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:

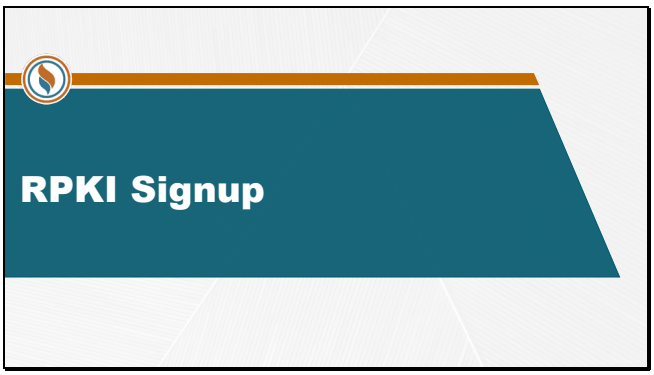
The organization has more control and independence

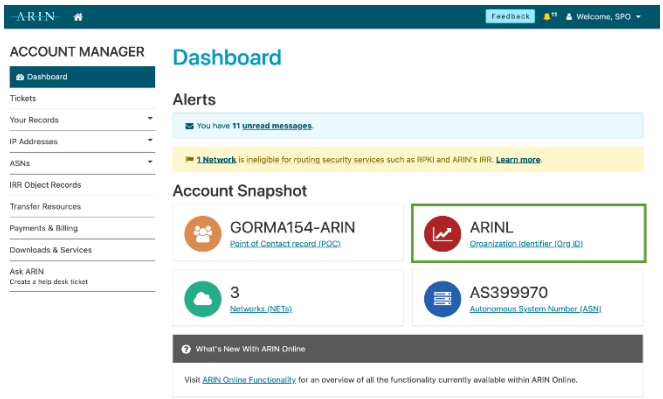
- Runs their own Certificate Authority (CA) to manage object signing
- Separation of the publication of cryptographic functions

Delegated with Remote Publication Service (RPS):

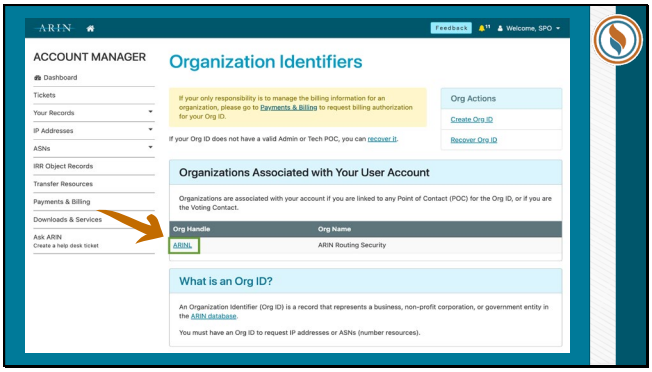
The organization runs the Certificate Authority

- Delegates the repository and publication services to ARIN

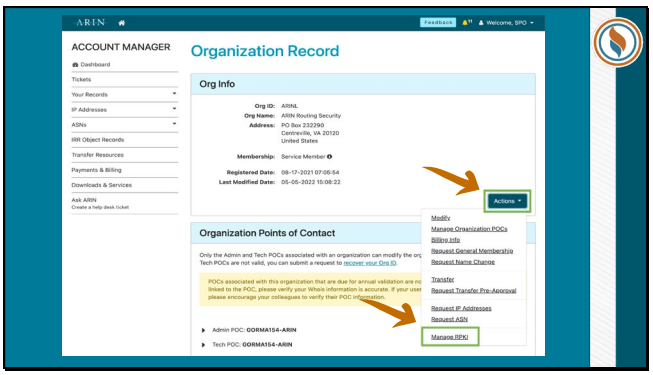




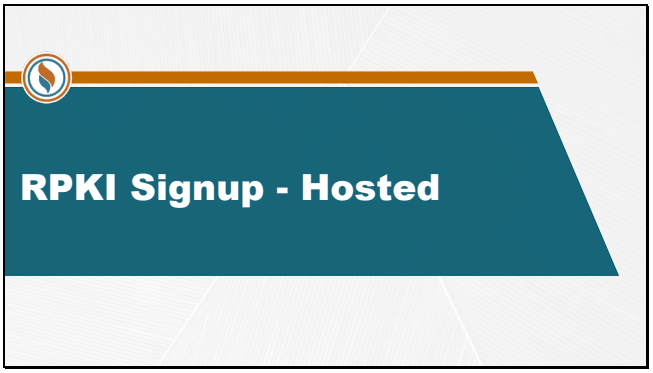
At the initial signup to use RPKI through ARIN, you will need to choose between Hosted or Delegated RPKI. On the ARIN Online Account Manager Dashboard, select the Organization Identifier (ORG ID).

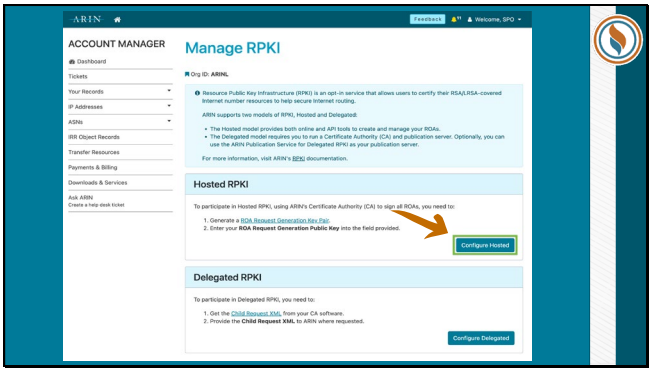


On the Organization Identifiers page, select the Org Handle for which you want to manage RPKI.

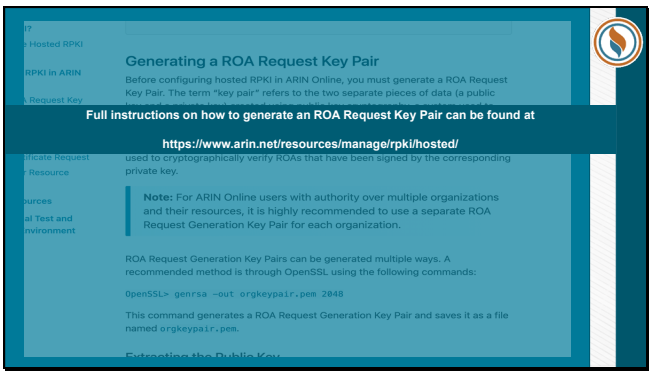


Next, on the Organization Record page, select the Actions button. Then, in the drop down menu, select Manage RPKI.



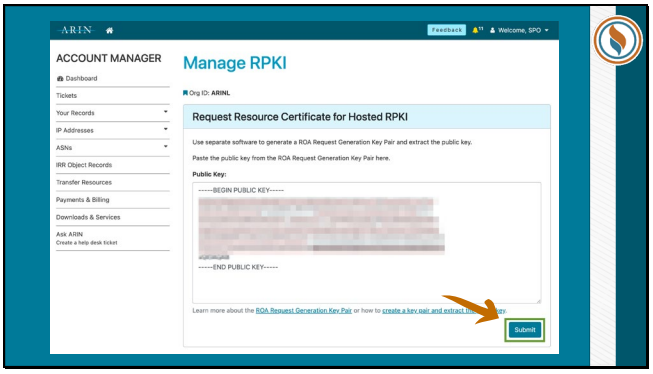


To begin setting up Hosted RPKI, select Configure Hosted on the Manage RPKI page.

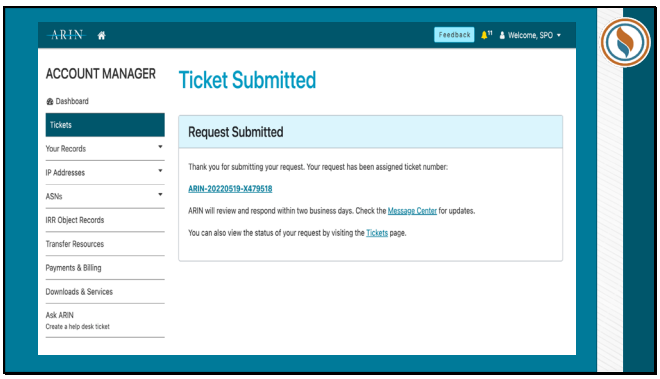


The full instructions on how to generate an ROA Request Key Pair can be found at https://www.arin.net/resources/manage/rpki/hosted/, as well as slides 38-41 of this presentation.

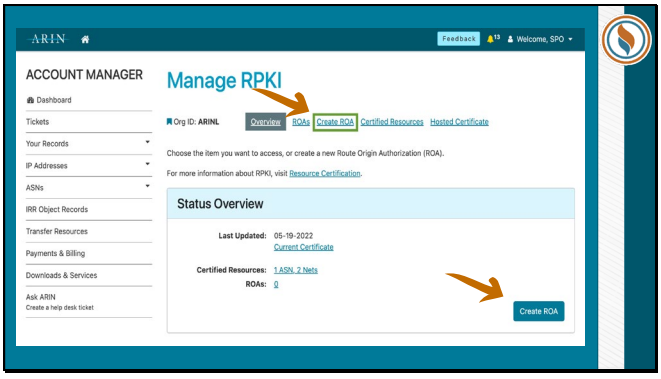
As a hosted RPKI participant, you generate and use ROA Request Generation Key Pairs to secure your ROAs and resource certificate data and cryptographically verify your identity. Your public key is provided to ARIN and is used to cryptographically verify ROAs that have been signed by the corresponding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



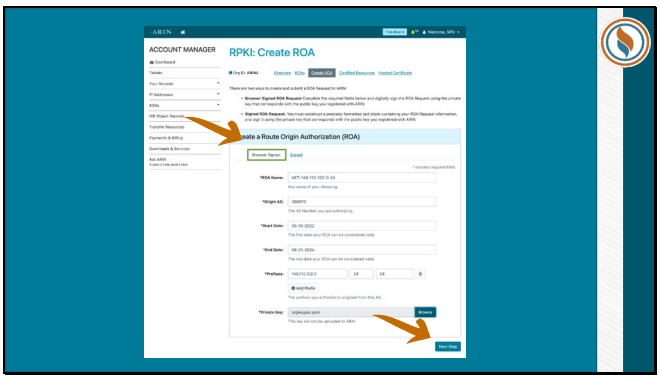
Once the RIR Request Key Pair has been generated, copy and paste the public key into the field provided and select submit.



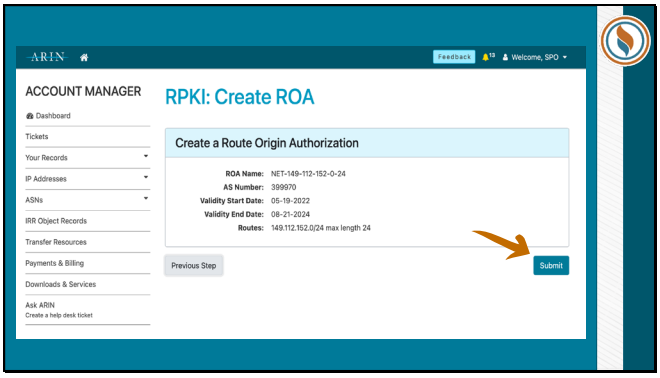
This will complete the request, which will be assigned a ticket number. This ticket will be reviewed by ARIN, and its status can be tracked through the Tickets page.



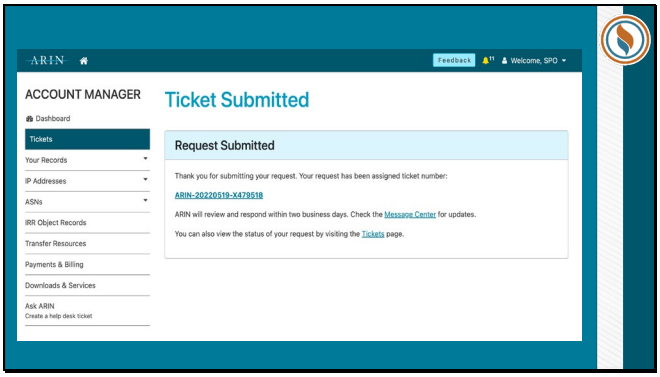
Once your ticket has been resolved, to create a new Route Origin Authorization (ROA), select Create ROA on the Manage RPKI page.



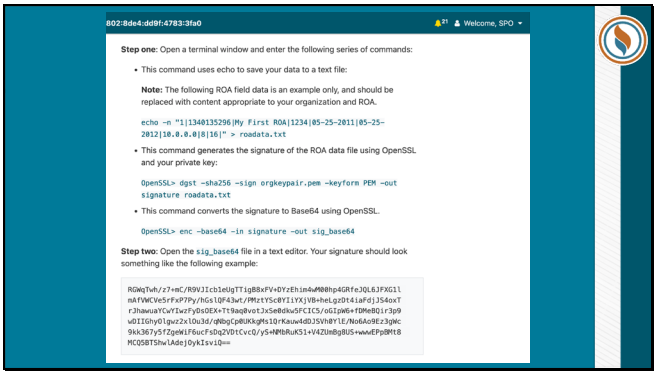
On the RPKI: Create ROA page, select Browser Signed, complete the form provided, and select Next Step.



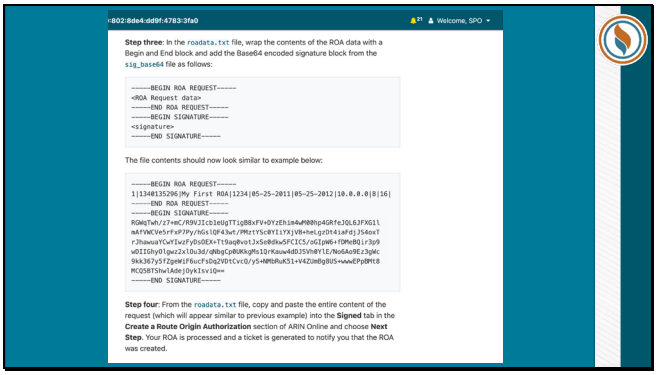
You will be provided with a summary of the submitted information to review. Select Previous Step to make any corrections if needed; otherwise select Submit.



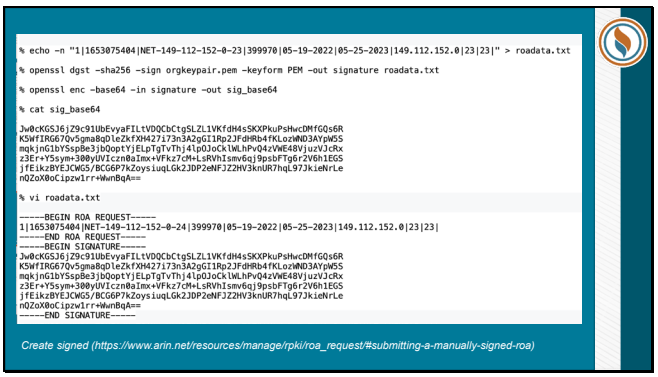
This will complete the request, which will be assigned a ticket number. This ticket is part of an automated process, and its status can be tracked through the Tickets page.



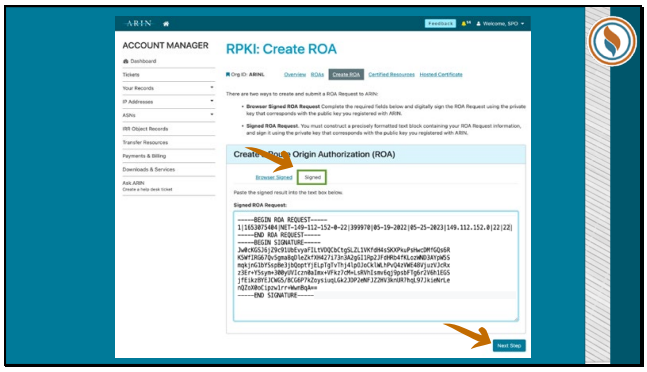
These slides provide detailed instructions to complete a manually-signed ROA request.



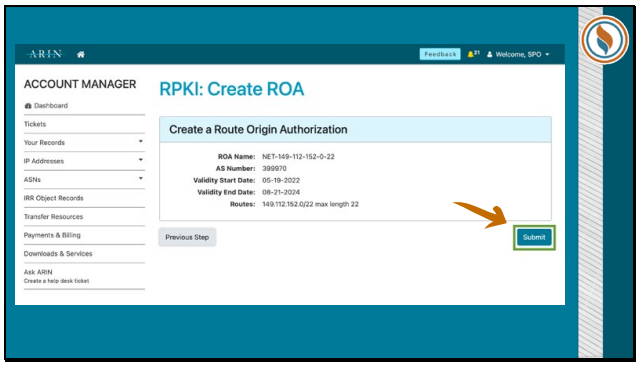
These slides provide detailed instructions to complete a manually-signed ROA request.



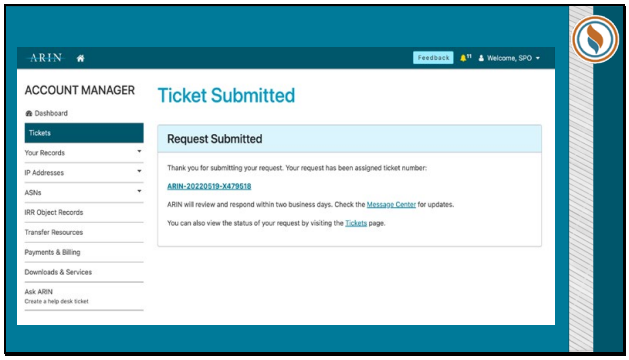
This capture of the Command Line interface shows formatted content necessary for a manually-signed ROA to be completed.



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.