Set-Up

Requirements

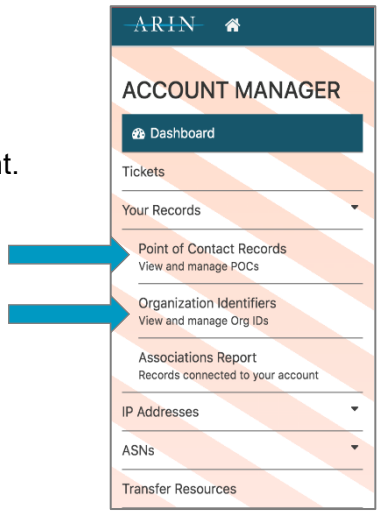
In order to complete this process you must have the following:

1. ARIN Online Account
2. POC linked to your account
3. OpenSSL or similar to generate an RSA keypair

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 Point of Contact 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
   ```

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

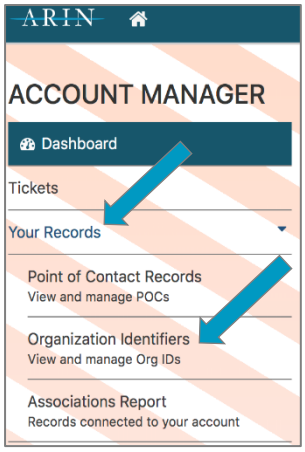
4. To extract the public key so you can enter it in ARIN Online, enter the following command:

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

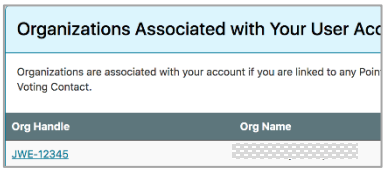
   - This command saves it as a file named `org_pubkey.pem`

Submitting a Certificate Request

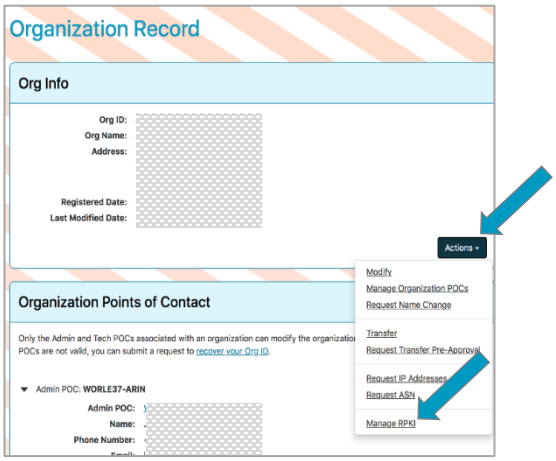
1. After logging into https://account.ote.arin.net/public/login, select **Your Records > Organization Identifiers** from the center tiles or the left side navigation menu.



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



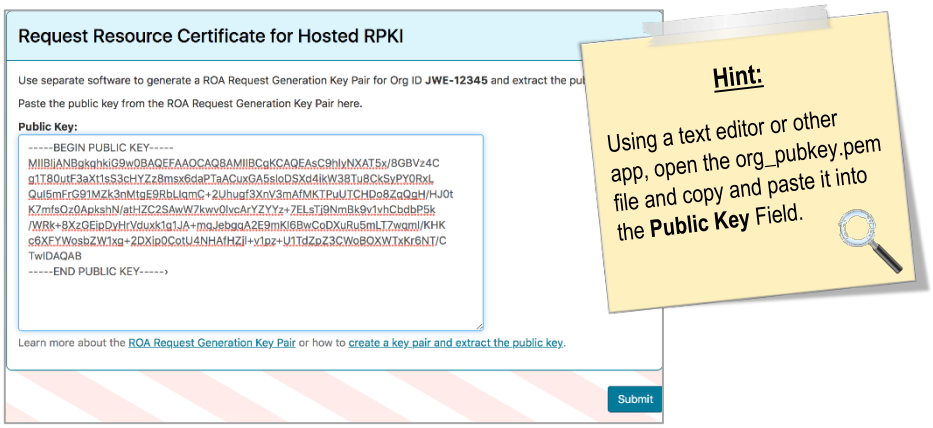
3. Choose **Actions** and select **Manage RPKI.**



Note: ARIN also offers a Delegated RPKI option for organizations that request their own delegated resource certificates and host their own Certificate Authority (CA). We have also added a Publication Service for Delegated RPKI for organizations that want to use delegated RPKI without publishing their own repositories in-house. You can learn more about these options at: https://www.arin.net/resources/manage/rpki/delegated/

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**.

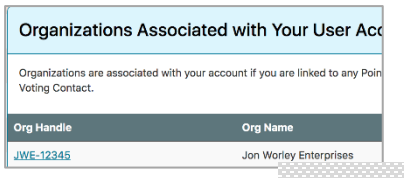


- Choosing **Submit** generates a ticketed request for ARIN to generate a resource certificate covering your Internet number resources.
- More information on this topic can be found at

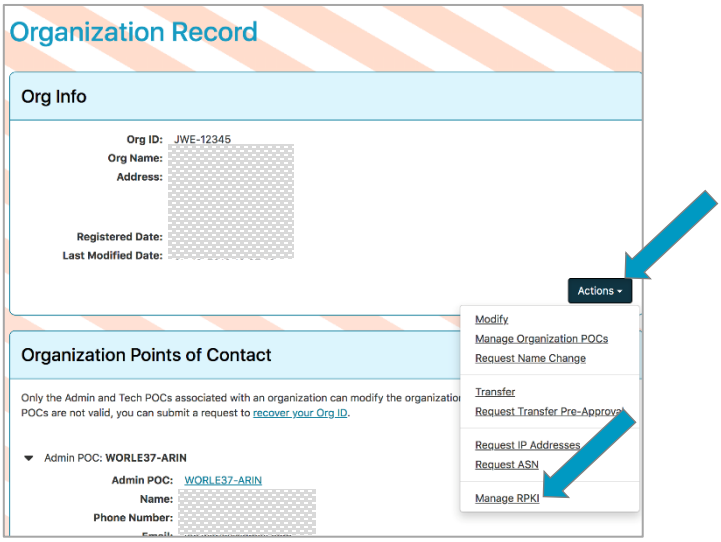
Creating a ROA using Hosted RPKI at ARIN

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

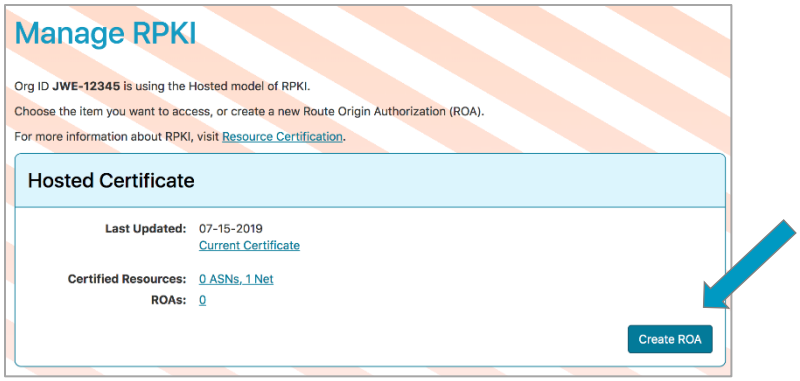
2. Choose the organization for which you want to configure RPKI.



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



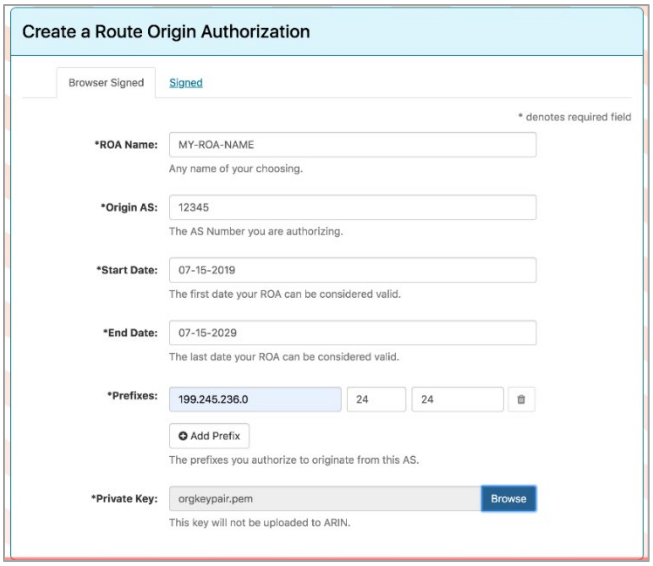
4. Select **Create ROA.**



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

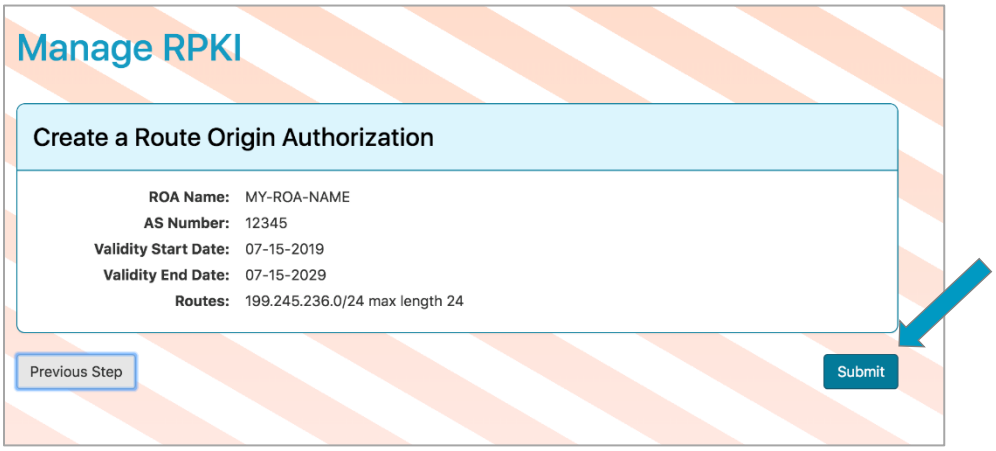
Browser Signed ROA Request

1. Complete all the fields of the form.



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**.



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