN in its sole discretion.

10. ENTIRE AGREEMENT

a. This Agreement constitutes the entire agreement between You and ARIN regarding the RPKI Services, and supersedes all prior agreements, understandings, and communications between You and ARIN relating to the RPKI Services.

11. MISCELLANEOUS

a. This Agreement may not be assigned by You without the prior written consent of ARIN.

b. The failure of ARIN to exercise or enforce any right or provision of this Agreement shall not constitute a waiver of such right or provision.

c. If any provision of this Agreement is held to be invalid or unenforceable, such provision shall be struck and the remaining provisions shall be enforced.

d. The headings in this Agreement are for convenience only and do not affect the interpretation of this Agreement.

12. NOTICES

a. All notices required or permitted under this Agreement shall be in writing and shall be deemed given upon receipt by the party to which such notice is directed.

13. REMEDIES

a. ARIN may seek injunctive relief in addition to any other remedies available at law or equity.

b. ARIN may seek any other remedy available at law or equity.

14. ATTORNEY’S FEES

a. In the event that ARIN is required to proceed to arbitration in order to enforce any right under this Agreement, the prevailing party shall be entitled to recover its reasonable attorney’s fees and costs.

15. NO RESERVATION

a. ARIN reserves the right to modify or update the RPKI Policies at any time without notice.

16. NO AMENDMENTS

a. No amendment to this Agreement shall be effective unless agreed to in writing by both parties.
Participating in RPKI

7. Generate a 2048-bit key pair

- Save each key as a separate .pem file (public.pem and private.pem)
Participating in RPKI

8. Provide your public key

RESOURCE CERTIFICATE REQUEST FOR ORG ID
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.

Submit
Participating in RPKI

- Click Submit

ARIN will then generate a resource certificate covering your Internet number resources
Participating in RPKI

• Within “Manage RPKI” you can:
  – View which resources your certificate covers
  – View and manage your resource certificate
  – Request and manage ROAs
ROA Requests

1|1340135296|My First ROA|1234|05-25-2011|05-25-2012|10.0.0.0|8|16|

Version Number: This must be set to 1.
ROA Requests

Timestamp: This must be specified in seconds since 1 January 1970 (AKA seconds since the epoch).
ROA Requests

1|1340135296|My First ROA|1234|05-25-2011|05-25-2012|10.0.0.0|8|16|

ROA Name: This can be any name of your choosing, it is for your own identification purposes only. A ROA name can only contain letters, numbers, spaces and dash "-" characters. There may not be more than 256 characters to a name.
Origin Autonomous System (AS): The number of the AS that will be authorized to announce the IP prefix(es) you specify. You are not restricted to putting in your own AS, however you can only put in one AS per ROA. If you intend to originate your prefixes from more than one AS, you will need to create a ROA for each one.
ROA Requests

Validity Start Date: The first date for which this ROA should be considered valid. This date must be within the validity date range of your CA certificate, and expressed in mm-dd-yyyy format.
## ROA Requests

<table>
<thead>
<tr>
<th>ID</th>
<th>ROA</th>
<th>Prefix</th>
<th>Start Date</th>
<th>End Date</th>
<th>Mask</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1340135296</td>
<td>1234</td>
<td>05-25-2011</td>
<td>05-25-2012</td>
<td>10.0.0.0</td>
<td>8</td>
</tr>
</tbody>
</table>

**Validity End Date:** The last date for which this ROA should be considered valid. This date must be within the validity date range of your CA certificate, and expressed in mm-dd-yyyy format.
ROA Requests

Prefix and Prefix Length: The prefix is the range of IP addresses authorized to be announced by the AS Number you specify. This prefix must be allocated to your organization and certified by your CA certificate. The prefix length specifies the size of that IP address range.

You may include more than one prefix at a time within a ROA request. If you wish to specify more than one prefix, you must provide a Prefix, Prefix Length, and Max Length field (may be blank) for each prefix. Show the ROA when multiple prefixes are allowed

Max Length: The Max Length field is the smallest exact prefix length announcement you will allow for this route and is optional; if it is not provided then only the exact prefix entered will be specified in the ROA. Show ROA request with blank Max Length field
### ROA Requests

<table>
<thead>
<tr>
<th>ID</th>
<th>ROA</th>
<th>Origin AS</th>
<th>Start Date</th>
<th>End Date</th>
<th>Prefix</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1340135296</td>
<td>1234</td>
<td>05-25-2011</td>
<td>05-25-2012</td>
<td>10.0.0.0</td>
<td>8</td>
</tr>
</tbody>
</table>

**Trailing Vertical Bar:** This character must follow each section of the ROA request.
ROA Request Generation and Signing

Within ARIN Online (browser signed)

1. Fill in the form provided for you within ARIN Online detailing each part of the ROA Request.
2. Attach the private.pem file you created earlier.
3. Using JavaScript, the browser signs the data you provided.

Note: Your private key is never uploaded to ARIN and the signing code is run only on your computer.
ROA Request Generation and Signing

Create a Route Origin Authorization

You are creating a Route Origin Authorization (ROA) on behalf of [username] under the Resource Class: ARIN resource certificate.

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.

**Browser Signed**

- ROA Name: [field]
- Origin AS: [field]
- Start Date: 07-25-2014
- End Date: 07-25-2024
- Prefix: [field] Max Length [field]
- Private Key: [field]

**Signed**

- ROA Name: [field]
- Origin AS: [field]
- Start Date: 07-25-2014
- End Date: 07-25-2024
- Prefix: [field] Max Length [field]
- Private Key: [field]

Sign and Continue
RPKI Walkthrough

• To get started, visit:
  – https://www.ote.arin.net/public/

• For your test Public/Private key, visit:
  – https://www.arin.net/resources/ote.html
Congratulations!

“You have taken your first step into a larger world.”
– Captain Kirk
Questions?