



# Delegated, Hybrid, and the API: *Beyond Hosted RPKI at ARIN*

---

## **Hosted:**

An Organization uses ARIN Online

- Requests a resource certificate stored on ARIN servers
- All cryptographic components are managed by ARIN
- Org creates and maintains their ROAs

## **Delegated:**

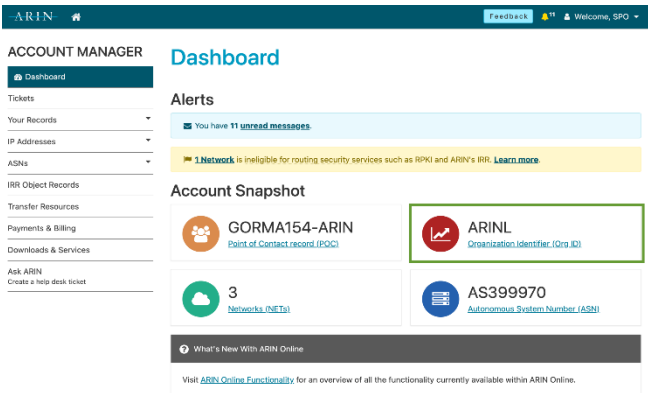
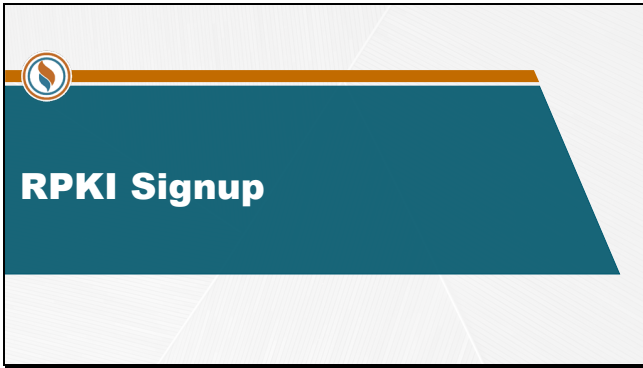
The organization has more control and independence

- Runs their own Certificate Authority (CA) to manage object signing
- Separation of the publication of cryptographic functions

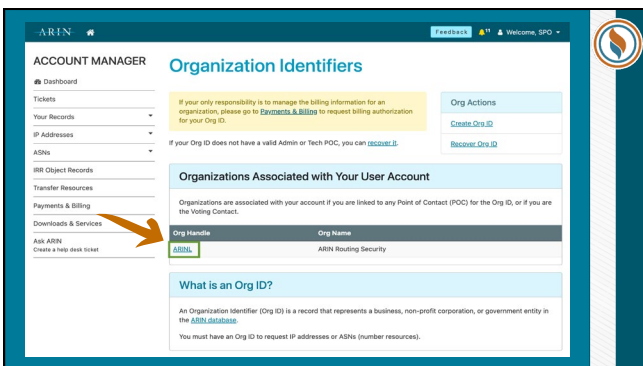
## **Delegated with Remote Publication Service (RPS):**

The organization runs the Certificate Authority

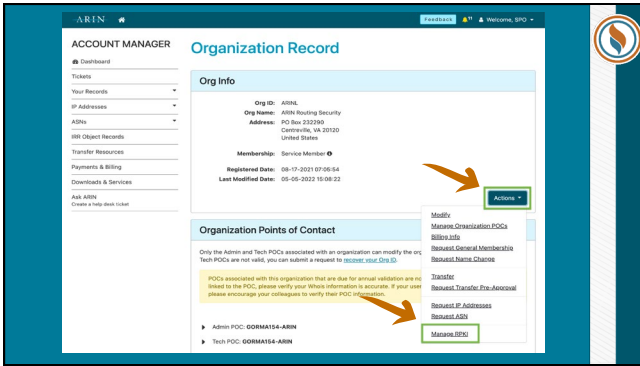
- Delegates the repository and publication services to ARIN



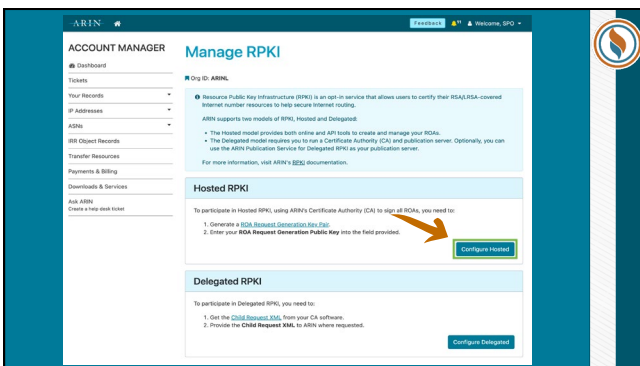
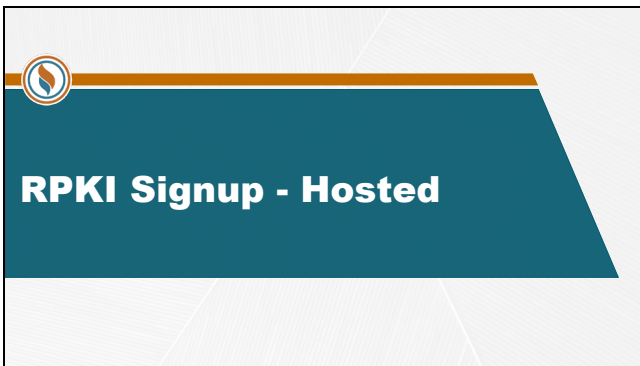
At the initial signup to use RPKI through ARIN, you will need to choose between Hosted or Delegated RPKI. On the ARIN Online Account Manager Dashboard, select the Organization Identifier (ORG ID).



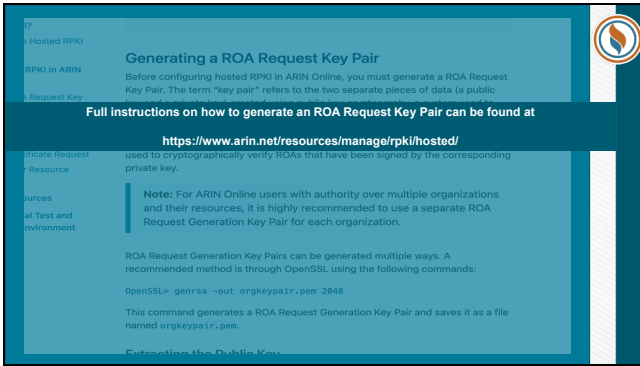
On the Organization Identifiers page, select the Org Handle for which you want to manage RPKI.



Next, on the Organization Record page, select the Actions button. Then, in the drop down menu, select Manage RPKI.



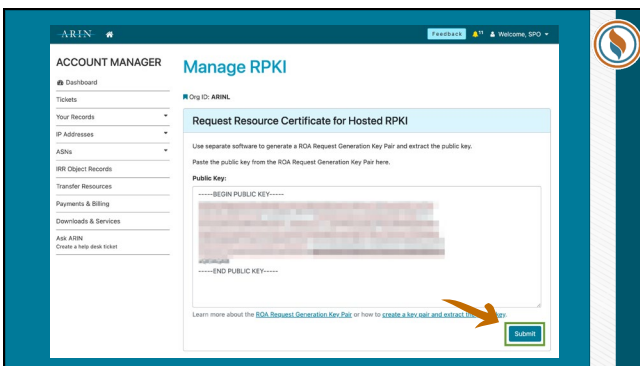
To begin setting up Hosted RPKI, select Configure Hosted on the Manage RPKI page.

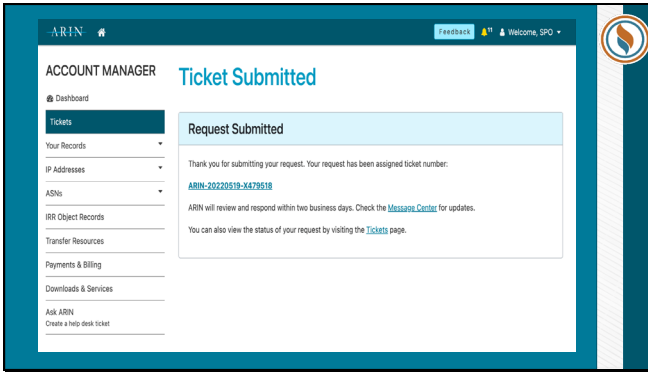


The full instructions on how to generate an ROA Request Key Pair can be found at <https://www.arin.net/resources/manage/rpki/hosted/>, as well as slides 38-41 of this presentation.

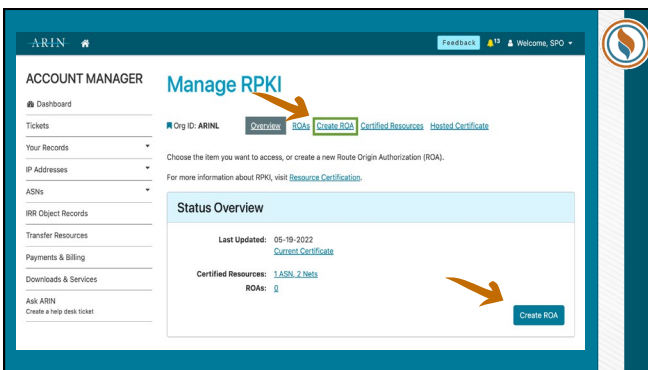
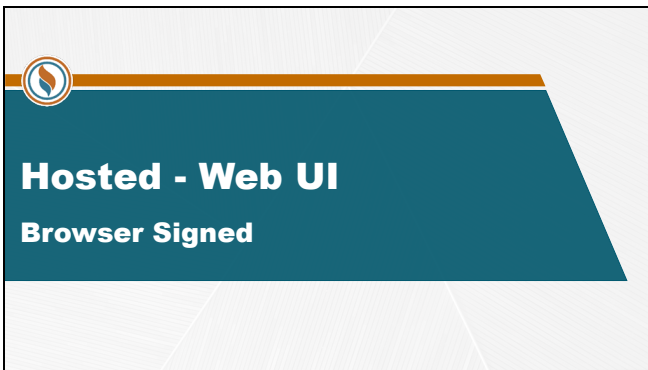
As a hosted RPKI participant, you generate and use ROA Request Generation Key Pairs to secure your ROAs and resource certificate data and cryptographically verify your identity. Your public key is provided to ARIN and is used to cryptographically verify ROAs that have been signed by the corresponding private key.

Once the RIR Request Key Pair has been generated, copy and paste the public key into the field provided and select submit.





This will complete the request, which will be assigned a ticket number. This ticket will be reviewed by ARIN, and its status can be tracked through the Tickets page.



Once your ticket has been resolved, to create a new Route Origin Authorization (ROA), select Create ROA on the Manage RPKI page.

On the RPKI: Create ROA page, select Browser Signed, complete the form provided, and select Next Step.

You will be provided with a summary of the submitted information to review. Select Previous Step to make any corrections if needed; otherwise select Submit.

This will complete the request, which will be assigned a ticket number. This ticket is part of an automated process, and its status can be tracked through the Tickets page.

# Hosted - Web UI

## Manually Signed

802-8de4-dd9f-4783-3fa0 Welcome, SPO

**Step one:** Open a terminal window and enter the following series of commands:

- This command uses echo to save your data to a text file:

**Note:** The following ROA field data is an example only, and should be replaced with content appropriate to your organization and ROA.

```
echo -n "11348135296|My First ROA|1234|85-25-2811|85-25-2812|18.8.8.8|816|" > roadata.txt
```

- This command generates the signature of the ROA data file using OpenSSL and your private key:

```
openssl dgst -sha256 -sign orgkeypair.pem -keyform PEM -out signature roadata.txt
```

- This command converts the signature to Base64 using OpenSSL.

```
openssl enc -base64 -in signature -out sig_base64
```

**Step two:** Open the sig\_base64 file in a text editor. Your signature should look something like the following example:

```
RDQW7hV/z7wC/R9VJ1c1lqgTT1g8BxPV-dtZeh3mHw@hpg4GRFzJOL6JFAG11  
n4FMQWVwFvFpYfY0GEX+T19aQvot2Se8du5FC1C5/vG1pW5+FDm801r3p9  
v0110y01puz2x10u3d/q8qcp8Kqg10+Kauw40D35H8Y1E/No6A9Ez3gMc  
9As3eT5yT2p8LFluFf8uQ2D0CvC/cU/y5m8hu5L1+v4Z0u8g5C5=wwdFp8H8  
KC08T5hw1AdeJ0yK1sv1Q=
```

These slides provide detailed instructions to complete a manually-signed ROA request.

802-8de4-dd9f-4783-3fa0 Welcome, SPO

**Step three:** In the roadata.txt file, wrap the contents of the ROA data with a Begin and End block and add the Base64 encoded signature block from the sig\_base64 file as follows:

```
-----BEGIN ROA REQUEST-----  
<ROA Request data>  
-----END ROA REQUEST-----  
-----BEGIN SIGNATURE-----  
<signature>  
-----END SIGNATURE-----
```

The file contents should now look similar to example below:

```
-----BEGIN ROA REQUEST-----  
11348135296|My First ROA|1234|85-25-2811|85-25-2812|18.8.8.8|816|  
-----END ROA REQUEST-----  
-----BEGIN SIGNATURE-----  
RDQW7hV/z7wC/R9VJ1c1lqgTT1g8BxPV-dtZeh3mHw@hpg4GRFzJOL6JFAG11  
n4FMQWVwFvFpYfY0GEX+T19aQvot2Se8du5FC1C5/vG1pW5+FDm801r3p9  
v0110y01puz2x10u3d/q8qcp8Kqg10+Kauw40D35H8Y1E/No6A9Ez3gMc  
9As3eT5yT2p8LFluFf8uQ2D0CvC/cU/y5m8hu5L1+v4Z0u8g5C5=wwdFp8H8  
KC08T5hw1AdeJ0yK1sv1Q=  
-----END SIGNATURE-----
```

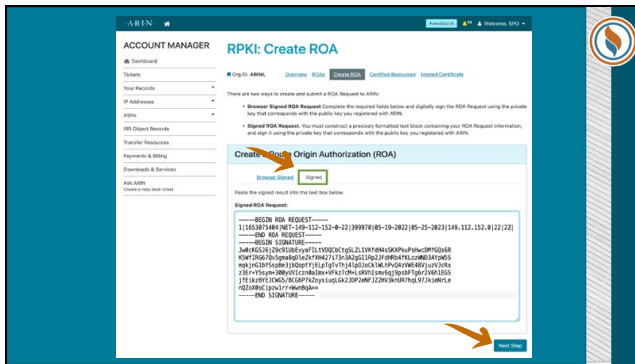
**Step four:** From the roadata.txt file, copy and paste the entire content of the request (which will appear similar to previous example) into the Signed tab in the Create a Route Origin Authorization section of ARIN Online and choose Next.

**Step:** Your ROA is processed and a ticket is generated to notify you that the ROA was created.

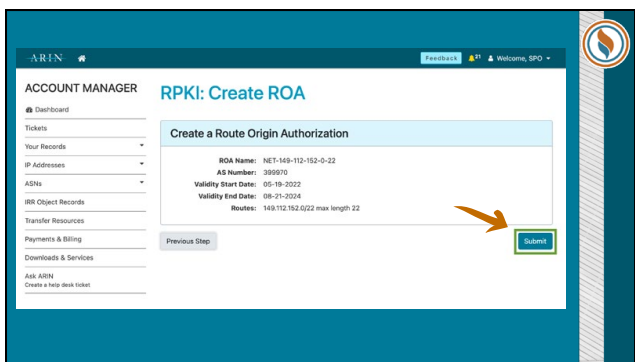
These slides provide detailed instructions to complete a manually-signed ROA request.

```
% echo -n "11653075484|NET-149-112-152-0-22|399970|05-19-2022|05-25-2023|149.112.152.0|23|23|" > roadata.txt
% openssl dgst -sha256 -sign orgkeypair.pem -keyform PEM -out signature roadata.txt
% openssl enc -base64 -in signature -out sig_base64
% cat sig_base64
JwACKG536jZ9C910bEvyafZLTV0QcCtqSLZL1VkfDh4+SKOPkUpShucDMFGQ6R
KSWfIRG670v5gmaBqDLeZkTXH427173n3A2gC1Rq2Jf4Rb4fLLeMD3AYpM5S
mqj1G02Y55pba3j3oogTYjELpTg7VTh4tp0JcK1MLpP424WE4BVjuzV3Ck
z3Er+Y5sym=380yDVIczn8aImx+Vfkz7cM+L8RVh1smV6Gj9psBfT6rZV6h1EGS
j1E1kzBfEJCWG5/BCG6P7KZ0ysLuqLGK2JDP2eNFJ2ZHV3knUR7hQ973k1eNLe
RQZ0X8C1zcd1rr+u4uBqgle=
% vi roadata.txt
-----BEGIN ROA REQUEST-----
11653075484|NET-149-112-152-0-22|399970|05-19-2022|05-25-2023|149.112.152.0|23|23|
-----END ROA REQUEST-----
-----BEGIN SIGNATURE-----
JwACKG536jZ9C910bEvyafZLTV0QcCtqSLZL1VkfDh4+SKOPkUpShucDMFGQ6R
KSWfIRG670v5gmaBqDLeZkTXH427173n3A2gC1Rq2Jf4Rb4fLLeMD3AYpM5S
mqj1G02Y55pba3j3oogTYjELpTg7VTh4tp0JcK1MLpP424WE4BVjuzV3Ck
z3Er+Y5sym=380yDVIczn8aImx+Vfkz7cM+L8RVh1smV6Gj9psBfT6rZV6h1EGS
j1E1kzBfEJCWG5/BCG6P7KZ0ysLuqLGK2JDP2eNFJ2ZHV3knUR7hQ973k1eNLe
RQZ0X8C1zcd1rr+u4uBqgle=
-----END SIGNATURE-----
Create signed (https://www.arin.net/resources/manage/rpki/roa_request#submitting-a-manually-signed-roa)
```

This capture of the Command Line interface shows formatted content necessary for a manually-signed ROA to be completed.

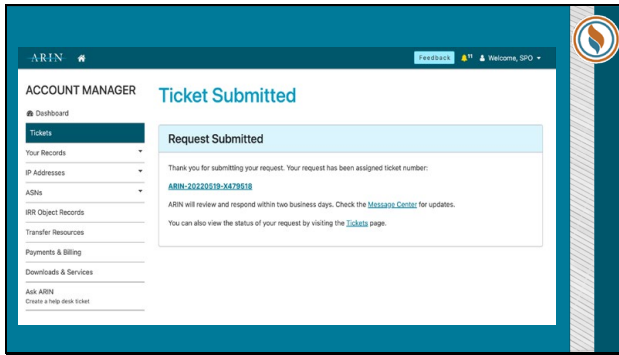


On the RPKI: Create ROA page, select Signed and paste the contents of roadata.txt and select Next Step.



You will be provided with a summary of the submitted information to review. Select Previous Step to make any corrections if needed; Otherwise select Submit.





This will complete the request, which will be assigned a ticket number. This ticket is part of an automated process, and its status can be tracked through the Tickets page.