

The logo for ARIN Training, featuring a stylized orange flame icon to the left of the text "ARIN Training".

ARIN Training

In order to get the most out of the lab portion of our training,
please make sure you have the following:



Java 8 JDK



Open SSL



An ARIN online account



**A POC linked to your ARIN
online Account**

Set Up

Requirements

In order to complete this process you must have the following:

1. ARIN Online Account
2. POC linked to your account
3. Open SSL
4. A computer onto which you can install the RIPE RPKI validator

ARIN has created an RPKI instance within its Operational Test and Evaluation environment (OT&E) for those wishing to experiment with RPKI without affecting production data. This exercise is described using that environment.

Check your account

1. Visit <https://account.ote.arin.net/public/login>
2. Log In as you would in your normal ARIN online account.
3. Verify you have a POC handle.
4. Verify you have an Org ID.



Creating Your Key Pair

1. Open a terminal window.
2. Enter the following command to start OpenSSL:
`openssl`
3. To generate a ROA Request Generation Key Pair enter the following command:

```
OpenSSL> genrsa -out orgkeypair.pem 2048
```

- o This command saves the key pair as a file named `orgkeypair.pem`

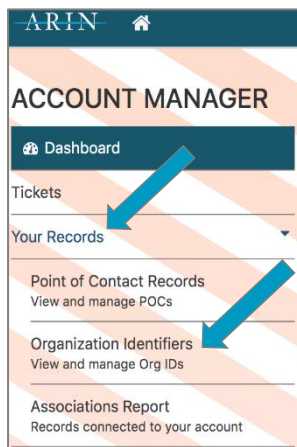
- To extract the public key so you can enter it in ARIN Online, enter the following command:

```
OpenSSL> rsa -in orgkeypair.pem -pubout -outform PEM -out org_pubkey.pem
```

- This command saves it as a file named `org_pubkey.pem`

Submitting a Certificate Request

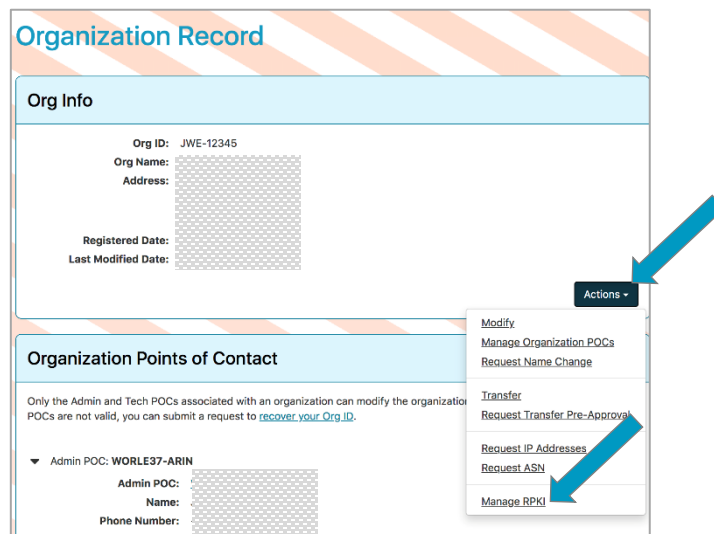
- After logging into <https://account.ote.arin.net/public/login>, select **Your Records > Organization Identifiers** from the left side navigation menu.



- Choose the organization for which you want to configure RPKI.

Org Handle	Org Name
JWE-12345	

- Choose **Actions** and select **Manage RPKI**.



Organization Record

Org Info

Org ID: JWE-12345
 Org Name:
 Address:
 Registered Date:
 Last Modified Date:

Organization Points of Contact

Only the Admin and Tech POCs associated with an organization can modify the organization. POCs are not valid, you can submit a request to [recover your Org ID](#).

Admin POC: WORLE37-ARIN
 Admin POC:
 Name:
 Phone Number:
 Email:

Actions:

- Modify
- Manage Organization POCs
- Request Name Change
- Transfer
- Request Transfer Pre-Approval
- Request IP Addresses
- Request ASN
- Manage RPKI

4. In the **Hosted RPKI Section**, choose **Configure Hosted**.
5. Paste your public key that you created into the **Public Key** field and Choose **Submit**.

Request Resource Certificate for Hosted RPKI

Use separate software to generate a ROA Request Generation Key Pair for Org ID **JWE-12345** and extract the public key. Paste the public key from the ROA Request Generation Key Pair here.

Public Key:

```

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCQA8AMIIBCgKCAQEAsC9hlyNXAT5y/8GBVz4C
g1T8OutF3aXt1sS3c+YZz8mex6daPTaAcuxGA5eloDSXd4ikW3BTu8CkSyYORxL
Qut5mFrG91Mzk3nMteE9RbLlamC+2Jhuaf3XnV3mAFMKTpuUTCHDe8ZqQaH/HJ0t
K7mfsOzQAkshN/atHZC2SawW7kvwOlvcArZYyz+7ELstj8NmBk9v1vhCbdP5k
/WRk+8XzGEipDyHrVduxk1g1JA+mqJebga2E9mKl8BwCoDXuRu5mlT7womj/KHK
c8XEYWoabZW1xg+2DXip0CotU4NHAFHzi+y1pz+U1TgZpZ3CWoBOXWTxkr6NT/C
TwIDAQAB
-----END PUBLIC KEY-----

```

Learn more about the [ROA Request Generation Key Pair](#) or how to [create a key pair and extract the public key](#).

Submit

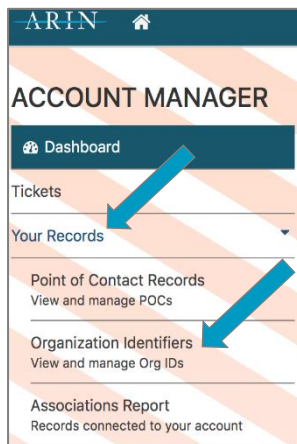
Hint:

Using a text editor or other app, open the org_pubkey.pem file and copy and paste it into the **Public Key** Field.

- Choosing **Submit** generates a ticketed request for ARIN to generate a resource certificate covering your Internet number resources.

Creating a ROA

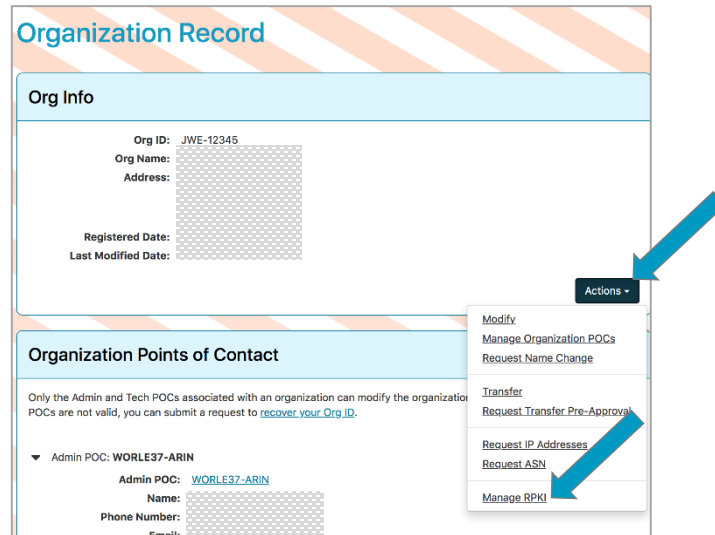
1. After logging into <https://account.ote.arin.net/public/login>, select **Your Records > Organization Identifiers** from the navigation menu.



2. Choose the organization for which you want to configure RPKI.

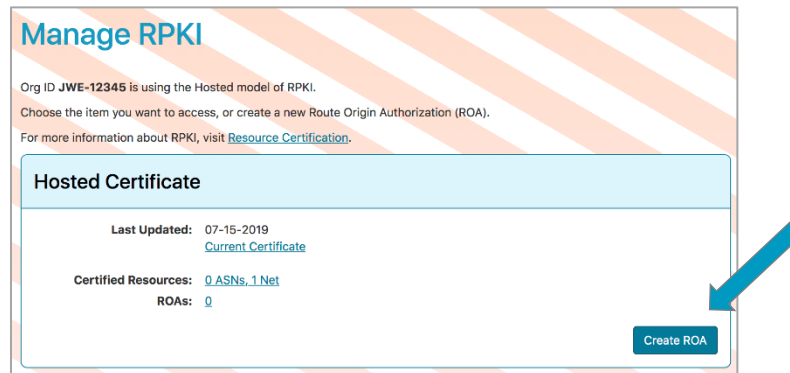
Organizations Associated with Your User Account	
Organizations are associated with your account if you are linked to any Point Voting Contact.	
Org Handle	Org Name
JWE-12345	

3. Choose **Actions** and select **Manage RPKI**.



The screenshot shows the 'Organization Record' page for Org ID JWE-12345. It includes sections for 'Org Info' and 'Organization Points of Contact'. An 'Actions' dropdown menu is open, showing options like 'Modify', 'Manage Organization POCs', and 'Manage RPKI'. A blue arrow points to the 'Manage RPKI' option.

4. Select **Create ROA**.

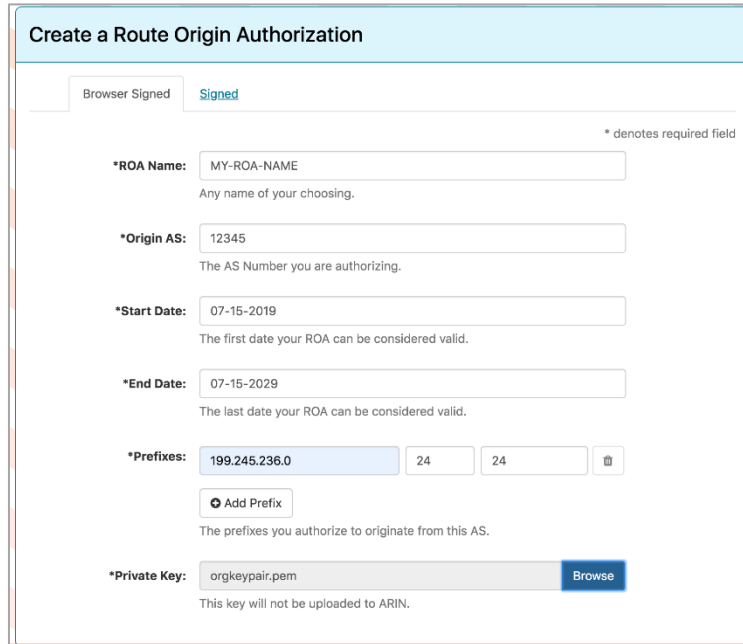


The screenshot shows the 'Manage RPKI' page for Org ID JWE-12345. It displays information about the 'Hosted Certificate' and a 'Create ROA' button. A blue arrow points to the 'Create ROA' button.

5. Select the tab corresponding to how you want to create and submit the ROA request: Browser-Signed (easiest) or Signed.

Browser Signed ROA Request

1. Complete all the fields of the form.



Create a Route Origin Authorization

Browser Signed **Signed**

* denotes required field

***ROA Name:** MY-ROA-NAME
Any name of your choosing.

***Origin AS:** 12345
The AS Number you are authorizing.

***Start Date:** 07-15-2019
The first date your ROA can be considered valid.

***End Date:** 07-15-2029
The last date your ROA can be considered valid.

***Prefixes:**

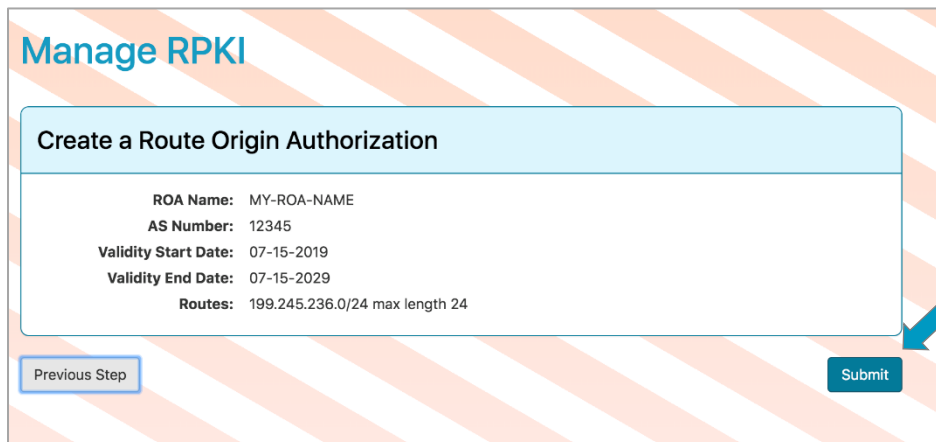
199.245.236.0	24	24	🗑️
---------------	----	----	----

➕ Add Prefix

The prefixes you authorize to originate from this AS.

***Private Key:** orgkeypair.pem **Browse**
This key will not be uploaded to ARIN.

2. In a previous step, you created a key pair. Choose **Browse** and attach that key pair file.
3. Choose **Next Step**
4. After reviewing the summary of the ROA information, choose **Submit**.



Manage RPKI

Create a Route Origin Authorization

ROA Name: MY-ROA-NAME
AS Number: 12345
Validity Start Date: 07-15-2019
Validity End Date: 07-15-2029
Routes: 199.245.236.0/24 max length 24

[Previous Step](#) [Submit](#)

Signed ROA Request

If you choose to use a signed ROA Request, you will need to create a precisely-formatted text block that includes your ROA information, and sign it using the private key that corresponds with the public key you provided to ARIN. You then copy and paste the entire signed text block into the **Signed** tab.

For step-by-step examples of using a signed ROA request, visit https://www.arin.net/resources/manage/rpki/roa_request/#using-a-signed-roa-request

RPKI Validator

The following instructions are demonstrated using the Apple Operating system; steps and commands may differ for other operating systems.

1. Visit the RIPE RPKI page and download the zipped validator file.

<https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources>

2. Extract the zip file
3. Open a terminal window
4. Change the directory that was created when the validator was unzipped:

```
cd <directory-name>
```

5. Start the application:

```
sh rpki-validator-3.sh
```

Note: the validator filename may change

6. After the application starts, bring up the validator in your web browser:

<http://localhost:8080>

7. Choose the different trust anchors to view them (RIPE/APNIC/LACNIC/AFRINIC)

Tools and Resources

Here you can find an overview of all information and tools for the Resource Certification (RPKI) service.

RIPE NCC RPKI Validator 3.1 (Updated 6 August 2019)

This application allows operators to download and validate the global RPKI data set for use in their BGP decision making process and router configuration. [Download Now](#)

System requirements: You will need a UNIX-like system with OpenJDK 8 or higher and rsync. You will also need at least 1.5GB available on your server (2GB in total if you also run the RPKI-RTR server). One (virtual) CPU should be enough. The repository objects are stored in a file-based database, rather than in memory, for which we recommend at least 10GB of available disk space.

For more information, [view the release notes](#). You can also contribute to the [project on GitHub](#).

Adding the ARIN OT&E Tal

Add the OT&E Tal to see your newly configured ROAs:

1. In a terminal window, from the base directory of the zip file, change to the preconfigured-tals directory:

```
cd <directory-name>/preconfigured-tals
```

2. Use your text editor of choice to create the tal file. For example, if using vi, enter:

```
vi arin-ote.tal
```

3. Add the text of the OT&E Tal File and save the file. The OT&E Tal File is located at: <https://www.arin.net/reference/tools/testing/#trust-anchor-locator-tal>

Restarting the Validator

1. Change to the directory where the validator is running:

Likely something such as: `directory-name>/conf/tal directory`

2. Stop the validator
3. Restart the validator
4. Return to your web browser, check the trust anchors, and verify that the OT&E TAL is listed.