
# RPKI Tutorial

Andy Newton
Chief Engineer, ARIN

# Agenda

- Resource Public Key Infrastructure(RPKI)
- Route Origin Authorizations (ROAs)
- Certificate Authorities (CAs)
- ARIN Online Overview
- Operational Test and Evaluation Environment (OT&E) Walk-through
  - **Account Creation**
  - **Key Pair Generation**
  - **ROA requests**

# What is RPKI?

- A robust security framework for verifying the association between resource holders and their Internet resources
- "Resource Holders"
  - **Regional Internet Registries (RIR)**
  - **Local Internet Registries (LIRs)**
  - **Internet Service Providers (ISPs)**
  - **End-user organizations (no acronym)**

# What is RPKI?

- A robust security framework for verifying the association between resource holders and their Internet resources
- "Resource Holders"
  - **Regional Internet Registries (RIR)**
  - **Local Internet Registries (LIRs)**
  - **Internet Service Providers (ISPs)**
  - **End-user organizations (no acronym)**

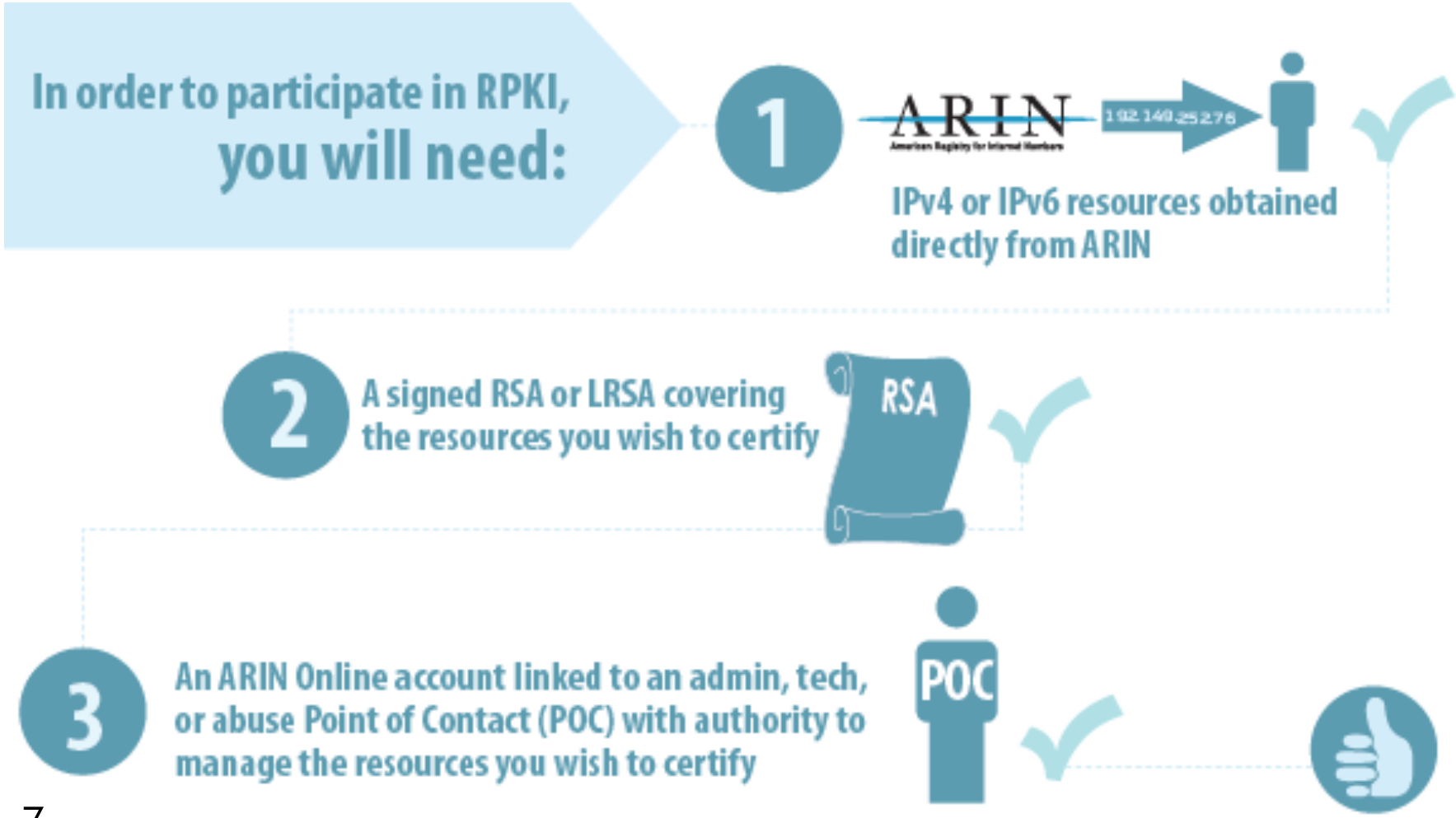
# Key Elements of RPKI

- Resource Certificates
  - verifiable digital statement that an Internet number resource has been registered by that RIR
- Route Origin Authorizations (ROAs)
  - cryptographically signed object that states which Autonomous System (AS) is authorized to originate a particular prefix or set of prefixes

# Certificate Authorities (CAs)

- A CA is any entity that issues digital certificates
- Hosted RPKI
  - **ARIN is the CA**
- Delegated RPKI
  - **Direct resource holders act as a CA for their customers**

# Hosted RPKI Requirements



# Delegated RPKI Requirements

- Before signing up, you must have:
  - **IPv4 or IPv6 resources obtained directly from ARIN**
  - **A signed RSA or LRSA covering the resources you wish to certify**
  - **An ARIN Online account linked to an admin or tech Point of Contact (POC) with authority to manage the resources you wish to certify**
  - **An Up/Down identity**

# Delegated RPKI Requirements


- Once you become a participant, you must:
  - **Exchange your public key associated with your Delegated RPKI private key with ARIN via ARIN Online**
  - **Create an infrastructure in which to host a CA, both hardware- and software-wise**
  - **Perform all work required for maintaining a CA and publishing a Certificate Practice Statement**
  - **Create an RPKI repository in which to host:**
    - **Resource certificates**
    - **ROAs**
    - **Manifest**
    - **Certificate Revocation List**

# A Note about Early Registration Transfer (ERX)

- ERX resources: Resources allocated before the Regional Internet Registries (RIRs) came about
- Many of these are still managed by ARIN
- Some ERX resources may not be eligible for RPKI until ARIN coordinates further with other RIRs

# ARIN's Certificate Authority

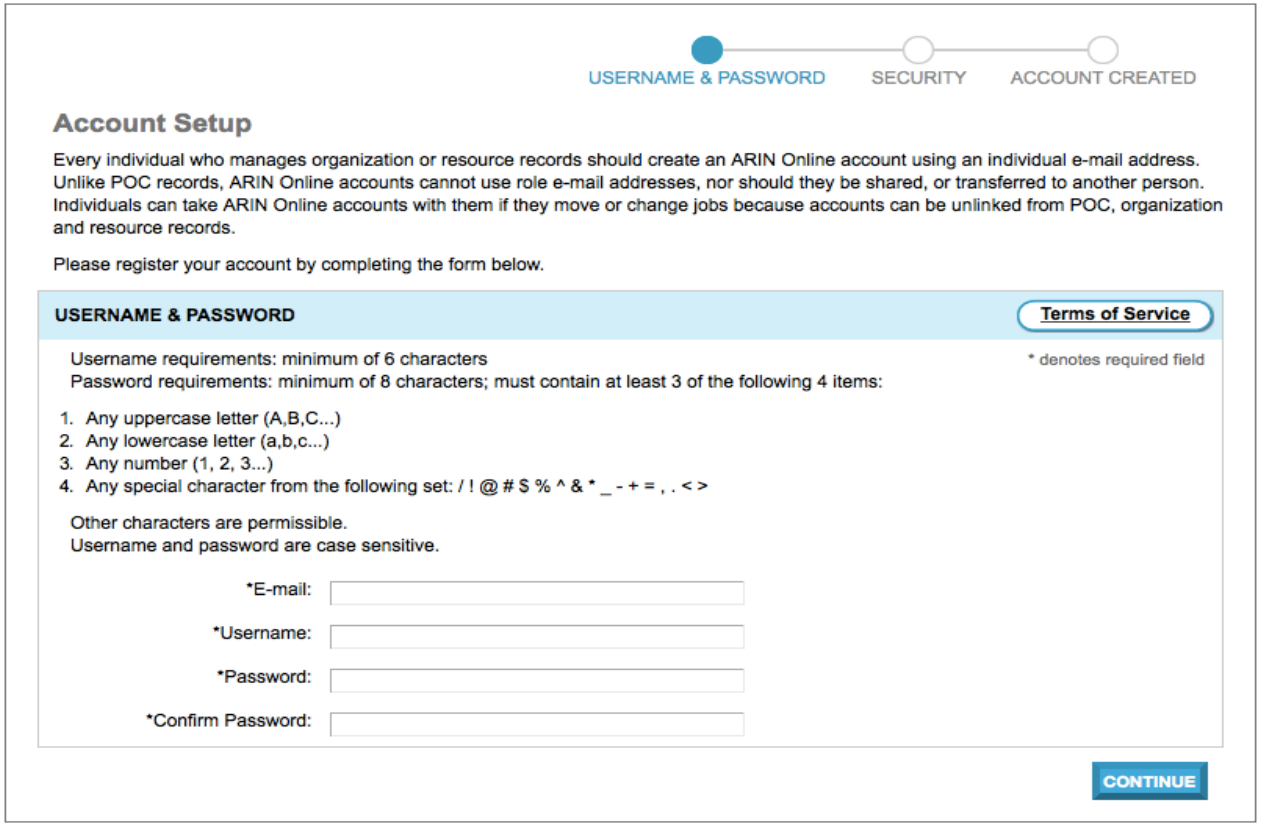
- ARIN's CA Contains:
  - **Resource certificates**
  - **ROAs**
  - **Manifest**
  - **Certificate Revocation List**

# ARIN Online Account Creation

1. Go to www.arin.net and select “new user?”

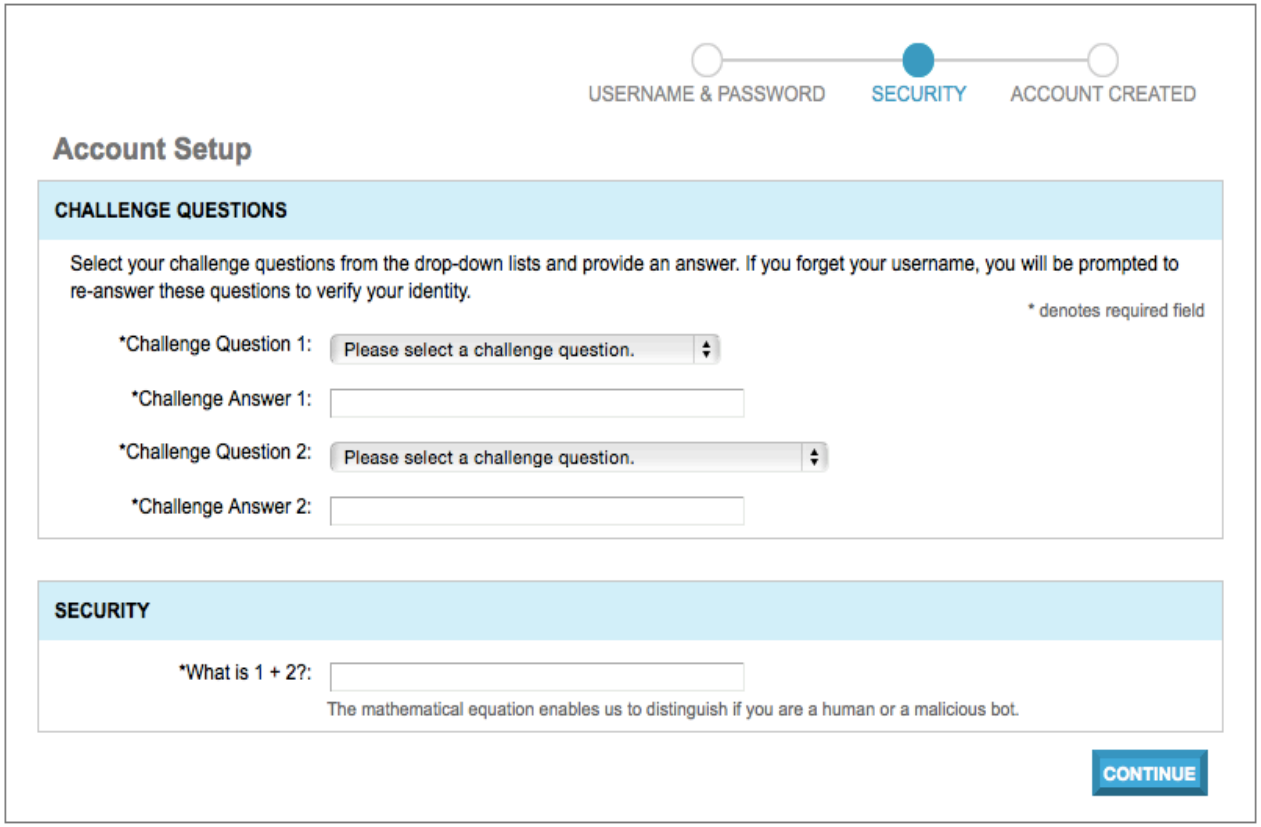
# ARIN Online Account Creation

## 2. Complete this form



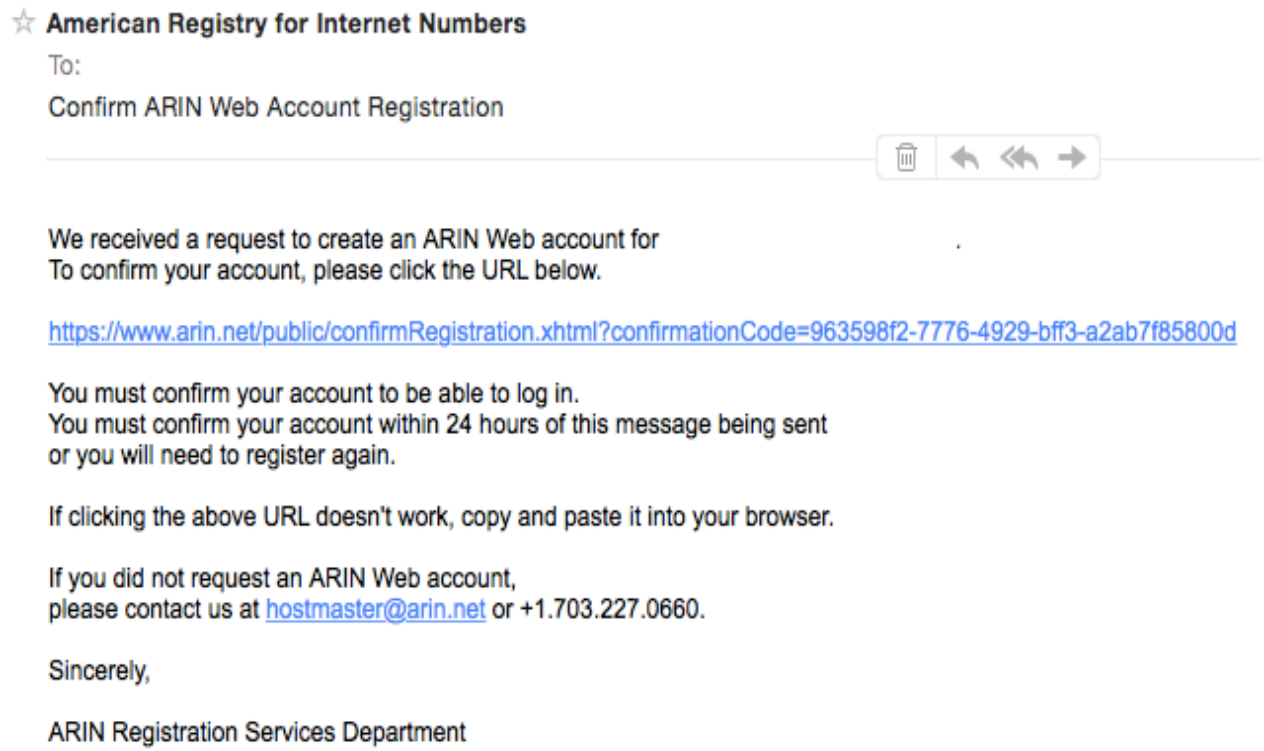
# ARIN Online Account Creation

## 3. Challenge Question/Math Problem



# ARIN Online Account Creation

4. Check your email!



**American Registry for Internet Numbers**

To:

Confirm ARIN Web Account Registration

We received a request to create an ARIN Web account for .
To confirm your account, please click the URL below.

https://www.arin.net/public/confirmRegistration.xhtml?confirmationCode=963598f2-7776-4929-bff3-a2ab7f85800d

You must confirm your account to be able to log in.
You must confirm your account within 24 hours of this message being sent
or you will need to register again.

If clicking the above URL doesn't work, copy and paste it into your browser.

If you did not request an ARIN Web account,
please contact us at hostmaster@arin.net or +1.703.227.0660.

Sincerely,

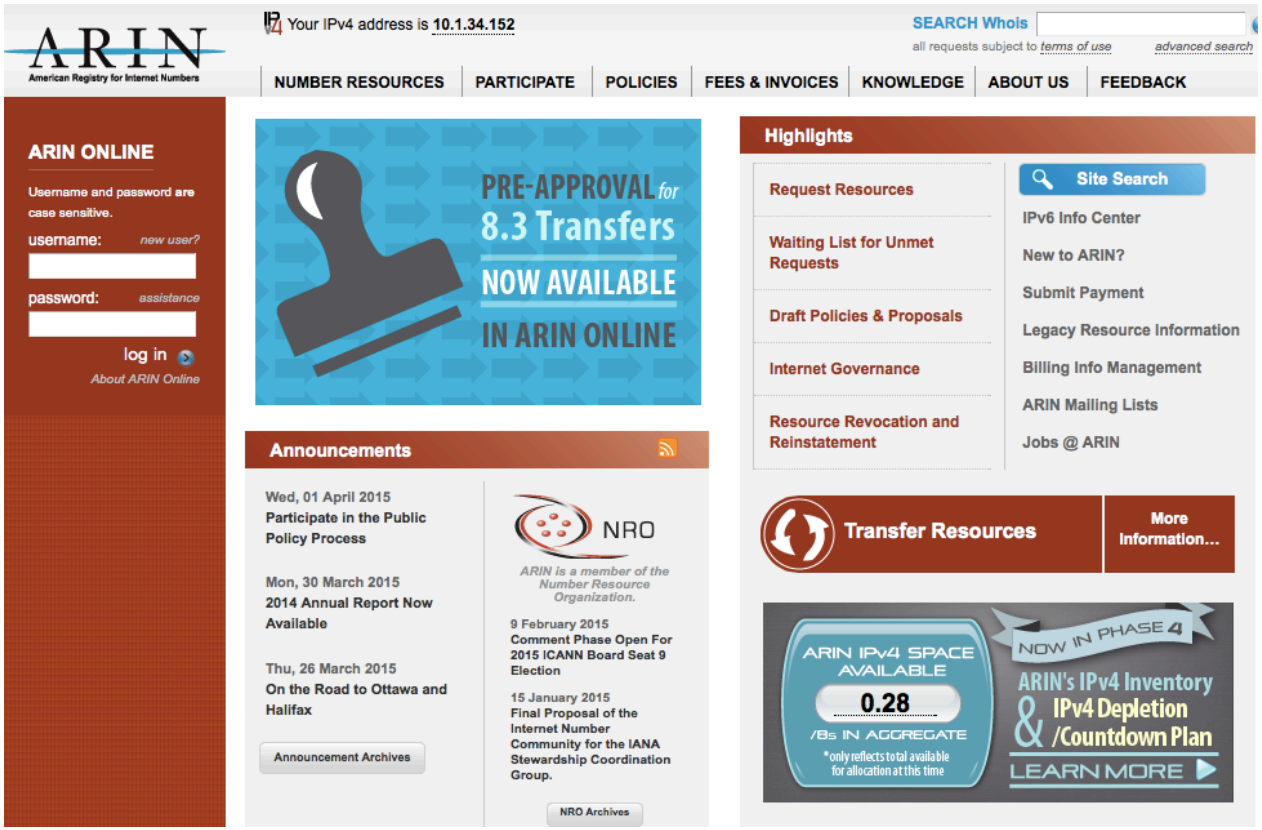
ARIN Registration Services Department

# ARIN Online Account Creation

4. Check your email!

# Participating in RPKI

## 1. Log into ARIN Online

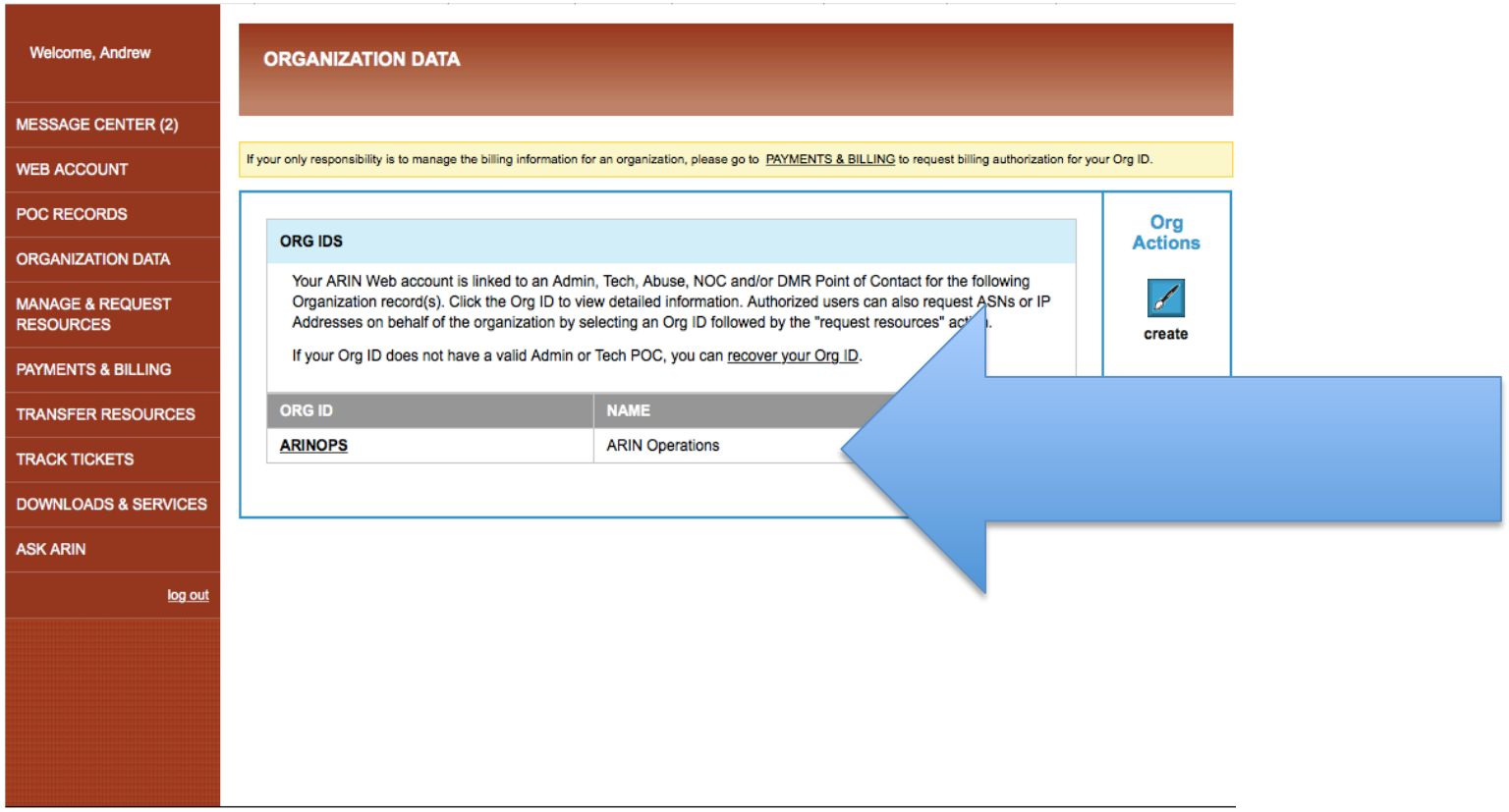


# Participating in RPKI

## 2. Select ORGANIZATION DATA

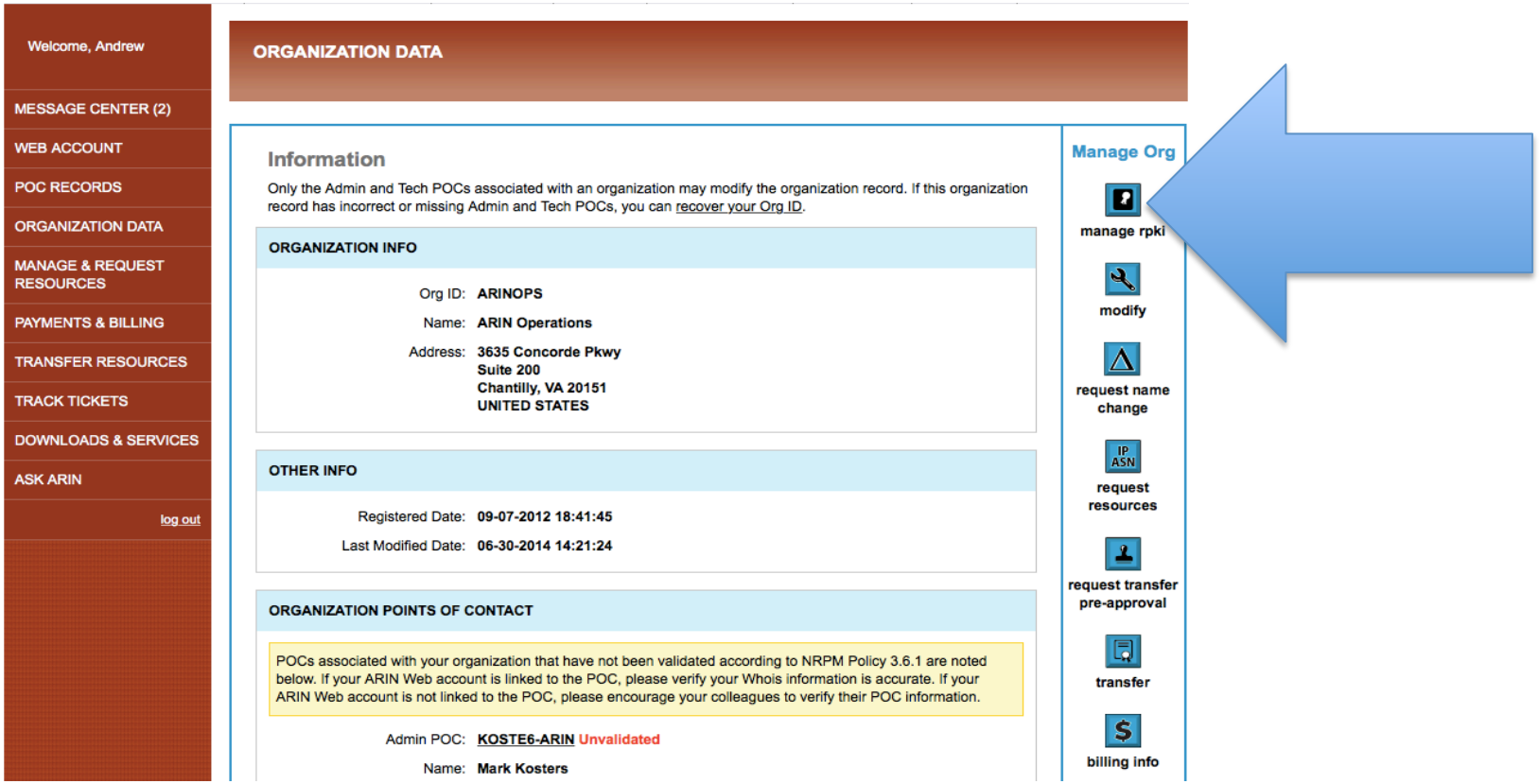
# Participating in RPKI

## 3. Select an Organization Identifier (Org ID)



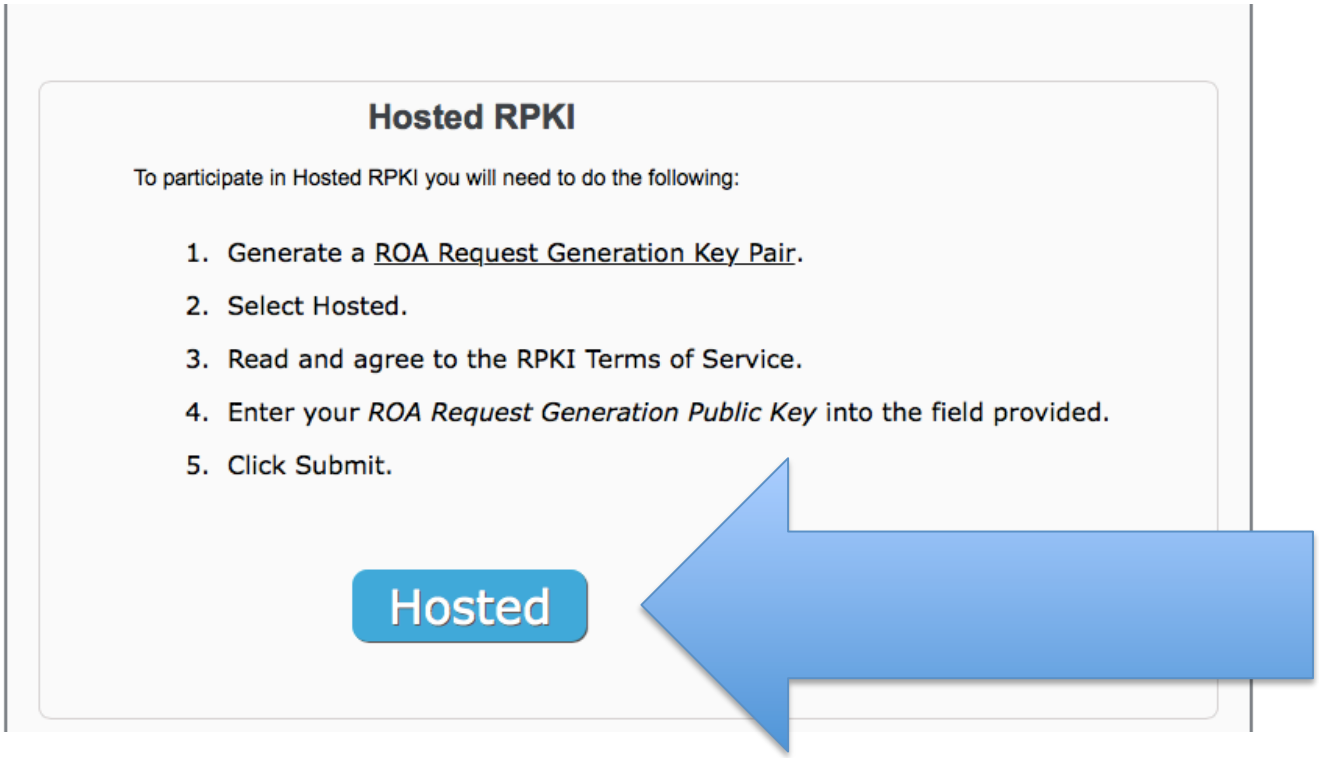
# Participating in RPKI

## 4. Select Manage RPKI



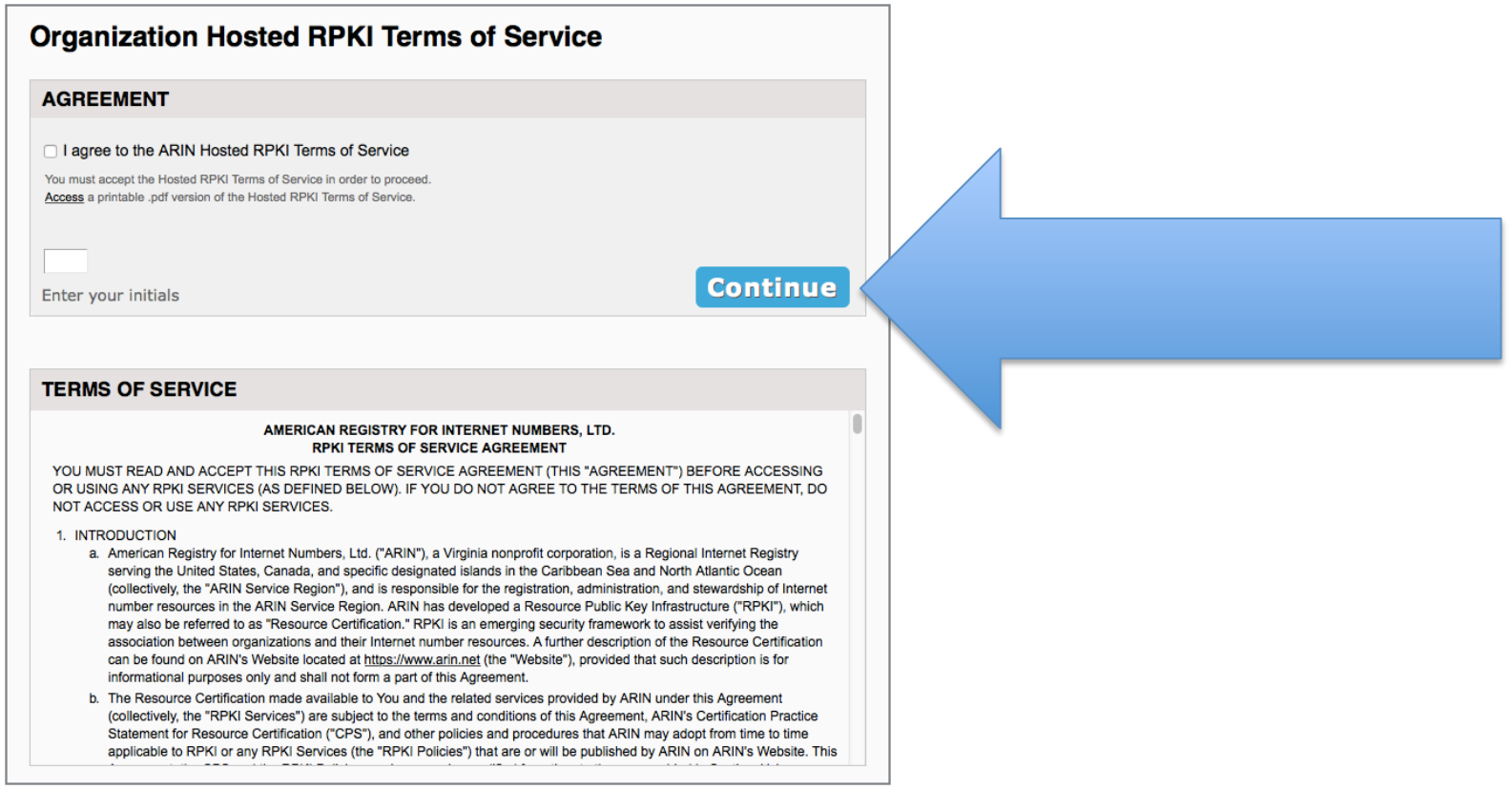
# Participating in RPKI

5. Select “Hosted”



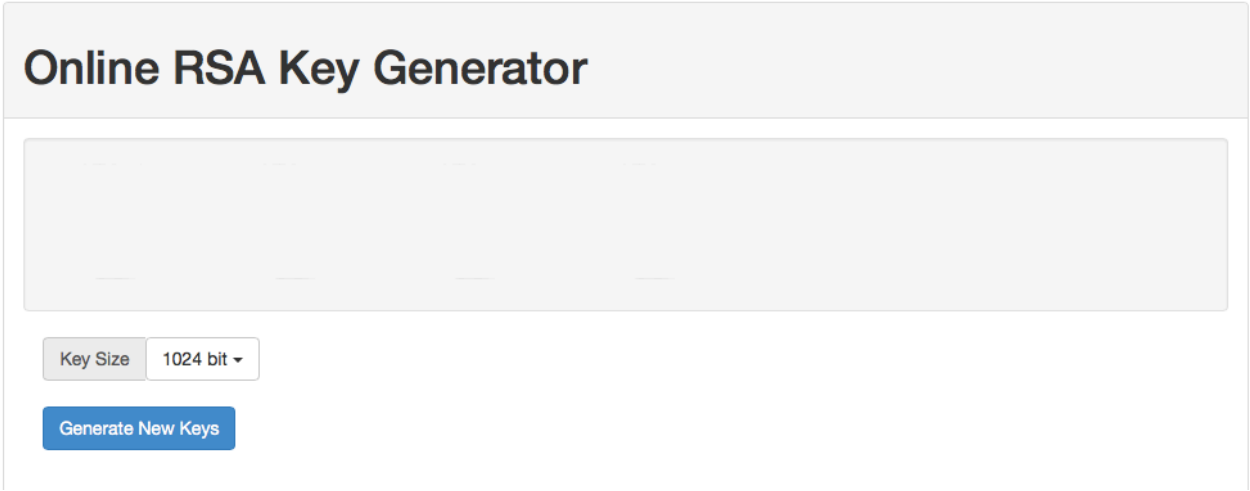
# Participating in RPKI

## 6. Agree to the RPKI Terms of Use



# Participating in RPKI

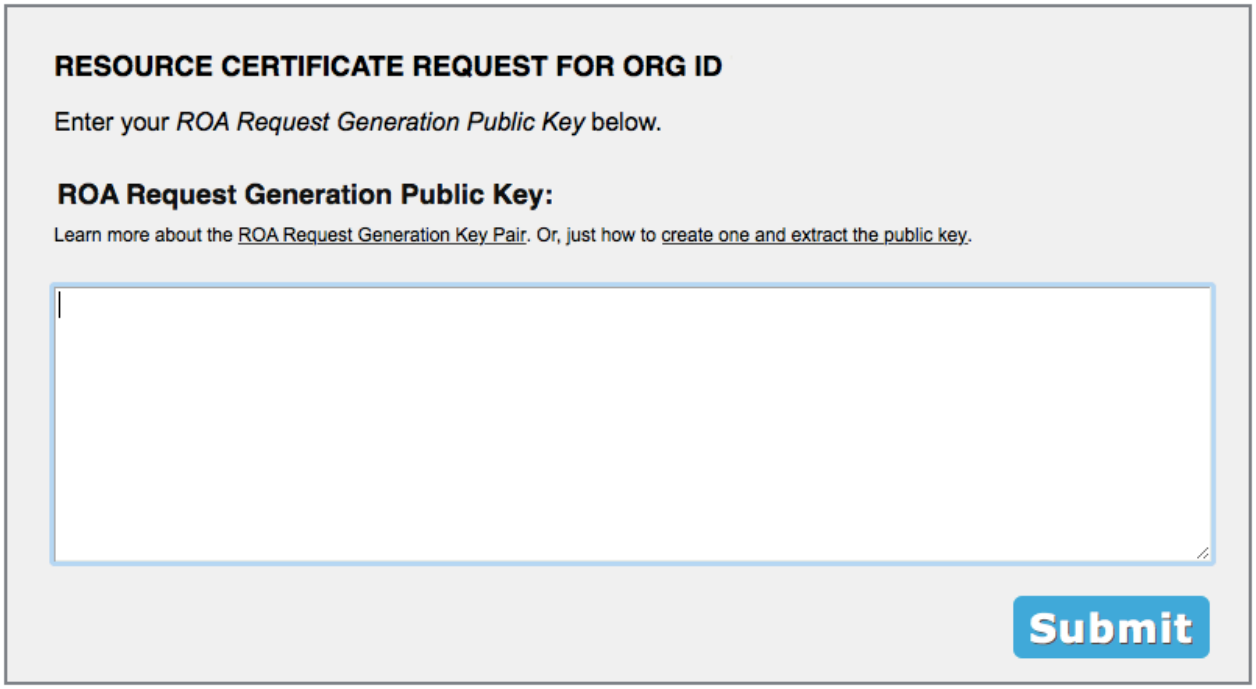
7. Generate a 2048-bit key pair




- **Visit http://travistidwell.com/jsencrypt/demo/**
- **Save each key as a separate .pem file (public.pem and private.pem)**

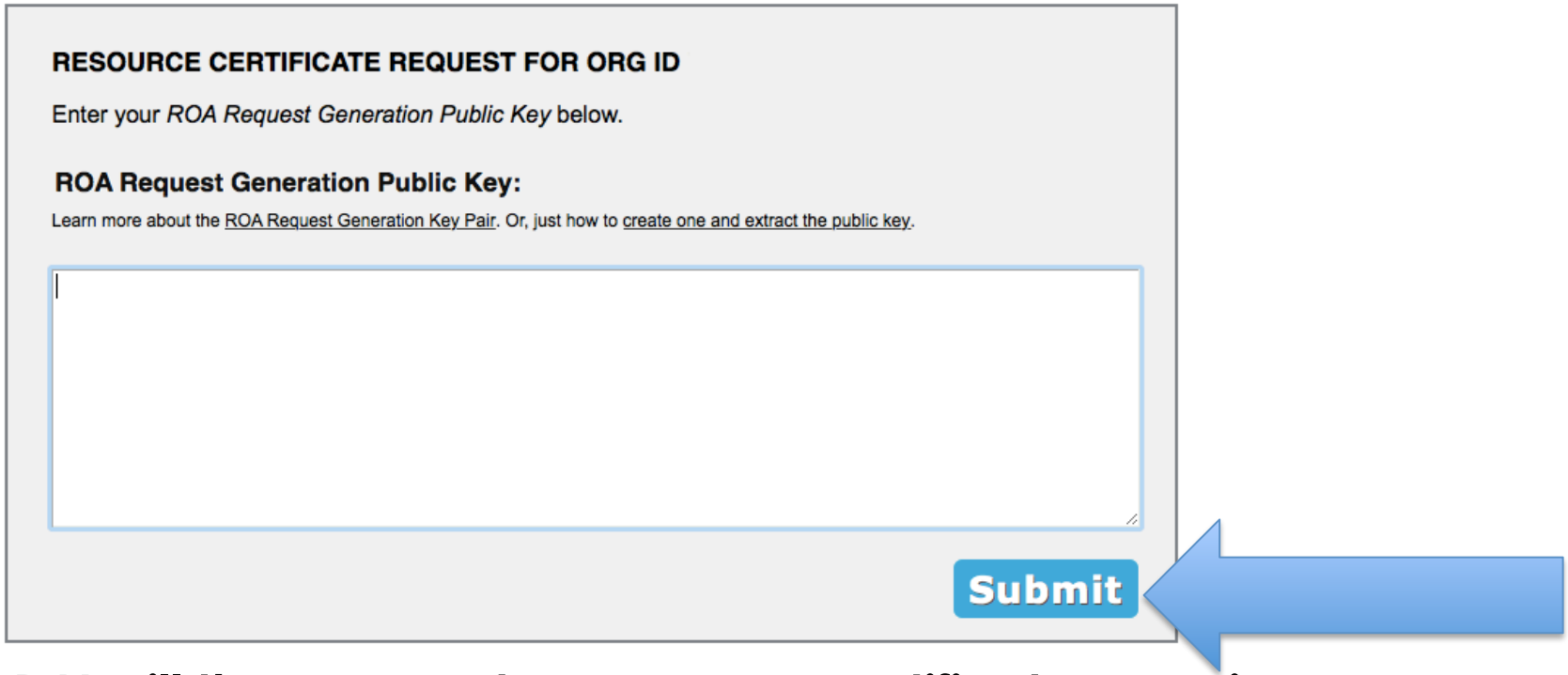
# Participating in RPKI

8. Provide your public key



# Participating in RPKI

- Click Submit




- **ARIN will then generate a resource certificate covering your Internet number resources**

# Participating in RPKI

- Within "Manage RPKI" you can:
  - **View which resources your certificate covers**
  - **View and manage your resource certificate**
  - **Request and manage ROAs**

# ROA Requests

1|1340135296|My First ROA|1234|05-25-2011|05-25-2012|10.0.0.0|8|16|

Version Number: This must be set to 1.

# ROA Requests

1|1340135296|My First ROA|1234|05-25-2011|05-25-2012|10.0.0.0|8|16|

**Timestamp:** This must be specified in seconds since 1 January 1970 (AKA seconds since the epoch).

# ROA Requests

1|1340135296|My First ROA|1234|05-25-2011|05-25-2012|10.0.0.0|8|16|

**ROA Name:** This can be any name of your choosing, it is for your own identification purposes only. A ROA name can only contain letters, numbers, spaces and dash "-" characters. There may not be more than 256 characters to a name.

# ROA Requests

1|1340135296|My First ROA|1234|05-25-2011|05-25-2012|10.0.0.0|8|16|

roa request

**Origin Autonomous System (AS):** The number of the AS that will be authorized to announce the IP prefix(es) you specify. You are not restricted to putting in your own AS, however you can only put in one AS per ROA. If you intend to originate your prefixes from more than one AS, you will need to create a ROA for each one.

# ROA Requests

1|1340135296|My First ROA|1234|05-25-2011|05-25-2012|10.0.0.0|8|16|

**Validity Start Date:** The first date for which this ROA should be considered valid. This date must be within the validity date range of your CA certificate, and expressed in mm-dd-yyyy format.

# ROA Requests

1|1340135296|My First ROA|1234|05-25-2011|05-25-2012|10.0.0.0|8|16|

**Validity End Date:** The last date for which this ROA should be considered valid. This date must be within the validity date range of your CA certificate, and expressed in mm-dd-yyyy format.

# ROA Requests

1|1340135296|My First ROA|1234|05-25-2011|05-25-2012|10.0.0.0|8|16|

Prefix and Prefix Length: The prefix is the range of IP addresses authorized to be announced by the AS Number you specify. This prefix must be allocated to your organization and certified by your CA certificate. The prefix length specifies the size of that IP address range.

You may include more than one prefix at a time within a ROA request. If you wish to specify more than one prefix, you must provide a Prefix, Prefix Length, and Max Length field (may be blank) for each prefix. Show the ROA when multiple prefixes are allowed Clear

Max Length: The Max Length field is the smallest exact prefix length announcement you will allow for this route and is optional; if it is not provided then only the exact prefix entered will be specified in the ROA. Show ROA request with blank Max Length field Clear

# ROA Requests

1|1340135296|My First ROA|1234|05-25-2011|05-25-2012|10.0.0.0|8|16|

**Trailing Vertical Bar:** This character must follow each section of the ROA request.

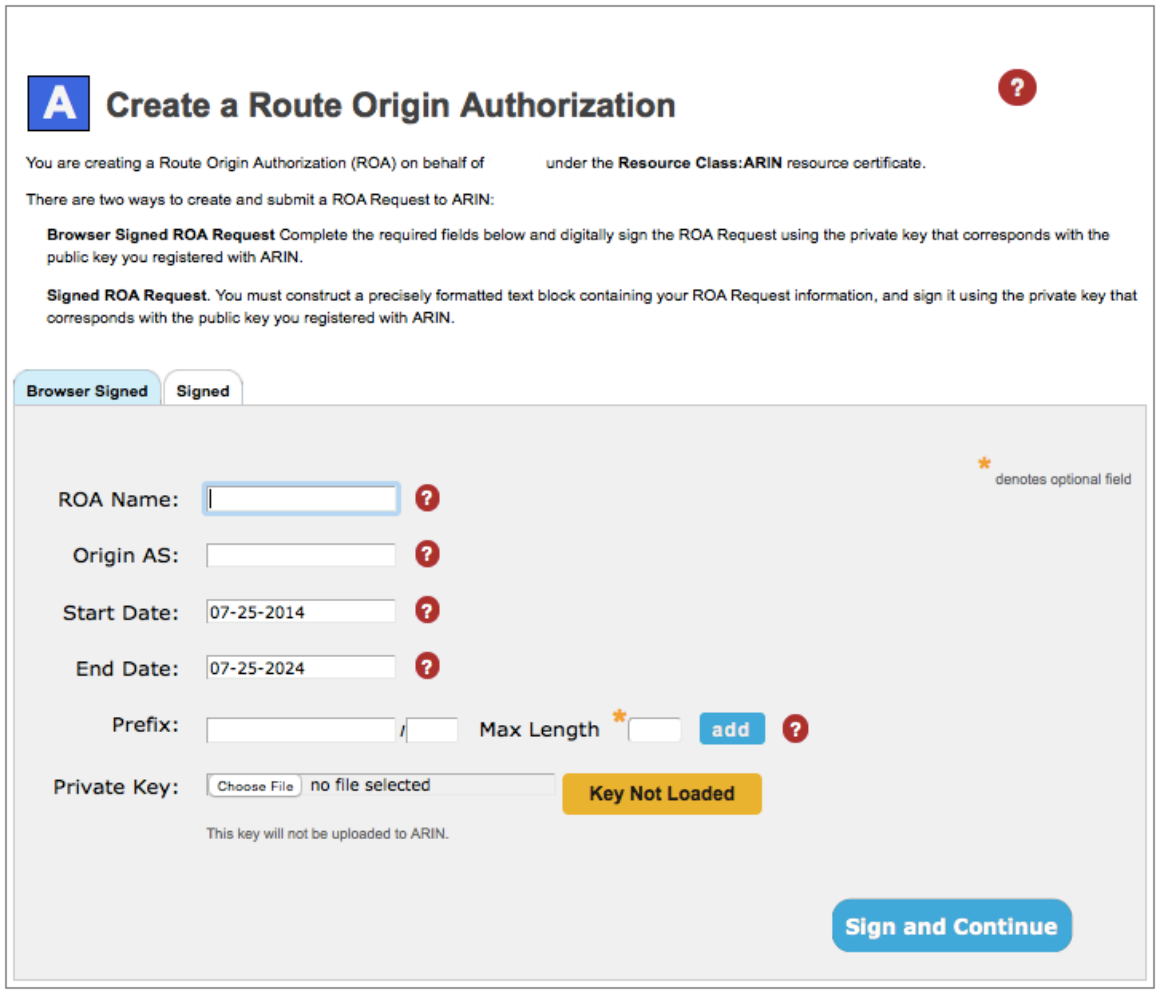
# ROA Request Generation and Signing

Within ARIN Online (browser signed)

1. **Fill in the form provided for you within ARIN Online detailing each part of the ROA Request.**
2. **Attach the private.pem file you created earlier**
3. **Using JavaScript, the browser signs the data you provided.**

***Note: Your private key is never uploaded to ARIN and the signing code is run only on your computer.***

# ROA Request Generation and Signing



# RPKI Walkthrough

- To get started, visit:
  - **https://www.ote.arin.net/public/**

- For your test Public/Private key, visit:
  - **https://www.arin.net/resources/ote.html**

# Congratulations!

"You have taken your first step into a larger world."

– Captain Kirk


# Questions?