



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:

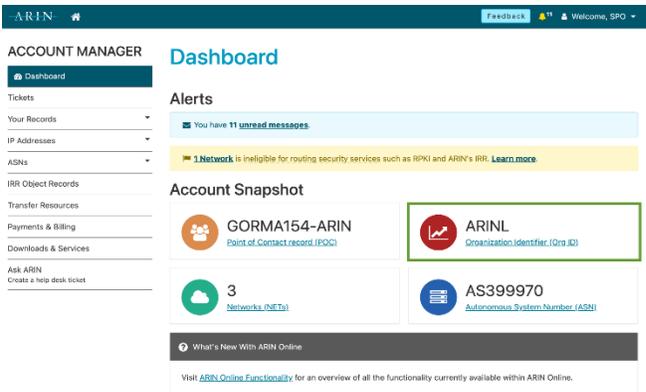
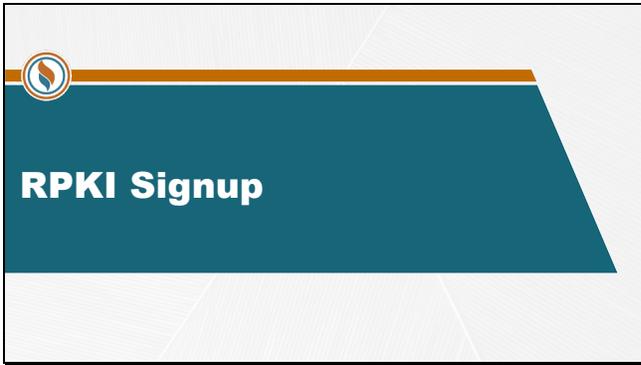
The organization has more control and independence

- 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

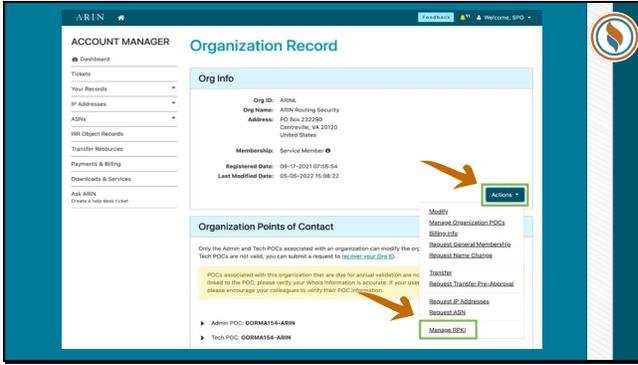
- Delegates the repository and publication services to ARIN



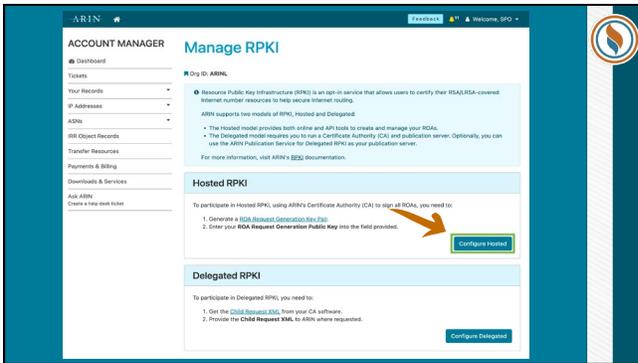
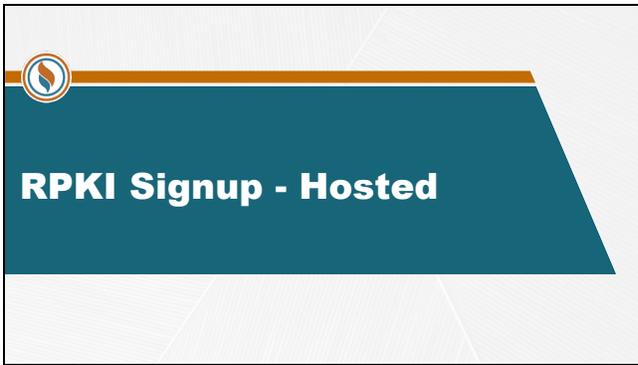
At the initial signup to use RPKI through ARIN, you will need to choose between Hosted or Delegated RPKI. On the ARIN Online Account Manager Dashboard, select the Organization Identifier (ORG ID).



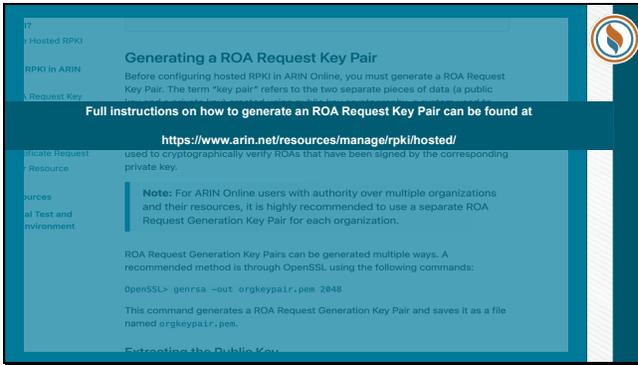
On the Organization Identifiers page, select the Org Handle for which you want to manage RPKI.



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



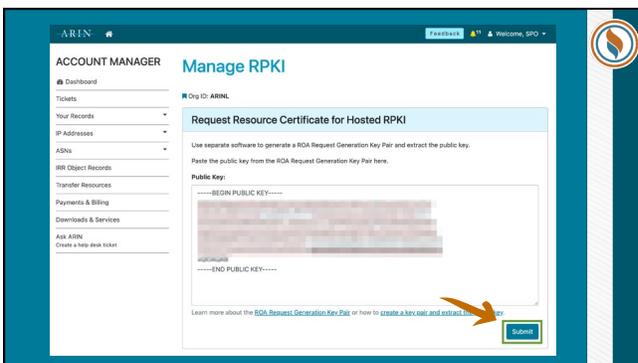
To begin setting up Hosted RPKI, select Configure Hosted on the Manage RPKI page.

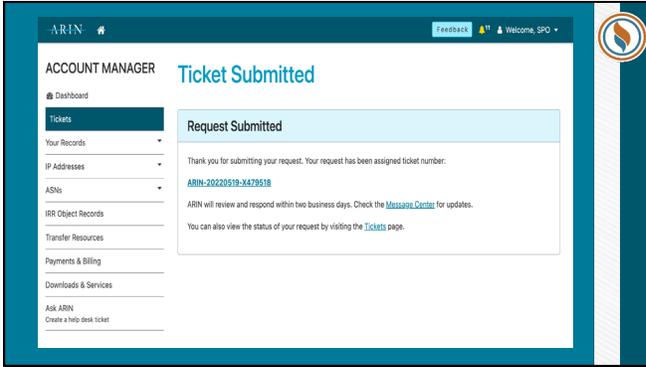


The full instructions on how to generate an ROA Request Key Pair can be found at <https://www.arin.net/resources/manage/rpki/hosted/>, as well as slides 38-41 of this presentation.

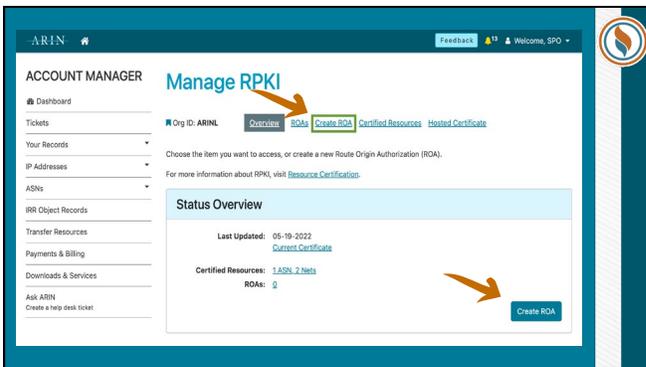
As a hosted RPKI participant, you generate and use ROA Request Generation Key Pairs to secure your ROAs and resource certificate data and cryptographically verify your identity. Your public key is provided to ARIN and is used to cryptographically verify ROAs that have been signed by the corresponding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

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

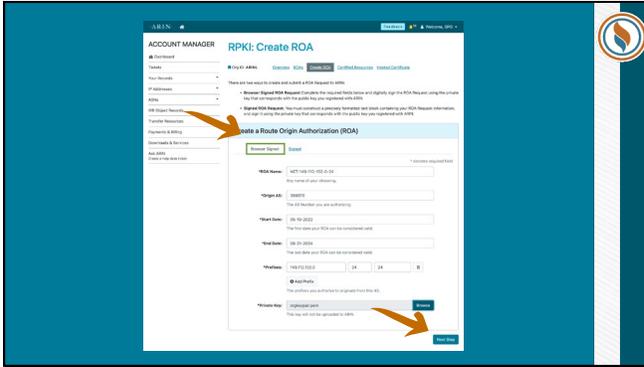




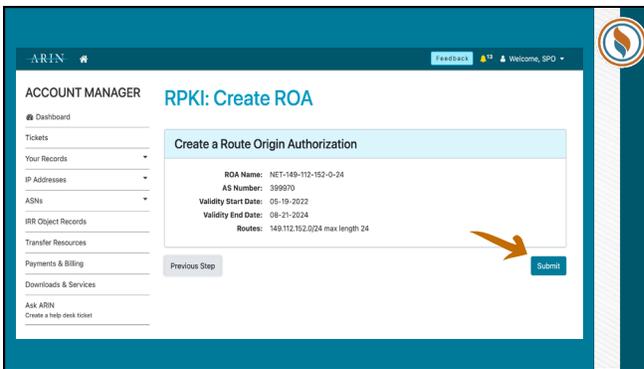
This will complete the request, which will be assigned a ticket number. This ticket will be reviewed by ARIN, and its status can be tracked through the Tickets page.



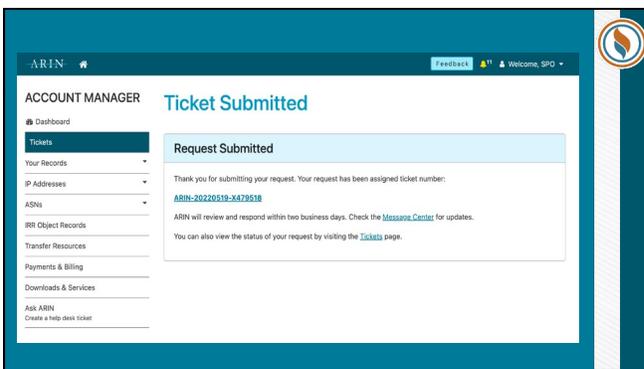
Once your ticket has been resolved, to create a new Route Origin Authorization (ROA), select Create ROA on the Manage RPKI page.



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.

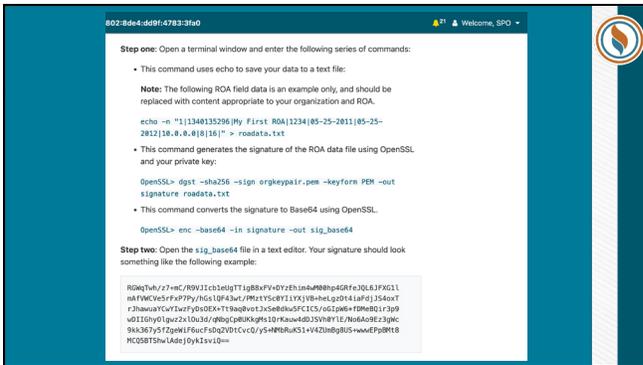


This will complete the request, which will be assigned a ticket number. This ticket is part of an automated process, and its status can be tracked through the Tickets page.



Hosted - Web UI

Manually Signed



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|8.8.8|8|16|" > 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
```

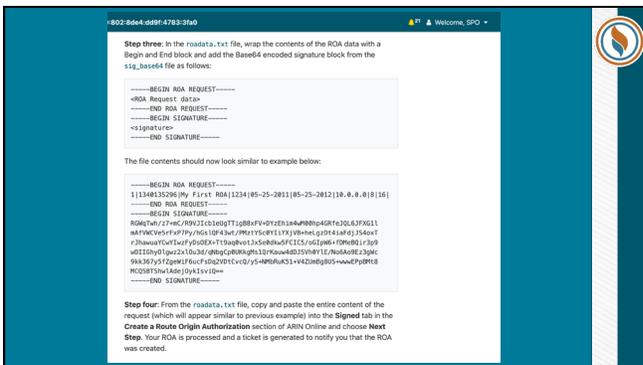
- This command converts the signature to Base64 using OpenSSL.

```
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:

```
RDQ6Tuh/z7wC/R9VJ1c31eJgTT1g8xPV-dTz2h3m4w@Bp4GRf6J0L6JFKG11
e4TfW6VvFpF7pYf9G10P43w/P9R1V98RT1X3Y8m6gD14L8F6J34wT
r2hauuTCvYtwFYyGEX+T19a@vot2k5e8du5FC1C5/0G1pW6+FDm801r3p9
w0110yY1gz2x10u3z/8BgcP8Kq9s10rKaw480J5Vh8Y1E.Nu6A89Ez3pK
9As387y5T2p8lFfauF5bQZD1CvC1/y5-m8u8u31v4E218g810c-wwdFy8F8
MC08T5hw1AdeJyK1sv1Q==
```

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



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|8.8.8|8|16|
-----END ROA REQUEST-----
-----BEGIN SIGNATURE-----
RDQ6Tuh/z7wC/R9VJ1c31eJgTT1g8xPV-dTz2h3m4w@Bp4GRf6J0L6JFKG11
e4TfW6VvFpF7pYf9G10P43w/P9R1V98RT1X3Y8m6gD14L8F6J34wT
r2hauuTCvYtwFYyGEX+T19a@vot2k5e8du5FC1C5/0G1pW6+FDm801r3p9
w0110yY1gz2x10u3z/8BgcP8Kq9s10rKaw480J5Vh8Y1E.Nu6A89Ez3pK
9As387y5T2p8lFfauF5bQZD1CvC1/y5-m8u8u31v4E218g810c-wwdFy8F8
MC08T5hw1AdeJyK1sv1Q==
-----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 Admin 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-149-112-152-0-23|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
Jw0cKGSj6|Z9C910uEvyafILVDOQCctgSLZL1VKfDH4+SOKPkuPshuCDHFGQ6R
KSWfIRG670v5gma8QDleZkT9H427173n3A2gG1Rp2Jf4Rb44FLLoND3AYpMS
mqNjGIG2Y5Sp8e3j0oogY1ELpTg7V7h41p0JOCKLMLPv042ME48V1uV3J0K
z3E+YSSym=380yUVIczn8Im+Vfkz7cmLrSVH1smV6j|9psBfT6rZV6hIEGS
jFEJk2BfE3CWC5/BC6GP7kZ0ysluoL6K2JDP2NFJZHV3kUR7h9L973kIeNrLe
RZDZ0X8C1pzd1rrr4kmsBqfse
% vi roadata.txt
-----BEGIN ROA REQUEST-----
11653075484|NET-149-112-152-0-24|399970|05-19-2022|05-25-2023|149.112.152.0|23|23|
-----END ROA REQUEST-----
-----BEGIN SIGNATURE-----
Jw0cKGSj6|Z9C910uEvyafILVDOQCctgSLZL1VKfDH4+SOKPkuPshuCDHFGQ6R
KSWfIRG670v5gma8QDleZkT9H427173n3A2gG1Rp2Jf4Rb44FLLoND3AYpMS
mqNjGIG2Y5Sp8e3j0oogY1ELpTg7V7h41p0JOCKLMLPv042ME48V1uV3J0K
z3E+YSSym=380yUVIczn8Im+Vfkz7cmLrSVH1smV6j|9psBfT6rZV6hIEGS
jFEJk2BfE3CWC5/BC6GP7kZ0ysluoL6K2JDP2NFJZHV3kUR7h9L973kIeNrLe
RZDZ0X8C1pzd1rrr4kmsBqfse
-----END SIGNATURE-----

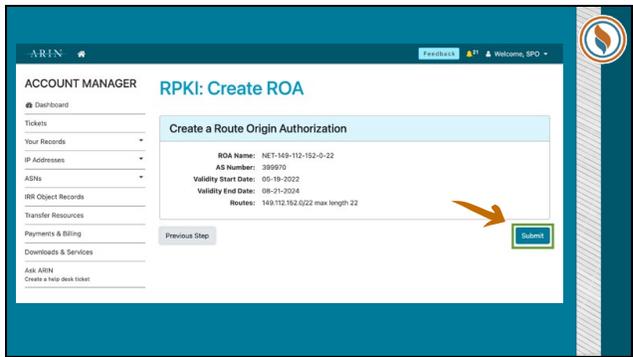
```

Create signed (https://www.arin.net/resources/manage/rpki/roa_request#submitting-a-manually-signed-roa)

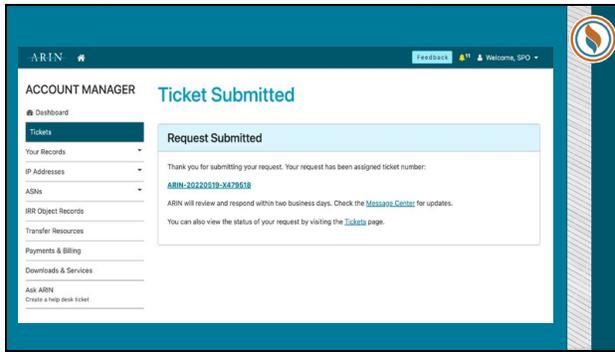
This capture of the Command Line interface shows formatted content necessary for a manually-signed ROA to be completed.



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.