



RPKI Tutorial

Andy Newton

Chief Engineer, ARIN

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



In order to participate in RPKI,
you will need:

1

ARIN
American Registry for Internet Numbers

192.149.25.278



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



Delegated RPKI Requirements



- 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?”

The screenshot shows the ARIN Online website interface. At the top, the ARIN logo is on the left, and a search bar is on the right. Below the logo, the text "American Registry for Internet Numbers" is visible. A navigation menu includes links for NUMBER RESOURCES, PARTICIPATE, POLICIES, FEES & INVOICES, KNOWLEDGE, ABOUT US, and FEEDBACK. On the left side, there is a "ARIN ONLINE" section with a login form. The form has fields for "username:" and "password:". The "username:" field contains the text "new user?". A large blue arrow points from the right towards the "new user?" text. Below the login form, there is a "log in" button and a link to "About ARIN Online". In the center, there is a banner for "IN ARIN ONLINE" with a blue arrow pointing left. To the right, there is a "Highlights" section with various links. Below that, there is an "Announcements" section with several news items. At the bottom right, there is a "Transfer Resources" section and a banner for "ARIN IPv4 Space Available" with a "0.28" counter and a "LEARN MORE" button.

ARIN Online Account Creation



2. Complete this form

USERNAME & PASSWORD SECURITY ACCOUNT CREATED

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[Terms of Service](#)

Username requirements: minimum of 6 characters
Password requirements: minimum of 8 characters; must contain at least 3 of the following 4 items: * denotes required field

- Any uppercase letter (A,B,C...)
- Any lowercase letter (a,b,c...)
- Any number (1, 2, 3...)
- Any special character from the following set: / ! @ # \$ % ^ & * _ - + = , . < >

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

*E-mail:

*Username:

*Password:

*Confirm Password:

[CONTINUE](#)

ARIN Online Account Creation



3. Challenge Question/Math Problem

○ ——— ● ——— ○
USERNAME & PASSWORD SECURITY ACCOUNT CREATED

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:

*Challenge Answer 1:

*Challenge Question 2:

*Challenge Answer 2:

SECURITY

*What is 1 + 2?:

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

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

The screenshot shows the ARIN Online website interface. At the top, the ARIN logo is on the left, and the text "Your IPv4 address is 10.1.34.152" is in the center. On the right, there is a "SEARCH Whois" search bar with a "SEARCH" button and links for "terms of use" and "advanced search". Below the header is a navigation menu with links: NUMBER RESOURCES, PARTICIPATE, POLICIES, FEES & INVOICES, KNOWLEDGE, ABOUT US, and FEEDBACK.

The main content area is divided into several sections:

- ARIN ONLINE**: A login section with a note "Username and password are case sensitive." It includes input fields for "username:" (with a "new user?" link) and "password:" (with an "assistance" link), and a "log in" button with a globe icon and a link to "About ARIN Online".
- PRE-APPROVAL for 8.3 Transfers NOW AVAILABLE IN ARIN ONLINE**: A blue banner with a pushpin icon.
- Announcements**: A section with a feed icon, listing several announcements with dates and titles, such as "Participate in the Public Policy Process" (Wed, 01 April 2015) and "2014 Annual Report Now Available" (Mon, 30 March 2015). It includes an "Announcement Archives" button.
- NRO**: A section for the Number Resource Organization, stating "ARIN is a member of the Number Resource Organization." It lists two announcements: "Comment Phase Open For 2015 ICANN Board Seat 9 Election" (9 February 2015) and "Final Proposal of the Internet Number Community for the IANA Stewardship Coordination Group." (15 January 2015). It includes an "NRO Archives" button.
- Highlights**: A section with a list of links: Request Resources, Waiting List for Unmet Requests, Draft Policies & Proposals, Internet Governance, Resource Revocation and Reinstatement, Site Search, IPv6 Info Center, New to ARIN?, Submit Payment, Legacy Resource Information, Billing Info Management, ARIN Mailing Lists, and Jobs @ ARIN.
- Transfer Resources**: A section with a circular arrow icon and a "More Information..." link.
- ARIN IPv4 SPACE AVAILABLE**: A blue banner showing "0.28 /Bs IN AGGREGATE" and "NOW IN PHASE 4" with a "LEARN MORE" button.

Participating in RPKI



2. Select ORGANIZATION DATA

Welcome,

WELCOME BACK

MESSAGE CENTER

WEB ACCOUNT

POC RECORDS

ORGANIZATION DATA

MANAGE & REQUEST RESOURCES

PAYMENTS & BILLING

TRANSFER RESOURCES

TRACK TICKETS

DOWNLOADS & SERVICES

ASK ARIN

log out

ARIN Online is a secure portal through which individuals and organizations may manage their ARIN records, request information, and view their account information. This is a one-hand menu to the menu.

IANA Stewardship TRANSITION

RECENTLY IMPLEMENTED FUNCTIONALITY

- > IPv4 Pre-approvals within ARIN Online (January 2015)
- > IPv4 pre-approval amounts added organization details page (December 2014)
- > Transfers between Specified Recipients within the ARIN Region (September 2014)
- > DNSSEC Improvements (September 2014)
- > 2010.7 IP whois community problem reporting system (July 2014)
- > 2014.6 RPKI ROAS WITH AN ORIGIN OF AS0 (July 2014)
- > 2013.15 AVAILABILITY OF ARIN ONLINE MESSAGES TO ALL POCs OF AN ORG ID (July 2014)
- > 2013.13 AVAILABILITY OF TICKET INFORMATION TO ALL POCs OF AN ORG ID (July 2014)
- > 2011.7 DISPLAY AGREEMENTS ASSOCIATED WITH ORGANIZATIONS (July 2014)

[View a full listing of implemented functionality](#)

Participating in RPKI



3. Select an Organization Identifier (Org ID)

Welcome, Andrew

MESSAGE CENTER (2)

WEB ACCOUNT

POC RECORDS

ORGANIZATION DATA

MANAGE & REQUEST RESOURCES

PAYMENTS & BILLING

TRANSFER RESOURCES

TRACK TICKETS

DOWNLOADS & SERVICES

ASK ARIN

log out

ORGANIZATION DATA

If your only responsibility is to manage the billing information for an organization, please go to [PAYMENTS & BILLING](#) to request billing authorization for your Org ID.

ORG IDS

Your ARIN Web account is linked to an Admin, Tech, Abuse, NOC and/or DMR Point of Contact for the following Organization record(s). Click the Org ID to view detailed information. Authorized users can also request ASNs or IP Addresses on behalf of the organization by selecting an Org ID followed by the "request resources" action.

If your Org ID does not have a valid Admin or Tech POC, you can [recover your Org ID](#).

ORG ID	NAME
ARINOPS	ARIN Operations

Org Actions

 create

Participating in RPKI



4. Select Manage RPKI

Welcome, Andrew

MESSAGE CENTER (2)

WEB ACCOUNT

POC RECORDS

ORGANIZATION DATA

MANAGE & REQUEST RESOURCES

PAYMENTS & BILLING

TRANSFER RESOURCES

TRACK TICKETS

DOWNLOADS & SERVICES

ASK ARIN

[log out](#)

ORGANIZATION DATA

Information

Only the Admin and Tech POCs associated with an organization may modify the organization record. If this organization record has incorrect or missing Admin and Tech POCs, you can [recover your Org ID](#).

ORGANIZATION INFO

Org ID: **ARINOPS**
Name: **ARIN Operations**
Address: **3635 Concorde Pkwy
Suite 200
Chantilly, VA 20151
UNITED STATES**

OTHER INFO

Registered Date: **09-07-2012 18:41:45**
Last Modified Date: **06-30-2014 14:21:24**

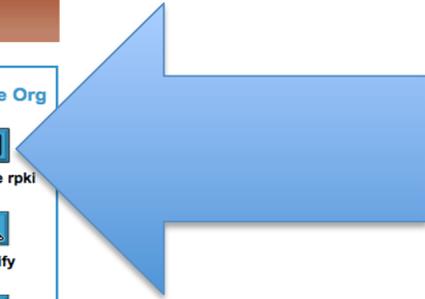
ORGANIZATION POINTS OF CONTACT

POCs associated with your organization that have not been validated according to NRPM Policy 3.6.1 are noted below. If your ARIN Web account is linked to the POC, please verify your Whois information is accurate. If your ARIN Web account is not linked to the POC, please encourage your colleagues to verify their POC information.

Admin POC: **~~KOSTEG-ARIN~~ Unvalidated**
Name: **Mark Kosters**

Manage Org

- manage rpk**
- modify**
- request name change**
- request resources**
- request transfer pre-approval**
- transfer**
- billing info**



Participating in 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.

Hosted ←

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 a 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



Participating in RPKI



7. Generate a 2048-bit key pair

Online RSA Key Generator

Key Size 1024 bit ▾

Generate New Keys

- Visit <http://travistidwell.com/jsencrypt/demo/>
- 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

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



- **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



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

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.

ROA Requests



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

roa request

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



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

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



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

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



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

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 [Clear](#)

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 [Clear](#)

ROA Requests



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

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



A Create a Route Origin Authorization ?

You are creating a Route Origin Authorization (ROA) on behalf of _____ 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 | Signed

ROA Name: ?

Origin AS: ?

Start Date: ?

End Date: ?

Prefix: / Max Length ^{*} ?

Private Key: no file selected

This key will not be uploaded to ARIN.

* denotes optional field

36

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?