

## Set-Up

### Requirements

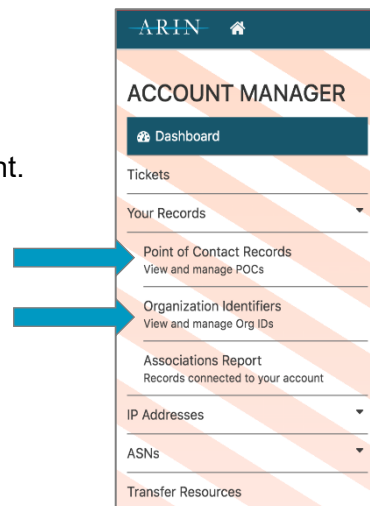
In order to complete this process you must have the following:

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:
3. To generate a ROA Request Generation Key Pair enter the following command:

```
openssl
```

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

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

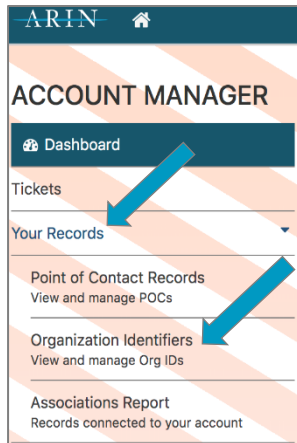
4. To extract the public key so you can enter it in ARIN Online, enter the following command:

```
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

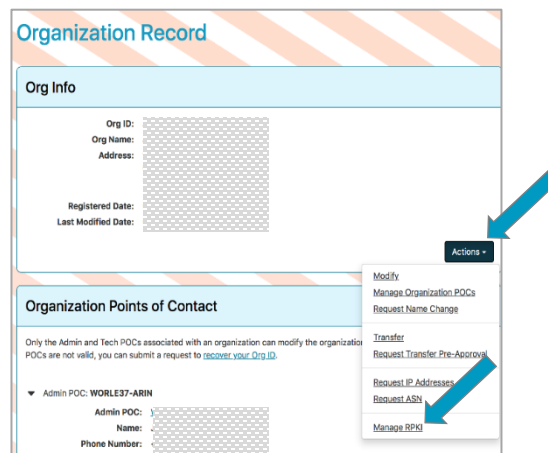
1. After logging into <https://account.ote.arin.net/public/login>, select **Your Records > Organization Identifiers** from the center tiles or the left side navigation menu.



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

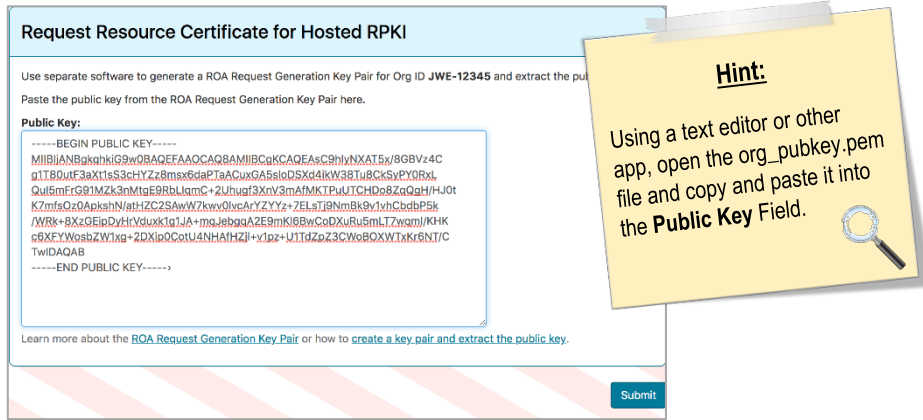
Organizations Associated with Your User Account	
Organizations are associated with your account if you are linked to any Point of Contact.	
Org Handle	Org Name
JWE-12345	

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/>

- In the **Hosted RPKI Section**, choose **Configure Hosted**.
- 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 from the ROA Request Generation Key Pair here.

**Public Key:**

```
-----BEGIN PUBLIC KEY-----
MIIBIANBgkqhkiG9w0BAQEFAAOCAG8AMIIBCAQAEAsC9hhYNYAT5v/BGBV:4C
q1T8duF38X1tS58chTZz8mss6daC7aACwGAS6wDS4H4IKW38Iu8Ck5vCYORL
Qul6mFrG8IMZk3mMtgE9RblLmnc+2Jlugf3XvY2mAMKTPuJTGHD98ZqQgHfHJot
K7mfsOz0pikshNathZC2SAwW7kws0lvcArYZYYz+7ELat9NmBK9vYhCndbP5K
/WRK+BXzGEIshDyHvduktq1JA+mgJebqaA2E9mKl6BwCoDXuRu5mLT7wamIKHK
66KEYWosbZW7kg+2DXip0CoIU4NH4HfZl+YJz+U1TdZz3CWoBOXWtKf6NT/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](#).

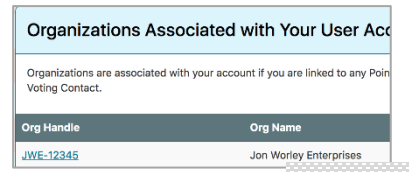
**Submit**

**Hint:**  
Using a text editor or other app, open the org\_pubkey.pem file and copy and paste it into the **Public Key** Field.

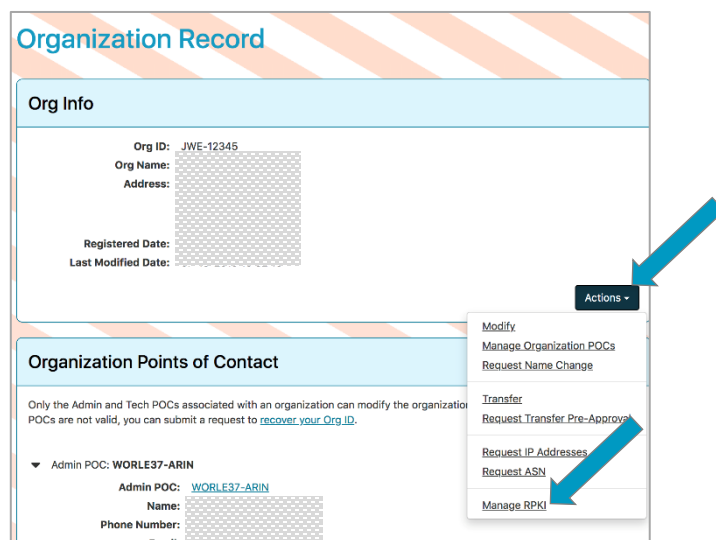
- Choosing **Submit** generates a ticketed request for ARIN to generate a resource certificate covering your Internet number resources.
- More information on this topic can be found at [https://www.arin.net/resources/ip/roa/roa.html](#)

## Creating a ROA using Hosted RPKI at ARIN

- After logging into <https://account.ote.arin.net/public/login>, select **Your Records > Organization Identifiers** from the tiles or left navigation menu.
- Choose the organization for which you want to configure RPKI.
- Choose **Actions** and select **Manage RPKI**.



Org Handle	Org Name
JWE-12345	Jon Worley Enterprises



**Organization Record**

**Org Info**

Org ID: JWE-12345

Org Name: [Redacted]

Address: [Redacted]

Registered Date: [Redacted]

Last Modified Date: [Redacted]

**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: WORLE37-ARIN

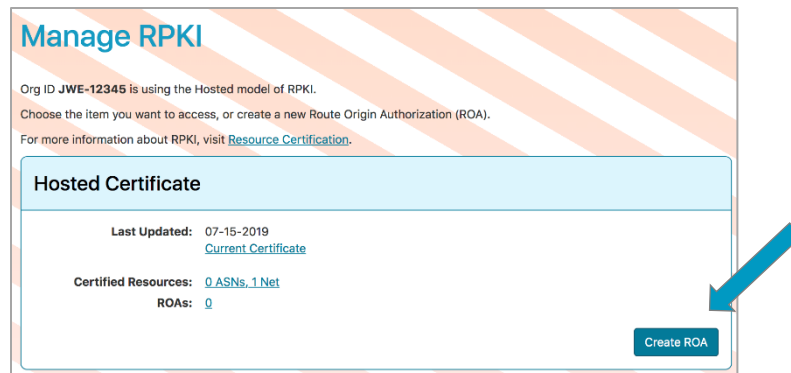
Name: [Redacted]

Phone Number: [Redacted]

**Actions**

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

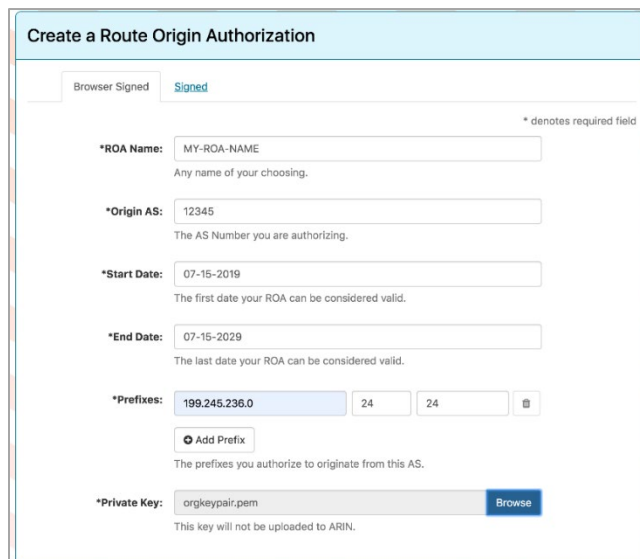
4. Select **Create ROA**.



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.



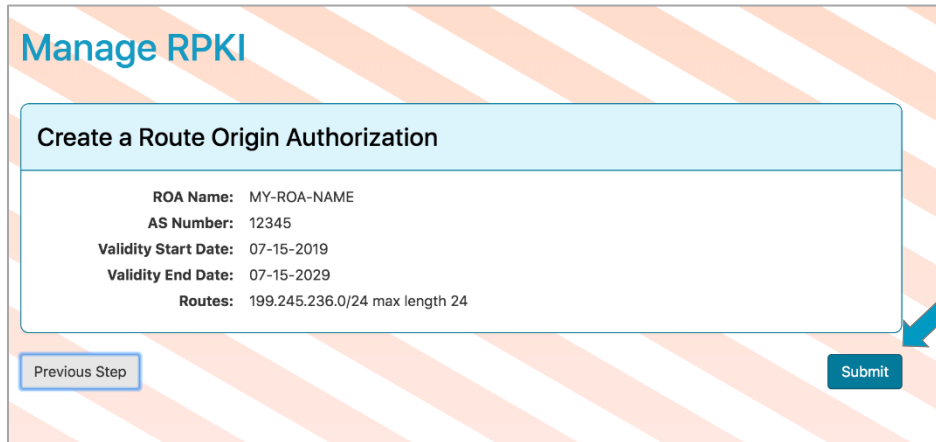
The screenshot shows the 'Create a Route Origin Authorization' form. The 'Signed' tab is selected. The form contains the following fields:

- \*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 (The prefixes you authorize to originate from this AS.)
- \*Private Key:** orgkeypair.pem (This key will not be uploaded to ARIN.)

A 'Browse' button is next to the Private Key field. A legend indicates that an asterisk (\*) denotes a required field.

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

## 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](https://www.arin.net/resources/manage/rpki/roa_request/#using-a-signed-roa-request)