

# **RPKI Workshop**

**Starting ~8:45**





# Using ARIN's Hosted RPKI Services

**CHI NOG 13**  
**27 May 2026**

# Brad Gorman

Director of Customer Technical  
Services



# Our Exploration Plan

- Routing Security Fundamentals
- ARIN's RPKI Services
- Hosted RPKI Hands on Workshop

A blurred background image showing a group of people in a meeting or conference. Several individuals have their hands raised, indicating an interactive session or a Q&A period. The focus is on the hands and arms, with the faces and bodies of the participants being out of focus.

**Ask questions!  
Get involved!**

# Border Gateway Protocol (BGP) and Routing Security

# Border Gateway Protocol (BGP)

The standardized routing protocol used to exchange information between different networks on the Internet

- Autonomous Systems (AS) are comprised of routers that share a single routing policy
- It allows for bidirectional connection between Autonomous Systems to exchange routing information
- That information is used to build the global routing table
- Data packets are then routed through the Internet based on that information

# BGP Enabled The Internet We Know Today

---

BGP provides a framework to establish peering sessions with other networks

Originally, the Internet was a network of trusted peers: government, universities, and researchers

The transition to a commercial platform means the Internet scaled beyond a trust-based model for routing security

# Routing is Easy, Security is Not

## Routing protocols provide transport

They allow for data to be moved from source to destination

With BGP, routing “just happens”

They do not ensure shared routing information is legitimate

## Security adds complexity

- Data must be secured with encryption
- Routing segments should be controlled with Access Control Lists (ACL)
- Firewalls must be deployed to filter out malicious traffic
- Internet traffic must be secured with policy

# Why is Routing Security Important?


---

In our current digital landscape where data traverses thousands of networks, strong routing security helps maintain trust and stability, preventing disruptions and attacks that could compromise sensitive information or disrupt services.

# BGP Origination Errors

- In February 2008, the government of Pakistan ordered access to YouTube to be blocked in the country due to a video it deemed anti-Islamic.
- Pakistan Telecommunications Company Limited (PTCL) announced more-specific routes of YouTube's BGP announcements to intentionally hijack traffic to the video streaming service.
- PTCL's goal was to black hole the traffic, preventing Pakistanis from being able to access YouTube.
- PTCL leaked these more-specific routes to international transit providers, thereby blocking YouTube for a large portion of the global Internet.

# Attacks on Cryptocurrency Services



- In 2018, attackers employed a BGP hijack that redirected traffic to Amazon's authoritative DNS service.
- Having hijacked the DNS traffic, the adversary answered DNS queries for the web-based cryptocurrency wallet "myetherwallet.com"
- Users that received this erroneous DNS response were directed to an imposter "myetherwallet.com" website.
- Some users had their login credentials stolen along with the contents of their cryptocurrency wallets.

# Traffic Manipulation with BGP

- Following the military coup in Myanmar in 2021 and the Russian crackdown of social media after its invasion of Ukraine in 2022, telecoms in each of these countries attempted to block access to Twitter/X.
- In each case, the intent of these intentional BGP hijacks was to blackhole traffic to the Twitter/X route.
- However, the hijacked BGP Twitter/X route was unintentionally propagated onto the Internet, affecting Twitter/X users outside of the originating countries.

# BGP is inherently insecure

## ... but all is not lost

- No confidentiality
- No authorization of advertisements
- No verification of integrity of received routing information
- Beyond any practical repair

# What is Routing Security?

---

Routing security refers to the set of practices and technologies used to protect the flow of data as it moves across the Internet from one network to another.

Its purpose is to ensure that data remains on its intended path and reaches the correct destination without interference, compromise, or misdirection.

# Why is Routing Security Important?

---

- In a world where data is the lifeblood of businesses, prioritizing routing security is no longer optional.
- Misconfigured, or malicious route announcements can lead to traffic interception, outages, and even financial losses.
- Essential for organizations that operate networks and rely on uninterrupted data flows.
- It's a global problem to solve.

# How do we secure routing?

- Using a Public Key Infrastructure
- Adding encryption
- Ensuring advertisements are authenticated
- Verifying the integrity of the routing information received

# It's a Global Problem to Solve

---

Network operators have been working to ensure the Internet works seamlessly to provide the best possible experience for their customers for many years. These operators realized the need for a globally accessible location to document their routing intentions.

Today there are two routing security tools in use that are integral in maintaining the security and reliability of the Internet.

# Commonly Used Routing Security Tools

---

- Internet Routing Registry (IRR)
- Resource Public Key Infrastructure (RPKI)

# Internet Routing Registry (IRR)

---

- The Internet Routing Registry is a broad ecosystem of databases run by the RIRs ISPs or other entities.
- Data is submitted and maintained by Internet Number Resource holders, containing information about Autonomous System Numbers (ASNs) and routing IP prefixes.
- IRR data can be used by ISPs to develop routing plans and create Access Control Lists to permit or deny traffic in their networks based on route registry information.

# Internet Routing Registry (IRR)

---

- User defined data in multiple separate 3<sup>rd</sup> party databases
- Contains a mix of authenticated and non-authenticated data
- No cryptographic chain of authority across the entire ecosystem
- Long lived – Widely deployed – Can contain old inaccurate and incomplete data

# Resource Public Key Infrastructure (RPKI)

- RPKI is a specialized security framework designed to provide a more robust, cryptographically verifiable method to address **long-standing vulnerabilities in BGP**.
- It uses cryptographically verifiable statements to ensure that Internet number resources are the authorized holders of those resources.
- RPKI gives resource holders the ability to authoritatively **state which ASNs are authorized to originate their IP prefixes**.

## Why is RPKI Important for Routing Security?

- Strong cryptographic control and chain of authenticity
- RIRs are authoritative source - confirm data entered by resource holders
- Accepted as the best available routing security tool today
- Ongoing development – Planned for long term support and use

# ROAs and Route Origin Validation

# Route Origin Authorization (ROA)

- A ROA is a statement: *"These are my IP addresses, and I authorize this AS number to announce them to the world"*
- RIRs are the authority for all number resources in their registry, and certify ROAs are created by authorized resource holders.
- They are signed objects that are critical to perform RPKI Route Origin Validation (ROV)

# Why are ROAs Important?

- ROAs that cover your IP resources are necessary to calculate the RPKI validity state of Internet route announcements.
- A growing number of Internet service providers require you to create ROAs before they start announcing your routes.
- As more resources are covered in ROAs, the benefits of RPKI deployments will grow.

# Route Origin Validation (ROV)

- The first RPKI routing security feature available, it can be implemented in ANY operator's network
- Intended to mitigate the impact of accidental misconfigurations or malicious route leaks
- Requires a conscious decision by the operator to implement — it's not automatic
- Not mandatory, but you should consider implementing if you provide connectivity services to your customers

## Not My Origin ASN

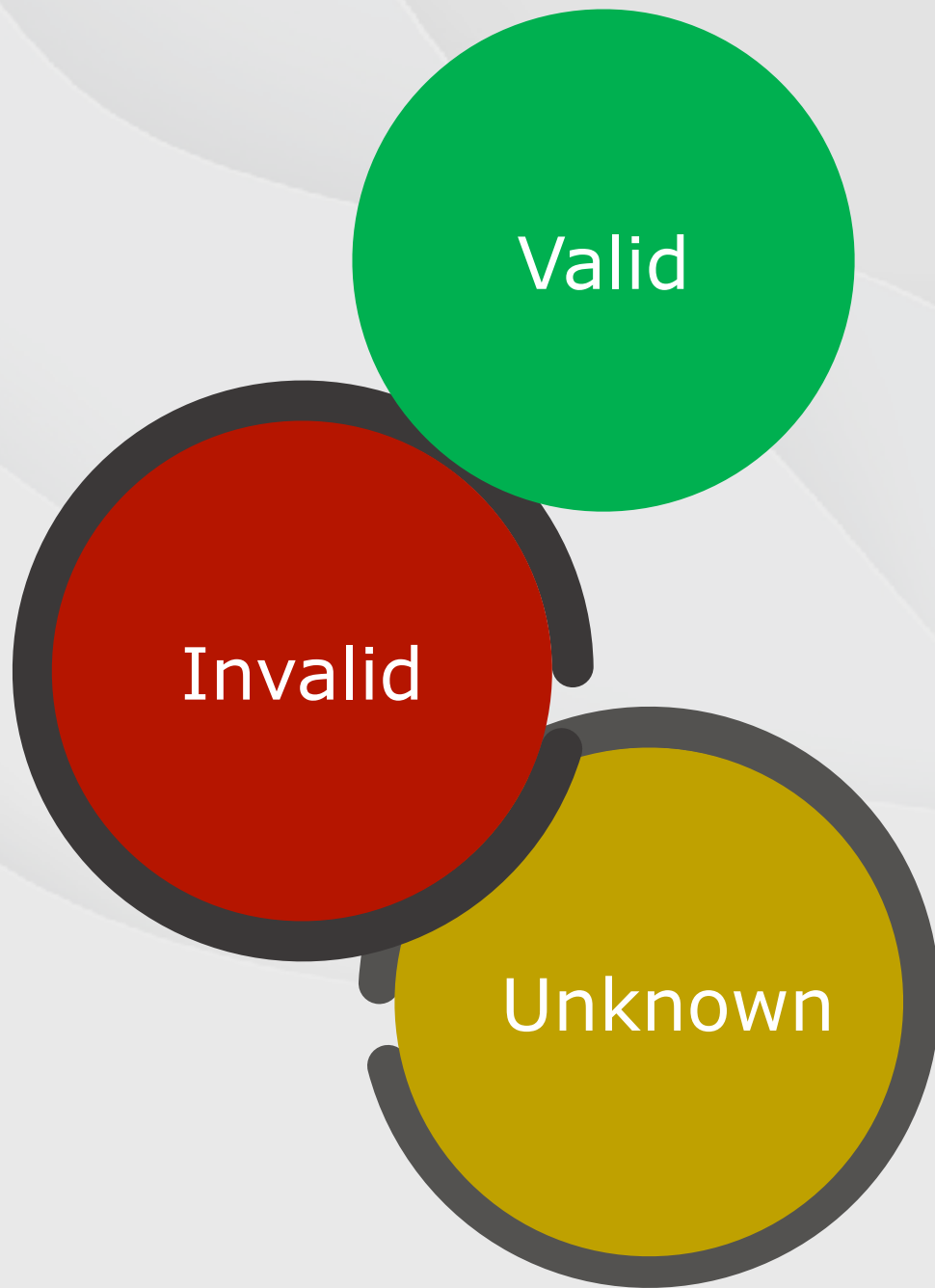
- The Origin AS in a ROA does not need to be allocated to you, only the IP prefixes.
- Bring Your Own IP (BYOIP) service providers source your IP prefix from their network. The Origin AS will be theirs — not yours — and the ROA must reflect that.
- A DDoS service provider will announce your IP prefix to provide protection. A ROA identifying that Origin AS must be in place for those services to work.

# The AS0 ROA

You are asserting: *"No ASN is authorized to announce this prefix or prefixes to the Internet."*

If any announcements with your IP addresses are seen in the global BGP table, they will be marked RPKI invalid, and operators performing RPKI-ROV will drop them.

**BE CAREFUL!** If you decide to create AS0 ROAs, any existing route announcements may be impacted, and reachability to your IP prefixes may be interrupted.



# Three Validity States

- **VALID:** A ROA containing an origin/prefix pair that matches or covers a route announcement is detected
- **INVALID:** An Internet route announcement is seen that does not match the content of an existing ROA
- **UNKNOWN:** No ROA exists that references IP prefixes present in the global BGP table

# The Fundamental Steps to RPKI-ROV



## Authorization

Authenticated **resource holders** create **ROAs** that reside in an RPKI repository



## Validation

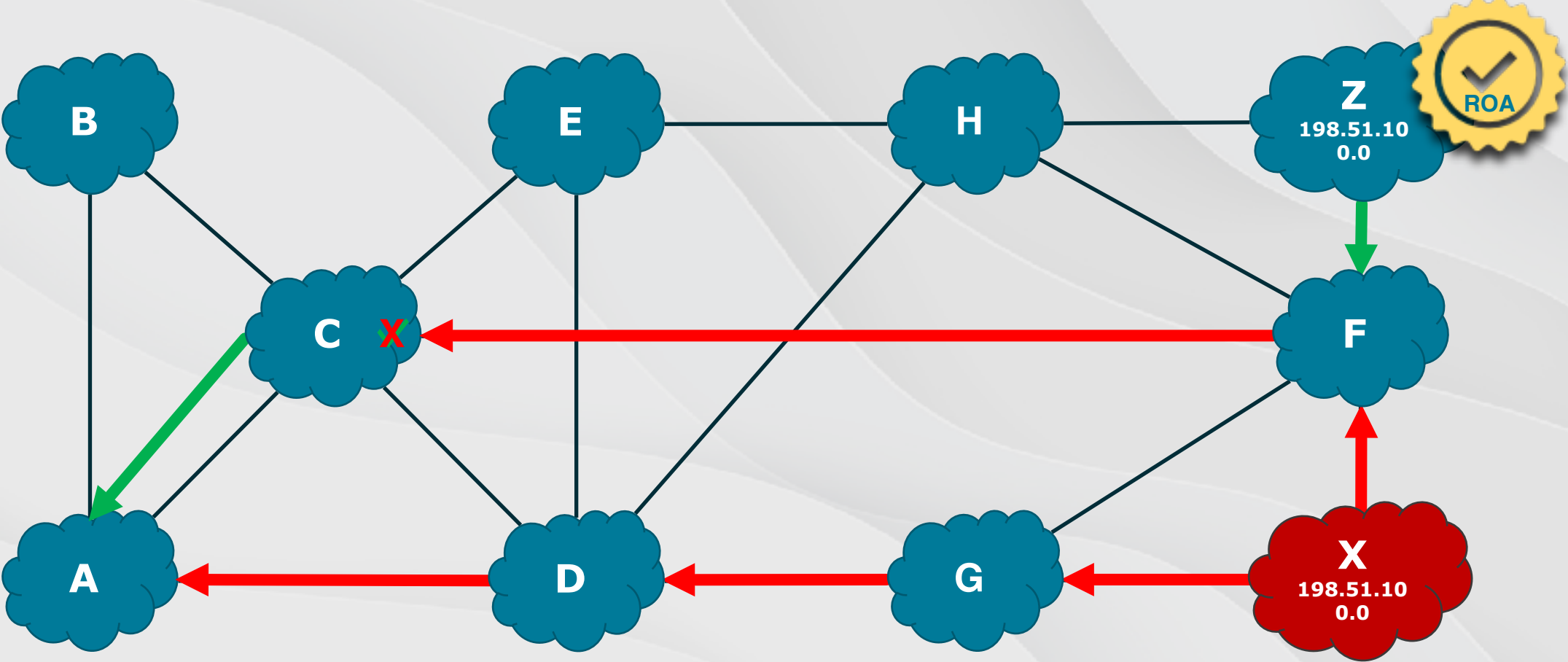
Relying Party software confirms repository data authenticity to **establish RPKI validity state**



## Action

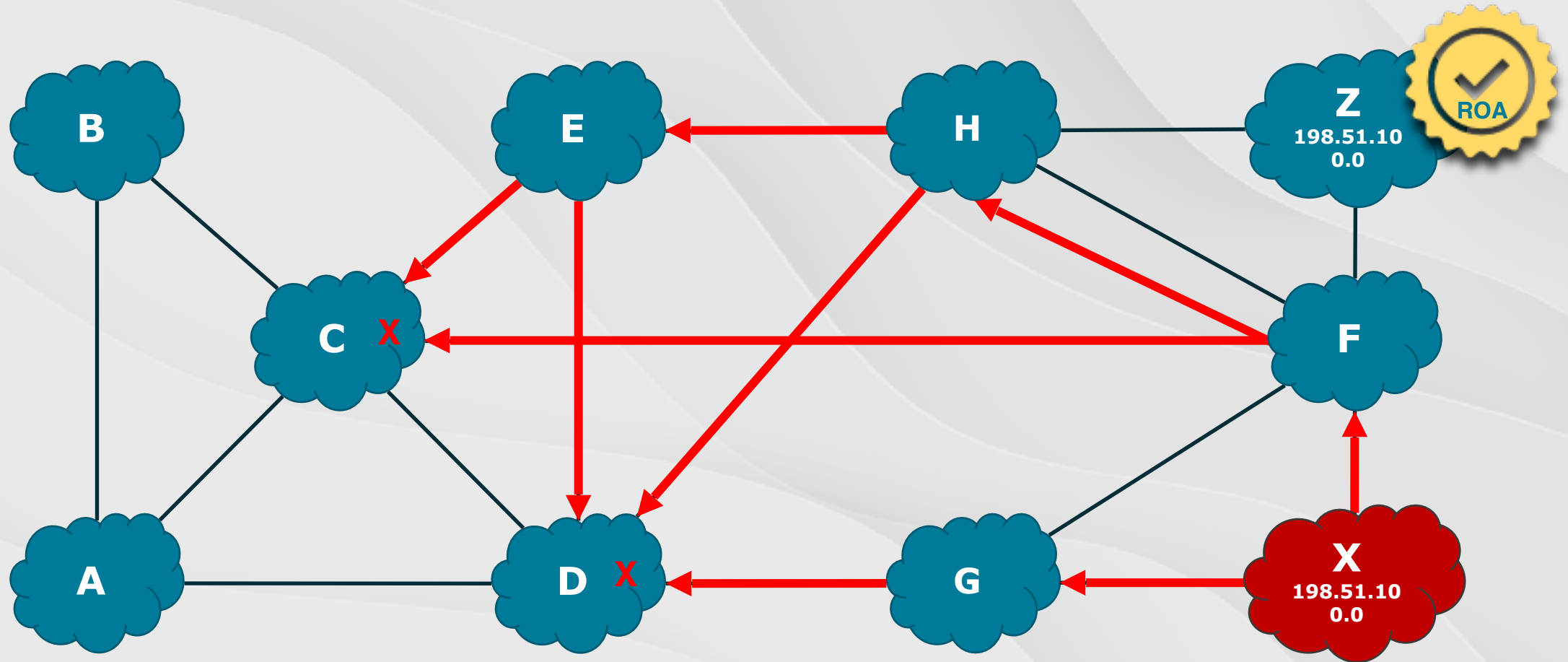
Network operators perform **ROV**, enhancing global routing security

# Route Origin Validation in Action

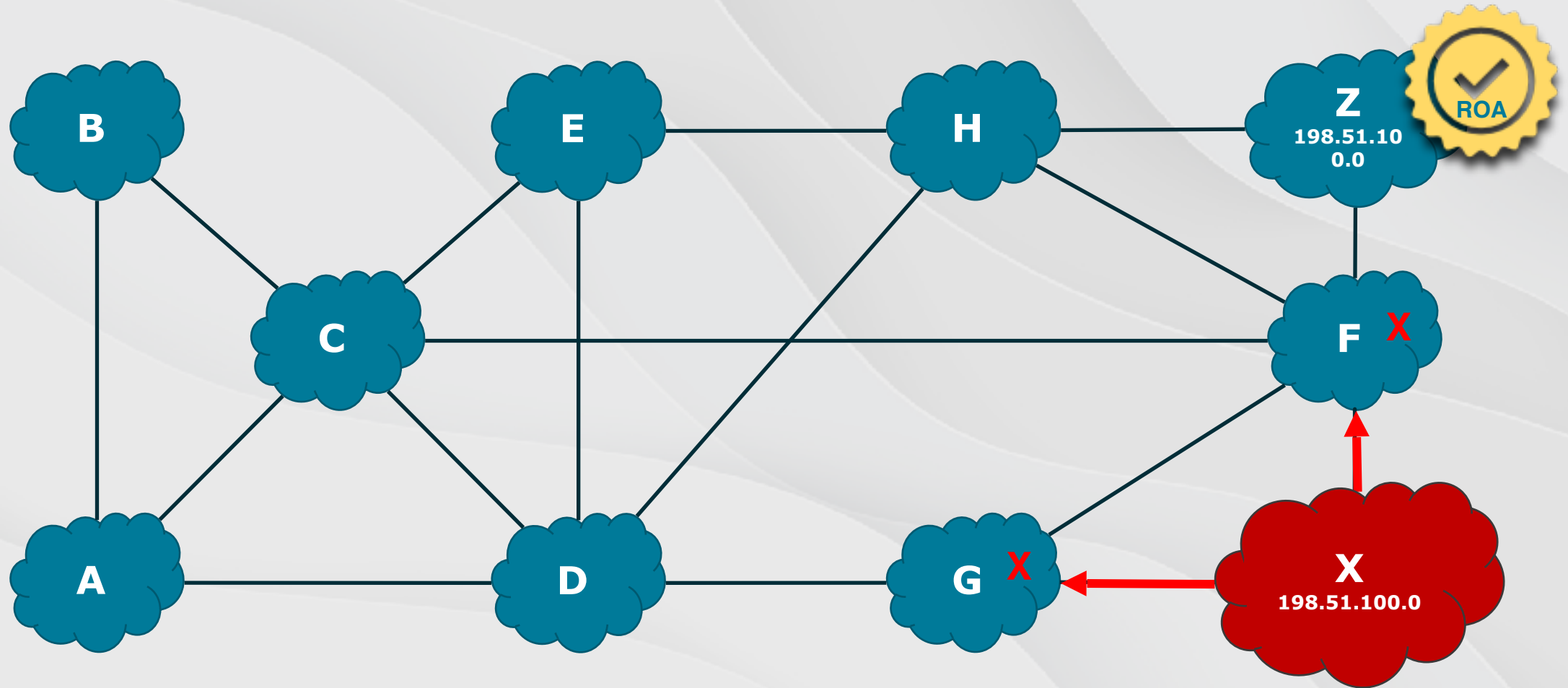


AS Z: 198.51.100.0/24  
AS X: 198.51.100.0/24

# Origin Validation in Action



# Origin Validation in Action



# ASPA and Path Validation

# AS Provider Authorization (ASPA)

- ASPA is a signed statement: *"This is my ASN, and I certify the following ASNs are my upstream providers."*
- Enables BGP to signal when the path should be considered ineligible for route selection.
- Intent is to protect against malicious route leaks and BGP AS\_PATH manipulations.

**Proposed IETF standard**

# Path Validation with ASPA

- Developed as a complimentary feature to ROV
- ASPA enforces “valley-free” routing – traffic goes up to a provider, optionally across a peer, then down to a destination.
- Compares received BGP AS\_PATH information to data in an ASPA object to establish validity
- Same validity states as ROV:  
**Valid, Invalid, and Unknown**

## Why Do We Need Path Validation?

- Route Origin Validation **ONLY** verifies the IP prefix is being originated from the authorized ASN.
- If the Origin AS is spoofed, unauthorized announcements could be marked as valid, defeating ROV.
- Utilizing Path Validation and Origin Validation together reduces the exposure to hijack attempts or misconfiguration, further enhancing routing security.

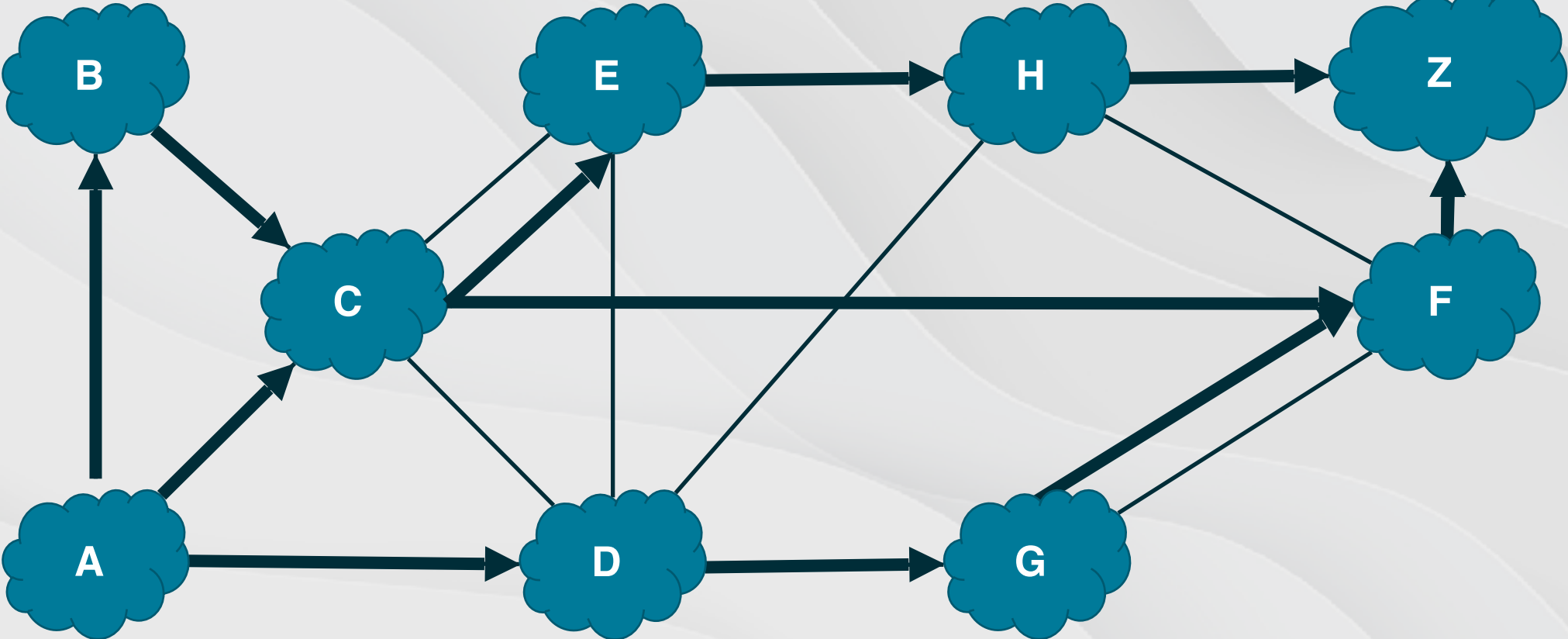
# The AS0 ASPA

The statement you are declaring is *“This is my ASN and I have no upstream providers.”*

- Tier-1 providers can create an AS 0 ASPA to identify an ASN used for settlement free peering.
- **BE CAREFUL!** If you create an AS0 ASPA, there WILL be unintended impact to your existing route announcements

# Path Verification - ASPA

Path: H,E,C,A  
F,G,D,A  
F,C,B,A



Customer: A  
Provider: C,D



# ARIN RPKI Feature Set

# RPKI Services to Choose From

## Hosted RPKI

Recommended for most orgs who are just getting started with RPKI and want access to ARIN developed tools. Least responsibility for the resource holder. Greater than 95% customers use Hosted RPKI.

## Delegated RPKI

Suggested for organizations that want/need cryptographic control of RPKI certificates; the organization should have a deeper understanding of RPKI, routing security, and a technical staff to maintain and publish the high availability repository.

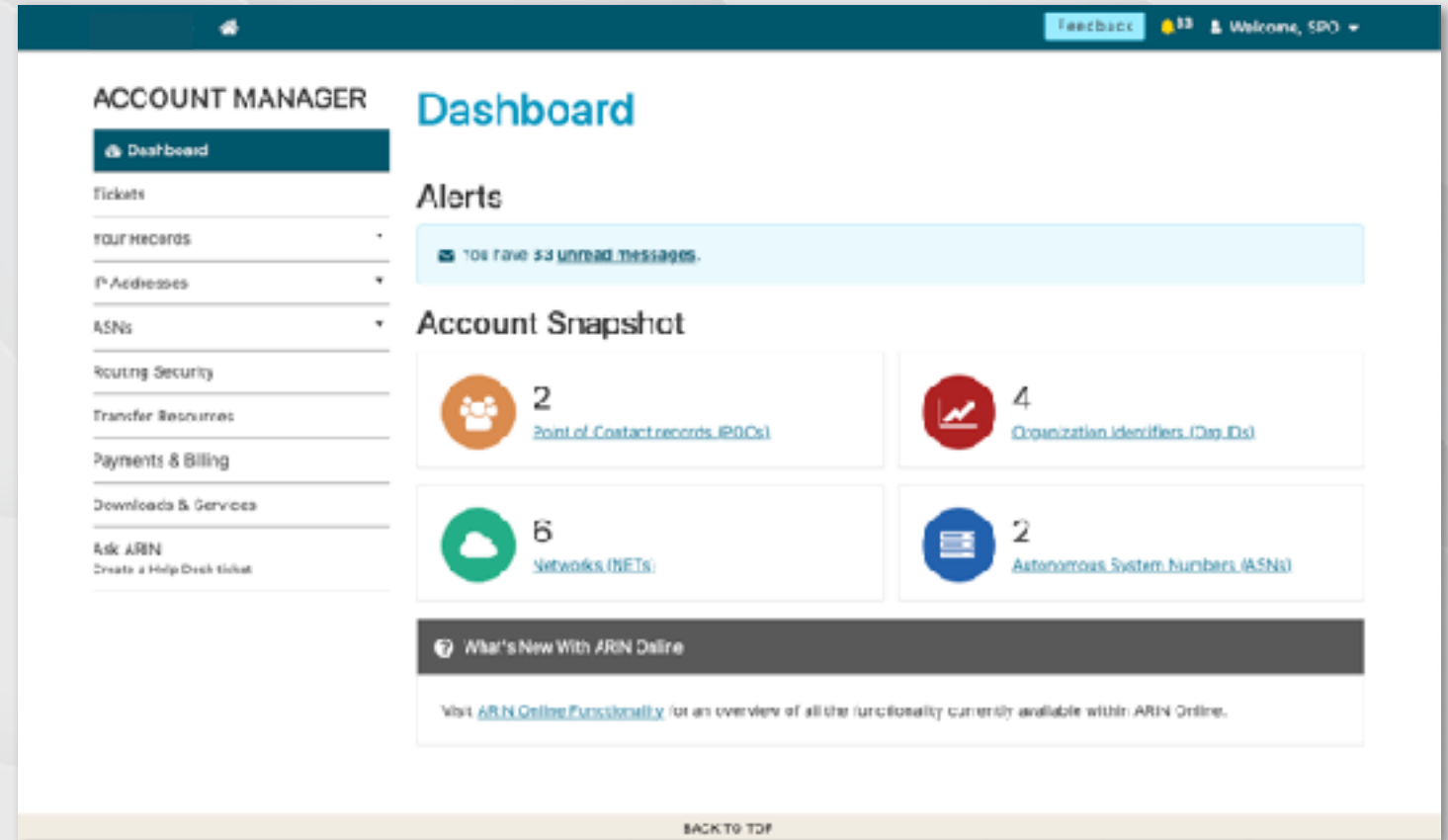
## Repository Publication Service

An option for organizations that wish to retain cryptographic control, but do not want to maintain the high availability repository and publication requirements.

# Two RPKI Environments

## ARIN Online

The live environment where your production decisions are applied

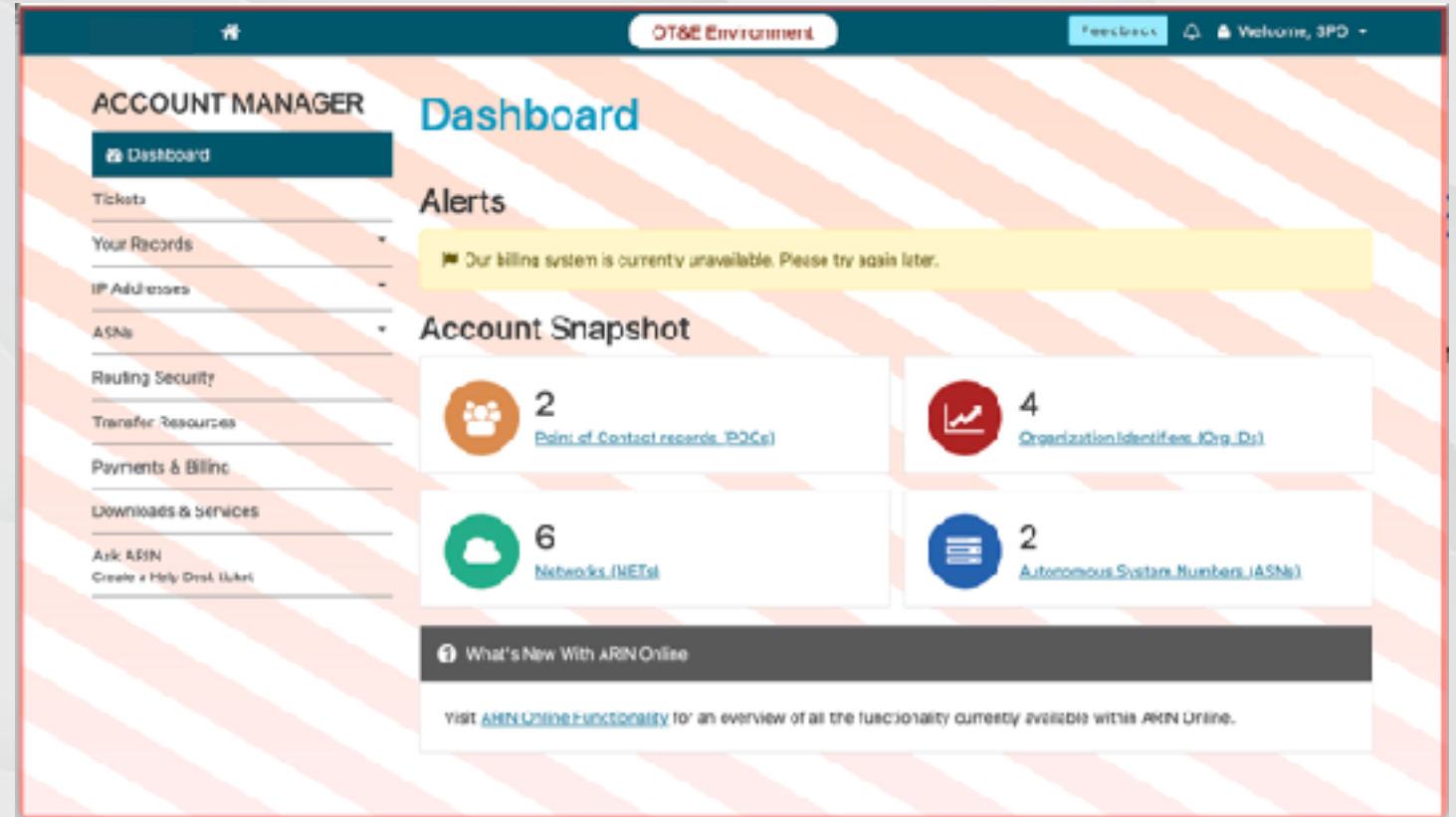


Log in at <https://account.arin.net>

# Two RPKI Environments

## Operational Test and Evaluation (OT&E)

A fully featured sandbox to test your configurations with zero impact in the real world



Log in at <https://account.ote.arin.net>

# One RESTful API Endpoint — RegRWS

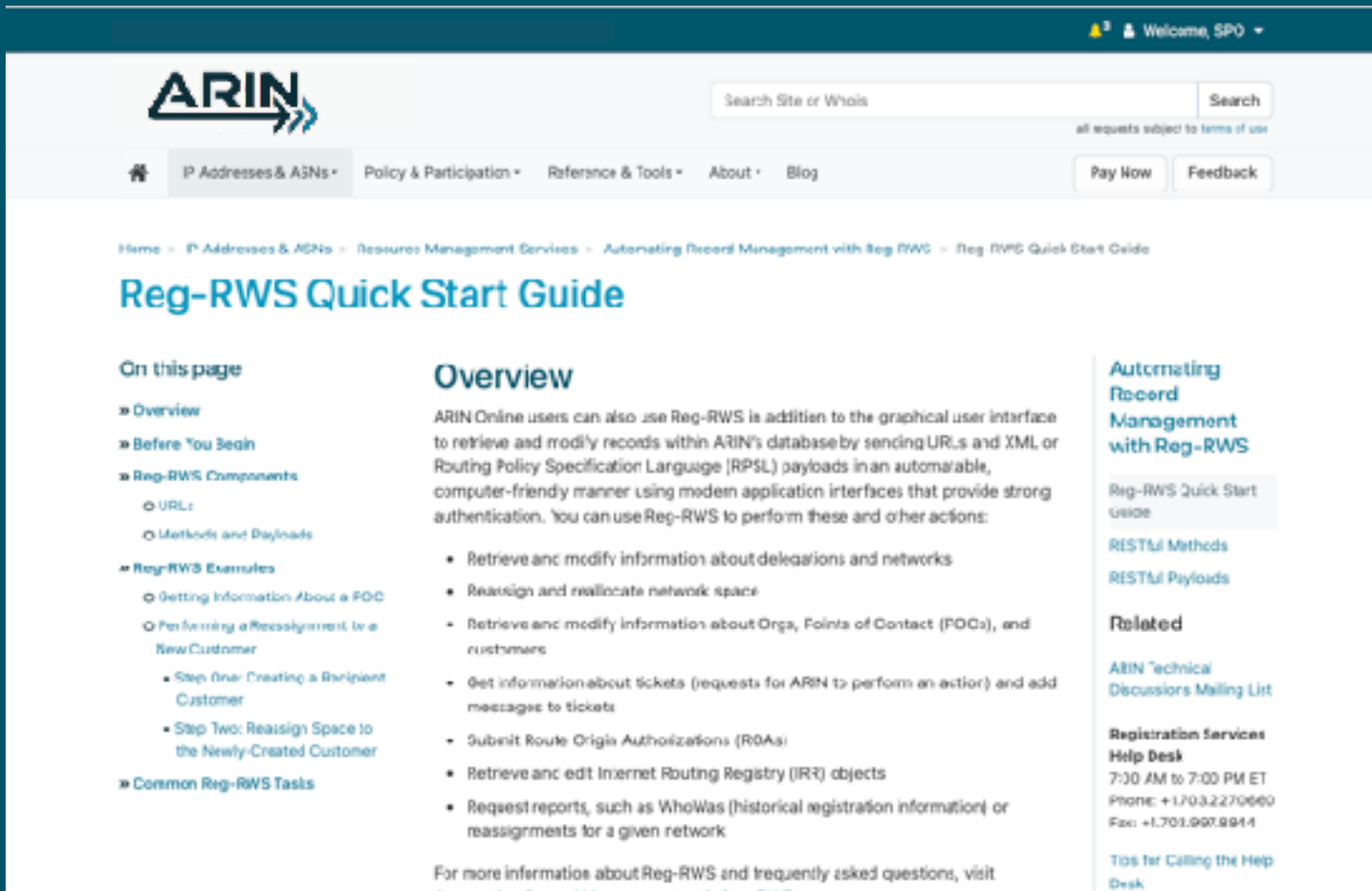
Feature parity with  
the ARIN Online  
web interface

Create and  
Delete actions  
made  
simultaneously

Able to make  
bulk atomic  
changes in one  
API call

Successfully  
tested making  
>1k changes in a  
single call

# Reg-RWS Quick Start Guide



The screenshot shows the ARIN website interface. At the top, there is a navigation bar with the ARIN logo on the left, a search box in the center, and a user greeting 'Welcome, SP0' on the right. Below the navigation bar, there are several menu items: 'IP Addresses & ASNs', 'Policy & Participation', 'Reference & Tools', 'About', and 'Blog'. There are also buttons for 'Pay Now' and 'Feedback'. The main content area features a breadcrumb trail: 'Home > IP Addresses & ASNs > Resource Management Services > Automating Record Management with Reg-RWS > Reg-RWS Quick Start Guide'. The title 'Reg-RWS Quick Start Guide' is prominently displayed. On the left side, there is a 'On this page' section with a list of links: 'Overview', 'Before You Begin', 'Reg-RWS Components' (with sub-links for 'URLs' and 'Methods and Payloads'), 'Reg-RWS Examples' (with sub-links for 'Getting Information About a POC' and 'Performing a Reassignment to a New Customer', which includes 'Step One: Creating a Recipient Customer' and 'Step Two: Reassign Space to the Newly-Created Customer'), and 'Common Reg-RWS Tasks'. The main content area has an 'Overview' section with a paragraph explaining that ARIN Online users can use Reg-RWS in addition to the graphical user interface to retrieve and modify records within ARIN's database by sending URLs and XML or Routing Policy Specification Language (RPSL) payloads in an automatable, computer-friendly manner using modern application interfaces that provide strong authentication. It lists several actions that can be performed: retrieve and modify information about delegations and networks; resign and reallocate network space; retrieve and modify information about Orgs, Points of Contact (POCs), and customers; get information about tickets (requests for ARIN to perform an action) and add messages to tickets; submit Route Origin Authorizations (ROAs); retrieve and edit Internet Routing Registry (IRR) objects; and request reports, such as WhoWas (historical registration information) or reassignments for a given network. At the bottom of the overview, it says 'For more information about Reg-RWS and frequently asked questions, visit Automating Record Management with Reg-RWS'. On the right side, there is a sidebar with the heading 'Automating Record Management with Reg-RWS'. It includes a link to 'Reg-RWS Quick Start Guide' (which is highlighted), 'RESTful Methods', and 'RESTful Payloads'. Below that is a 'Related' section with a link to 'ARIN Technical Discussions Mailing List'. At the bottom of the sidebar, there is a 'Registration Services Help Desk' section with the hours '7:30 AM to 7:00 PM ET', phone number '+1.703.227.0600', fax number '+1.703.997.9914', and a link to 'Tips for Calling the Help Desk'.

- <https://www.arin.net/resources/manage/regrws/quickstart/>
- <https://www.arin.net/resources/manage/regrws/methods/>

# Before You Get Started with RPKI, You Need the Following

IPv4 or IPv6 number resources directly allocated to your organization by ARIN

A user account linked to the organization as the Admin, Tech, or Routing Point of Contact (POC)

A signed Registration Services Agreement covering your resources

The Autonomous System Number (ASN) that is originating your prefixes

# Get Resources for Your Organization

The screenshot shows the ARIN website homepage. At the top, there is a dark blue header with the ARIN logo on the left and a search bar in the center. Below the header is a navigation menu with links for 'IP Addresses & ASNs', 'Policy & Participation', 'Reference & Tools', 'About', and 'Blog'. A 'Pay Now' button and a 'Feedback' link are also visible. A large blue banner below the navigation contains the text: 'ARIN is a nonprofit, member-based organization that administers IP addresses & ASNs in support of the operation and growth of the Internet.' Below the banner is a grid of five service tiles: 'New to ARIN' (info icon), 'Request IP Addresses & ASNs' (plus icon), 'Transfers' (recycling icon), 'IPv6 Info' (globe icon), and 'Get Involved' (handshake icon). Below the grid is an 'ANNOUNCEMENTS' section with three items: 'Apply Now for an ARIN Community Grant' (Governance, dated Thu, 17 Apr 2025), 'Consultation on Draft "Governance Document for the Recognition, Maintenance, and Derecognition of Regional Internet Registries"' (Governance, dated Mon, 16 Apr 2025), and 'New Features Added to ARIN's Registration Data Access Protocol Service' (Service Update, dated Wed, 21 May 2025).

- IPv6 is available today, join the IPv4 waitlist, ASNs
- Transfers
  - M&A
  - Qualified Facilitators
- Leasing

# Plan Out Your RPKI Deployment

Be certain of the which RPKI type you are going to deploy as changing in the future will be disruptive.

The ROAs you create will be visible in the RPKI repository after the next regeneration cycle is executed (every five minutes).

DDoS services may have specific requirements that could determine your ROA creation scheme.

The effect of a newly created ROA may not be realized for 30 to 60 minutes after publication.

# RPKI ROA Best Practices

# Limit the Use of maxLength

If you create a ROA for a /16 block with a maxLength of /24, you are indicating that every potential prefix – from the aggregate /16 down to the longest matching /24 originating from the specified AS – should be treated as authentic.

This includes 511 prefixes: all /24s, all /23s, all /22s, and so on. Liberal use of maxLength in ROAs exposes you to a forged-origin sub-prefix hijack.

More information can be found in [RFC 9319: The Use of maxLength in the Resource Public Key Infrastructure](#)

## Create ROAs **That Match** The Prefixes You Announce

If you have a /16 of IPv4 space or a /32 of IPv6 space, chances are you are not announcing every /24 or /48 subnet.

Creating ROAs that **exactly match your announcements** should reduce the number of ROAs you create, which not only saves time but also limits your exposure to hijacks resulting from misconfiguration or nefarious announcements.

# Create ROAs For The Most Specific Prefixes First

Suppose you are announcing a /16 aggregate and a subset of /24s within the aggregate block.

If you create a ROA for only the /16 aggregate, all existing /24 announcements will be marked as RPKI invalid.

Go backwards  
(/24, /23, /22, ..., /16).

**Let's take a break**



# Before We Get Started Again

- On the table up front, there are twenty sets of `student` credentials available for use during the hands-on portion of the workshop. Please come up and get a set.
- Take a workbook as well! — this will be used during our workshop today, It's yours to keep. Take it home for future reference.
- Please wait to log in until we reach the hands-on portion of today's workshop

## Wi-Fi Info:

# Parts of the Card

Login Information



User ID: RSUser1

Password: RoutingSecurityUser1!

Token Pin: RSUser2

Recovery Code!



**ARIN** | Deep Dive

# Getting Started with Hosted RPKI





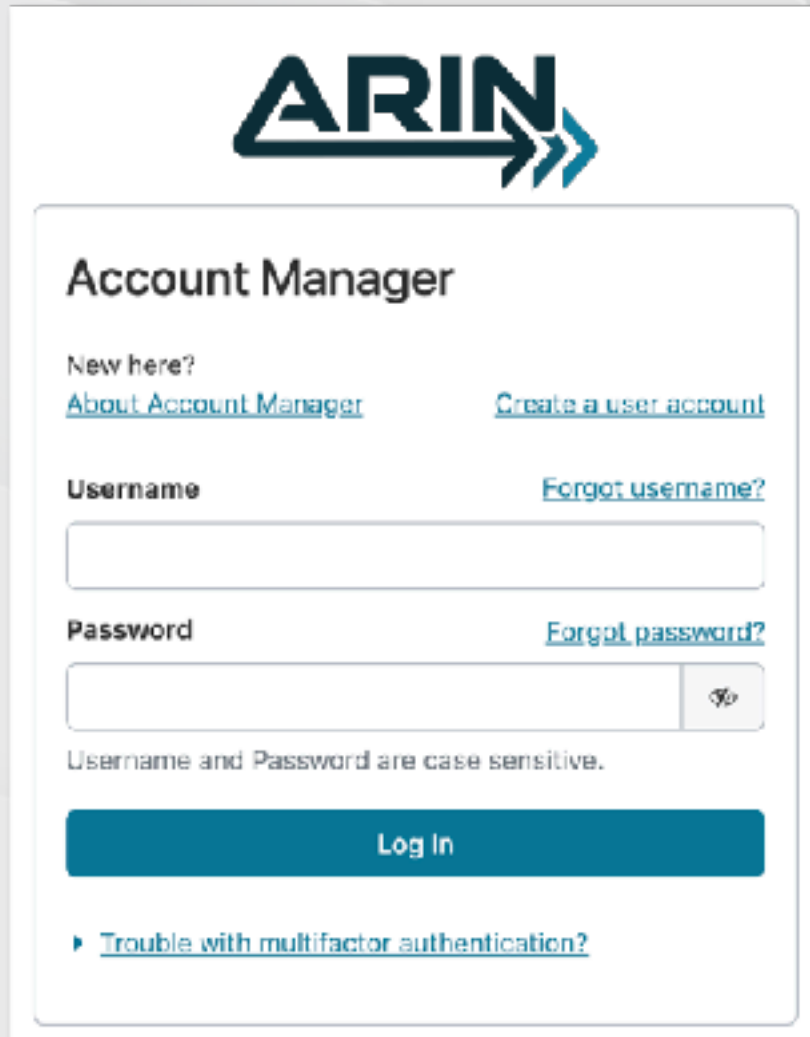
**Let's Begin**





# ARIN Online User Interface

# Accessing ARIN Online



The screenshot shows the ARIN Account Manager login interface. At the top is the ARIN logo. Below it is the title "Account Manager". There are two links: "About Account Manager" and "Create a user account". The "Username" field is followed by a "Forgot username?" link. The "Password" field is followed by a "Forgot password?" link and a toggle for password visibility. A note states "Username and Password are case sensitive." Below the fields is a blue "Log In" button. At the bottom, there is a link for "Trouble with multifactor authentication?".

- If you are a first-time customer of ARIN, select **Create a user account**.
- Instructional videos that explain how to complete the steps above can be found at [arin.net/howtovideos](https://arin.net/howtovideos)
- If you already have a user account, enter your credentials and select **Log In** to continue
- <https://account.arin.net>

# ARIN Online User Dashboard

The screenshot displays the ARIN Online User Dashboard. At the top, there is a dark teal header with a 'Feedback' button, a user profile icon, and the text 'Welcome, R5UserONE'. Below the header, the page is divided into a left sidebar and a main content area. The sidebar, titled 'ACCOUNT MANAGER', contains a 'Dashboard' link (highlighted in dark teal) and several other menu items: Tickets, Your Records, IP Addresses, AENa, Routine Security, Transfer Resources, Payments & Billing, Downloads & Services, Ask ARIN, and Create a Help Desk ticket. The main content area is titled 'Dashboard' and features an 'Account Snapshot' section. This section contains four data cards: 1. ARIND5-ARIN (Point of Contact record (POC)) with an orange icon and a link. 2. 2 Organization Identifiers (Org IDs) with a red icon and a link. 3. 4 Networks (NETs) with a green icon and a link. 4. 0 Autonomous System Numbers (ASNs) with a blue icon and a link. Below these cards is a 'What's New With ARIN Online' section with a dark teal header and a link to 'ARIN Online Functionality'.

- Once logged in, a user can see information related to all linked organizations.
- Functionality and access is based on the Point of Contact the user is linked to.
- To make RPKI decisions, the user must be the Admin, Tech, or Routing Point of Contact.
- Select Routing Security in the left navigation bar

# Routing Security Dashboard

## Routing Security Dashboard

ARIN supports routing security with two services: [Internet Routing Registry \(IRR\)](#) and [Resource Public Key Infrastructure \(RPKI\)](#). Registrants can use these services to help secure Internet routing for their eligible resources.

### Your Organizations

Organizations associated with your user account are listed alphabetically by Org ID.

Org ID	IRR		RPKI	
	Eligibility	Action	Eligibility	Action
ARIN-2	✓	<a href="#">Manage IRR</a>	✓	<a href="#">Sign up for RPKI</a>
ARIND-1	✓	<a href="#">Manage IRR</a>	✓	<a href="#">Sign up for RPKI</a>

- Search for your organization on the Routing Security dashboard
- Select **Sign up for RPKI**

# Manage RPKI – Selection Sign Up

**Manage RPKI**

Org ID: ARIND-1

ARIN's Resource Public Key Infrastructure (RPKI) service allows you to publish authorized originations for your routes to help secure Internet routing. On sign-up, ARIN generates a Resource Certificate for the number resources that are both directly assigned to the Org ID and covered under a signed Services Agreement (RSA/LRSA) with ARIN.

Use of the RPKI services via ARIN Online or through a RESTful API, including but not limited to the creation, modification, and usage of RPKI objects, is subject to [ARIN's RPKI Terms of Service](#).

### Choose Between Two Models of RPKI

Hosted RPKI	Delegated RPKI
<p>Use ARIN's infrastructure to create and manage your ROAs. <a href="#">Learn more about Hosted RPKI.</a></p> <ul style="list-style-type: none"><li>• Uses ARIN's CA and repository</li><li>• You can start right away</li><li>• Create ROAs with a simple web form</li><li>• ROAs are automatically renewed</li><li>• You can also automate with ARIN's <a href="#">Req-RWS API</a></li></ul> <p><a href="#">Sign up for Hosted</a></p>	<p>Run your own Certificate Authority (CA) to create and manage your ROAs. <a href="#">Learn more about Delegated RPKI.</a></p> <ul style="list-style-type: none"><li>• Use your CA</li><li>• To start, get the <a href="#">Child Request XML</a> from your CA software</li><li>• Run your own publication server or use <a href="#">ARIN's Publication Service</a></li></ul> <p><a href="#">Sign up for Delegated</a></p>

- The first time you reach the Manage RPKI page, you must pick your deployment type: **Hosted** or **Delegated**
- Hosted customers have access to RPKI tools developed by ARIN
- Delegated customers have more control of the cryptographic element, but are responsible for operating a Certificate Authority (CA), and publishing and maintaining a high availability RPKI repository
- Select **Sign up for Hosted**

# Manage RPKI – Status Overview

The screenshot shows the 'Manage RPKI' interface. At the top left, there is a dropdown menu for 'Org ID' set to 'ARINL'. To its right, under 'Hosted RPKI:', there are several tabs: 'Overview' (which is active), 'ROAs', 'ASPAs', and 'IRR Auto-Manager'. Below this, a link points to 'Resource Certification'. The main section is titled 'Status Overview' and contains the following information: 'Last Updated: 11-08-2025' with a link to 'Current Certificate'; 'Certified Resources: 1 ASN, 2 Nets'; 'ROAs: 0'; and 'ASPAs: 0'. At the bottom left, there is a link to 'View the ROA Change Log'. At the bottom right, there are two buttons: 'Create ASPA' and 'Create ROA'.

- The Status Overview table has links to the lists of ROAs and ASPAs
- Another link identifies Internet number resources allocated to you by ARIN and eligible for RPKI use
- You will find buttons that bring you to the ROA and ASPA creation forms
- There is a dropdown to navigate to all linked Org IDs signed up for RPKI services

# Manage RPKI – Certified Resources

ASNs		
No Autonomous System Numbers (ASNs) are covered by the Resource Certificate.		
IP Networks		
The following IPv4 and IPv6 network allocations are covered by the Resource Certificate.		
Prefixes (Net Range)	Net Handle and Name	Related ROAs
2502:FC3B:E000::/36	NET6-2502-FC3B-E000-1 (ARIND-1)	0
2520:10F:F000::/44	NET6-2520-10F-F000-1 (ARIN-DEPLOYATON)	0

- The certified resources table identifies the ASNs and IP networks that are on the RPKI resource certificate.
- The number in the related ROAs column is the count of times the specific resource shows up in a ROA.
- If you select the number, it will show a filtered list of the ROAs.

# RPKI – ROA Table

## Route Origin Authorizations (ROAs)

Filter ROAs by Origin AS or Prefix.

Resource:  [Search ROAs](#)

Example: AS64496 or 64496, 2001:db8::/48 or 192.0.2.0/24

Org ID ARINL has 7 ROAs in ARIN's RPKI Repository.

Origin AS	Prefixes	ROA Name	
12076	149.112.154.0/24	Azure BYOIP	<a href="#">Manage ROA</a>
399970	149.112.152.0/22	BG Services	<a href="#">Manage ROA</a>
399970	149.112.152.0/23	Max Length: 24 corporate offices	<a href="#">Manage ROA</a>
399970	149.112.152.0/24	Max Length: 32	<a href="#">Manage ROA</a>
399970	2602:FC3B::/33	training block	<a href="#">Manage ROA</a>
399970	2602:FC3B:1000::/36	East Coast datacenters	<a href="#">Manage ROA</a>
399970	2602:FC3B:1500::/40 2602:FC3B:1600::/40 2602:FC3B:1700::/40 2602:FC3B:1800::/40	Winchester-Hickory-Savannah-Annapolis	<a href="#">Manage ROA</a>

- The table is representative of an org with existing ROAs
- Use the search field to sort the ROAs and filter the origin AS or IP prefixes
- Select the **Create ROA** button above the table to access the ROA Create form

# Creating ROAs

# ROA Entry Form

Create a Route Origin Authorization (ROA)

\* denotes required field

\*Origin AS:

Prefix  Max Length

\*Prefixes:

ROA Name:

Optional: Provide a helpful nickname, such as DDoS\_Mitigation

- The ROA create form has two mandatory fields: Origin AS and Prefixes
- There are two optional fields: Max Length and ROA Name
- Select the **Create ROA** button above the table to access the ROA Create form

# Create ROA Review

## Review ROA

Origin AS: 399970  
Prefixes: 2602:fc3b:ef00::/40  
Auto-renewing: Yes  
ROA Name: NET-2602-fc3b-ef00-40

Allow IRR Auto-Manager to create and link 1 matching route object ?

[View 1 the object](#)

Create and auto-manage AS399970 - 2602:FC3B:EF00::/40

[Previous Step](#) [Submit](#)

- All ROAs created using ARIN Online (or the Reg-RWS RESTful endpoint) auto-renew every 90 days.
- The IRR Auto-Manager creates an IRR route object that matches each Origin AS and prefix in the ROA.
- If you are happy with the data you entered, select **Submit**.
- Select **Previous Step** to make changes.

# Create ROA Success

**Route Origin Authorizations (ROAs)**

Filter ROAs by Origin AS or Prefix.

Resource:  [Search ROAs](#)

Example: AS64496 or 64496, 2001:DB8::j4B or 192.0.0.0/24

Org ID AR:ND-1 has 1 ROA in ARIN's RPKI Repository.

Origin AS	Prefixes	ROA Name	
399970	2602:FC3B:EF00::/40	NET-2602-1c3b-ef00-40	<a href="#">Manage ROA</a>

- The table now shows the newly created ROA
- You will also see a green success banner displayed above the table
- Select the **Create ROA** to continue covering your number resources

# Create Multi-Prefix ROA

**Create a Route Origin Authorization (ROA)**

\* denotes required field

\*Origin AS:

Prefix ?	Max Length ?	
<input type="text" value="2602:fc3b:ef10::/44"/>	<input type="text"/>	<input type="button" value="✖"/>
<input type="text" value="2602:fc3b:ef20::/44"/>	<input type="text"/>	<input type="button" value="✖"/>
<input type="text" value="2602:fc3b:ef30::/44"/>	<input type="text"/>	<input type="button" value="✖"/>
<input type="text" value="2602:fc3b:ef40::/44"/>	<input type="text"/>	<input type="button" value="✖"/>

ROA Name:

Optional: Provide a helpful nickname, such as DDOS\_Mitigation

- There is no limit to the number of prefixes that can be entered into an individual ROA.
- Select the **Additional Prefix** button for every origin/prefix pair you want to add.
- Select the **Next Step** to proceed.

# Create Multi-Prefix ROA Review

## Review ROA

**Origin AS:** 339970

**Prefixed:** 2602:fc3b:ef10::/44  
2602:fc3b:ef20::/44  
2602:fc3b:ef30::/44  
2602:fc3b:ef40::/44

**Auto-renewing:** Yes

**ROA Name:** NET-2602-fc3b-ef10

Allow IRR Auto-Manager to create and link 4 matching route objects

[View the 4 objects](#)

Create and auto-manage	AS339970 - 2602:FC3B:EF10::/44
Create and auto-manage	AS339970 - 2602:FC3B:EF20::/44
Create and auto-manage	AS339970 - 2602:FC3B:EF30::/44
Create and auto-manage	AS339970 - 2602:FC3B:EF40::/44

[Previous Step](#) [Submit](#)

- The Review ROA table presents the same information as a single prefix ROA
- Select the **Submit** button to continue and return to the ROAs table

# Create Multi-Prefix ROA Success

**RPKI: ROAs**

✓ ROA for "AS389970 - 2602:fc3b:ef10::/44 ..." was saved successfully.

Org ID: ARIND-1 Hosted RPKI: [Overview](#) [ROAs](#) [ISB Auto-Manager](#) [Create ROA](#)

### Route Origin Authorizations (ROAs)

Filter ROAs by Origin AS or Prefix:

Resource:  [Search ROAs](#)

Example: AS64496 or 64496, 2001:DB8::/16 or 192.0.0.0/24

Org ID ARIND-1 has 2 ROAs in ARIN's RPKI Repository.

Origin AS	Prefixes	ROA Name	
389970	2602:FC3B:EF00::/40	NET-2602-fc3b-ef00-40	<a href="#">Manage ROA</a>
389970	2602:FC3B:EF10::/44 2602:FC3B:EF20::/44 2602:FC3B:EF30::/44 2602:FC3B:EF40::/44	NET-2602-fc3b-ef10	<a href="#">Manage ROA</a>

- You will see confirmation at the top of the page in the green bar
- New ROA added to the table
- Select **Manage ROA** next to the multi-prefix in the table, and we can go look at the available options

# Create ROA - Failure

## Create a Route Origin Authorization (ROA)

\* denotes required field

\*Origin AS:

Prefix  Max Length

\*Prefixes:

**The CIDR block you specified is not covered by this resource certificate.**

ROA Name:

**A ROA name must only contain the following characters: a-z A-Z 0-9 \_ - and space.**

Optional: Provide a helpful nickname, such as DDOS\_Mitigation

## Why might you get a ROA creation error?

- Attempting to use IP prefixes that are not allocated to you
- Use of a character not permitted in the ROA name field
- An overlapping origin/prefix pairing with an existing ROA
- Where can I look to find out why?

# Which Resources are Certified?

## ASNs

No Autonomous System Numbers (ASNs) are covered by the Resource Certificate.

## IP Networks

The following IPv4 and IPv6 network allocations are covered by the Resource Certificate.

Prefixes (Net Range)	Net Handle and Name	Related ROAs
2802:FC3B:ED0D::/36	NET6-2802-FC3B-ED0D-1 (ARIND-1)	1
2620:10F:F000::/44	NET6-2620-10F-F000-1 (ARIN-DEPLOYATON)	0

For more information about resources and ROAs, please visit [Resource Certification \(RPK\)](#).

- Go back to the Overview Tab and select **Certified Resources**
- Is the IP prefix you entered on your resource certificate?
- ARIN is the authority that identifies who has been allocated resources
- No misconfiguration or a nefarious attempt at creating a ROA with your resources by others is blocked

# Ineligible Resources – User Dashboard

The screenshot shows a user dashboard with the following sections:

- Dashboard** (header)
- Alerts** section containing two messages:
  - A light blue message: "You have an [unread message](#)."
  - A yellow message: "**1 Network** is ineligible for routing security services such as RPKI and ARIN's IRR. [Learn more](#)."
- Account Snapshot** section with four metrics:
  - ARIND5-ARIN Point of Contact record (POC) (orange icon)
  - 2 Organization Identifiers (Org IDs) (red icon)
  - 4 Networks (NETs) (green icon)
  - 0 Autonomous System Numbers (ASNs) (blue icon)

- The alerts field says there is one ineligible network.
- Select the **1 Network** link in the yellow alerts field.
- Alternatively, select **IP Addresses** then **Manage Networks** in the left-hand navigation to reach the same destination.

# Ineligible Resources – Manage Resources

Include the 0 networks you've reassigned in your search  
 Limit search to the 1 network not covered by RSA/LRSA

Net Handle	Net Range	Net Type	Net Name	Org ID	
<a href="#">NET6-2602-FC3B-C000-1</a>	2602:FC3B:C000::/36	Reallocated	NET-2602-FC3...	ARIND-1	+
<a href="#">NET6-2602-FC3B-E000-1</a>	2602:FC3B:E000::/36	Direct Alloca...	ARIND-1	ARIND-1	+
<a href="#">NET6-2620-10F-F000-1</a>	2620:10F:F000::/44	Direct Alloca...	ARIN-DEPLOYA...	ARIND-1	+
<a href="#">NET-205-196-98-0-1</a> *	205.196.98.0/24	Direct Alloca...	WEBINAR-TEST	ARIN-2	+

Networks highlighted and marked with an asterisk (\*) are not covered by an ARIN Registration Services Agreement (RSA) or Legacy RSA (LRSA).

To use ARIN's IRR and RPKI services, the network issued directly from ARIN must be under a signed RSA or LRSA. For assistance, call Registration Services at +1.703.227.0660.

- IP resources must be covered by an RSA to be eligible for RPKI use.
- Reallocated resources do not appear on the recipient's resource certificate
- The direct resource holder must create ROAs on the recipient's behalf

# Modifying ROAs

# Modify ROA

## Route Origin Authorizations (ROAs)

Filter ROAs by Origin AS or Prefix.

Resource:  Search ROAs

Example: AS64496 or 64496, 2001:DB8::/48 or 192.0.0.0/24

Org ID ARIND-1 has 2 ROAs in ARIN's RPKI Repository.

Origin AS	Prefixes	ROA Name	
389970	2602:FC3B:EF00::/40	NET-2602-fc3b-ef00-40	<span>Manage ROA</span>
399970	2602:FC3B:EF10::/44 2602:FC3B:EF20::/44 2602:FC3B:EF30::/44 2602:FC3B:EF40::/44		<span>Manage ROA</span>

- Back to the ROA table... note the **Manage ROA** button in each row for the corresponding ROA
- Select **Manage ROA** next to the multi-prefix in the table

# Modify ROA

### Modify Route Origin Authorization (ROA)

\* denotes required field

Origin AS: 399370

Prefix ?	Max Length ?	
<input type="text" value="2602:FC3B:EF10::/44"/>	<input type="text"/>	
<input type="text" value="2602:FC3B:EF20::/44"/>	<input type="text"/>	
<input type="text" value="2602:FC3B:EF30::/44"/>	<input type="text"/>	
<input type="text" value="2602:FC3B:EF40::/44"/>	<input type="text"/>	

ROA Name:

Optional: Provide a helpful nickname, such as DDOS\_Mitigation

- There is a trash can icon next to each prefix contained in the ROA.
- Select the **trash can** for a prefix you want to remove from the ROA.

# Modify ROA – post select change

### Modify Route Origin Authorization (ROA)

\* denotes required field

Origin AS: 399970

	Prefix ?	Max Length ?	
*Prefixes:	<input type="text" value="2602:FC3B:EF10::/44"/>	<input type="text"/>	<input type="button" value="🗑"/>
	<input type="text" value="2602:FC3B:EF20::/44"/>	<input type="text"/>	<input type="button" value="🗑"/>
	<input type="text" value="2602:FC3B:EF40::/44"/>	<input type="text"/>	<input type="button" value="🗑"/>
	<input type="button" value="➕ Additional Prefix"/>		

ROA Name:

Optional: Provide a helpful nickname, such as DDOS\_Mitigation

- The prefix is removed from the list
- You can add a prefix during the same modify sequence; both actions will be executed simultaneously
- Select **Next Step**

# Modify ROA Review


## Review Changes

**Origin AS:** 399970

**Prefixes:** 2602:FC3B:EF10::/44  
2602:FC3B:EF20::/44  
2602:FC3B:EF40::/44

**Auto-renewing:** Yes

**ROA Name:** NET-2602-fc3b-ef10

**IRR Auto-Manager:**  Delete the route object linked to the 1 prefix you removed 

[View the 1 object](#)

Delete	descr: ARIN	AS399970 - 2602:FC3B:EF30::/44
--------	-------------	--------------------------------

[Previous Step](#) [Submit](#)

- Review your changes
- Select **Submit**

## Modify ROA Success

### Route Origin Authorizations (ROAs)

Filter ROAs by Origin AS or Prefix

Resources:  [Search ROAs](#)

Example: AS84496 or 64496, 2001:DB8::/48 or 192.0.0.0/24

Org ID ARIND-1 has 2 ROAs in ARIN's RPKI Repository.

Origin AS	Prefixes	ROA Name	
899970	2602:FC3B:EF00::/40	NET-2602-fc3b-ef00-40	<a href="#">Manage ROA</a>
899970	2602:FC3B:EF10::/44 2602:FC3B:EF20::/44 2602:FC3B:EF40::/44	NET-2602-fc3b-ef10	<a href="#">Manage ROA</a>

The requested change is reflected in the ROA table.

# Removing ROAs

# Remove ROA

**Route Origin Authorizations (ROAs)**

Filter ROAs by Origin AS or Prefix.

Resource:  Search ROAs

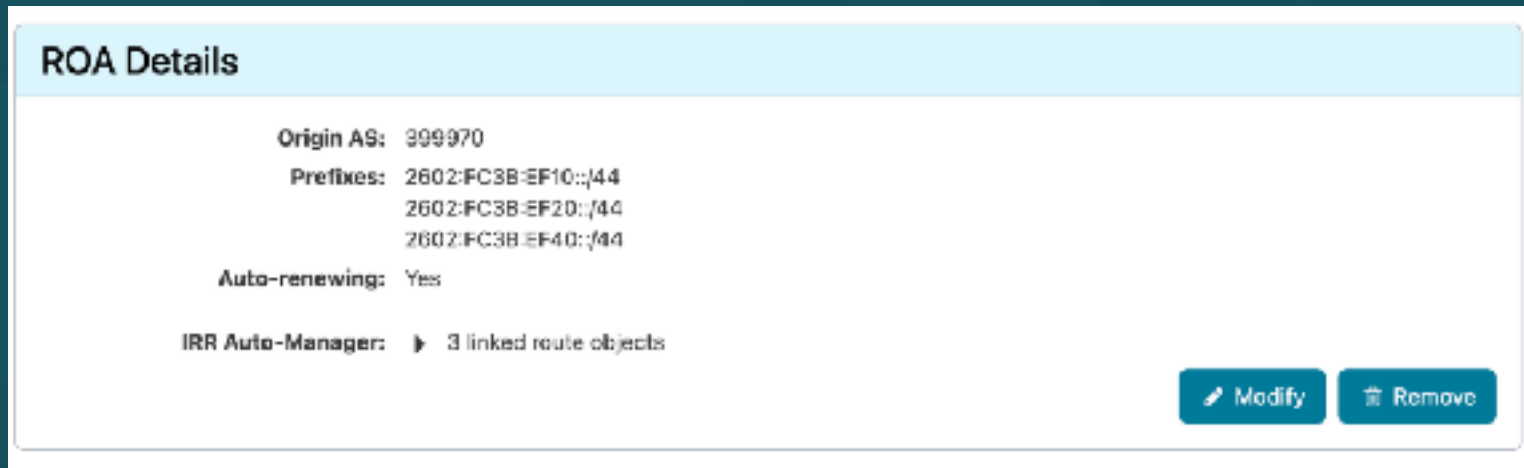
Example: ASE4496 or 64496, 2001:DB8::/48 or 192.0.0.0/24

Org ID ARIND-1 has 2 ROAs in ARIN's RPKI Repository.

Origin AS	Prefixes	ROA Name	
399970	2602:FC3B:EF00::/40	NET-2602-fc3b-e100-40	Manage ROA
399970	2602:FC3B:EF10::/44 2602:FC3B:EF20::/44 2602:FC3B:EF40::/44	NET-2602-fc3b-e110	Manage ROA

- The procedure to remove a ROA begins the same as modifying a ROA
- Return to ROAs table
- Select **Manage ROA** next to the multi-prefix ROA

# Remove ROA



The screenshot shows a 'ROA Details' window with the following information:

- Origin AS: 399970
- Prefixes: 2602:FC3B:EF10::/44, 2602:FC3B:EF20::/44, 2602:FC3B:EF40::/44
- Auto-renewing: Yes
- IRR Auto-Manager: 3 linked route objects

At the bottom right of the window, there are two buttons: 'Modify' and 'Remove'.

- In the ROA details window Select **Remove**

## Remove ROA – Confirm Request

### Are You Sure?

Are you sure you want to remove this ROA?  
There is no undo for this action.

**Origin AS:** 399970

**Prefixes:** 2602:FC3B:EF10::/44  
2602:FC3B:EF20::/44  
2602:FC3B:EF40::/44

Also delete the **3** route objects linked to this ROA

- There is a special confirmation step that notes there is no way to undo deleting a ROA.
- Confirm this is the ROA you want to remove by selecting **Remove**

# Remove ROA Success

### Route Origin Authorizations (ROAs)

Filter ROAs by Origin AS or Prefix.

Resource:  [Search ROAs](#)

Example: AS64496 or 64496, 2001:DB8::/48 or 192.0.0.0/24

Org ID ARIND-1 has 1 ROA in ARIN's RPKI Repository.

Origin AS	Prefixes	ROA Name	
399970	2802:FC3B:EF00::/40	NET-2802-fc3b-ef00-40	<a href="#">Manage ROA</a>

- A green bar show at the top of the page confirming the ROA was removed.
- The ROA table reflects the change as well, the multi-prefix ROA is no longer listed.

# Creating ASPAs

# ASPA Entry Form

## Create an Autonomous System Provider Authorization (ASPA)

\* denotes required field

\*Customer AS:

Specify an ASN registered to the selected Org ID.  
Example: AS64496 or 64496

**Set of Provider ASes**

Enter each upstream Provider AS that you authorize to handle traffic from the ASN.

\*Provider AS:

Example: AS64496 or 64496

Provider AS:

- Unlike the Origin AS in a ROA, the Customer AS **must be allocated to your organization** by ARIN
- The list of Provider ASNs should include upstream providers and non-transparent IXP route servers
- **DO NOT** include peer ASNs or customer ASNs
- Select **Create ASPA**

# ASPA Confirmation

✓ ASPA for "AS399970" with 2 providers was saved successfully.

## Autonomous System Provider Authorizations (ASPAs)

Org ID ARINL has 1 ASPA in ARIN's RPKI Repository.

Customer AS	Set of Provider ASes
399970	10746 20473

- You will receive confirmation the object creation was successful
- The ASPA will be listed in the table along with any others that were previously created

# Modifying an ASPA

# Modify an ASPA

Autonomous System Provider Authorizations (ASPA)	
Org ID ARINL has 1 ASPA in ARIN's RPKI Repository.	
Customer AS	Set of Provider ASes
399970	10745 20473



ASPA Object	
Customer AS:	399970
Set of Provider ASes:	10745 20473
<a href="#">Modify</a> <a href="#">Remove</a>	

- Modifying an ASPA works the same as modifying a ROA
- In the ASPA table, identify which object you want to modify and select the **Customer AS number**
- Select **Modify** to continue

# Modify an ASPA


## Modify Autonomous System Provider Authorization (ASPA)

\* denotes required field


Customer AS: 399970


### Set of Provider ASes

Update the list of upstream Provider ASes that you authorize to handle traffic from the ASN.

\*Provider AS:  

Example: AS64496 or 64496

Provider AS:  

 Additional Provider AS

- Here you can change a provider AS number, add a new provider AS, or delete a provider AS from the ASPA
- In this example, we are going to remove a provider AS from the ASPA
- Select the **trash can icon** next to provider **AS 20473**

# Modify an ASPA

## Modify Autonomous System Provider Authorization (ASPA)

\* denotes required field

Customer AS: 399970

**Set of Provider ASes**  
Update the list of upstream Provider ASes that you authorize to handle traffic from the ASN.

\*Provider AS:

Example: AS64496 or 64496

- The row with provider AS 20473 has been removed
- You may continue modifying the ASPA by changing the remaining provider AS number or adding a new one
- The changes can still be canceled at this point
- Select **Submit** to apply the changes

# Modify an ASPA

✓ Your ASPA has been updated.

## Autonomous System Provider Authorizations (ASPAs)

Org ID ARINL has 1 ASPA in ARIN's RPKI Repository.

Customer AS	Set of Provider ASes
<a href="#">399970</a>	10745

- Confirmation is received the change was successful
- The ASPA table shows the results of the modification

# Removing an ASPA

# Remove an ASPA

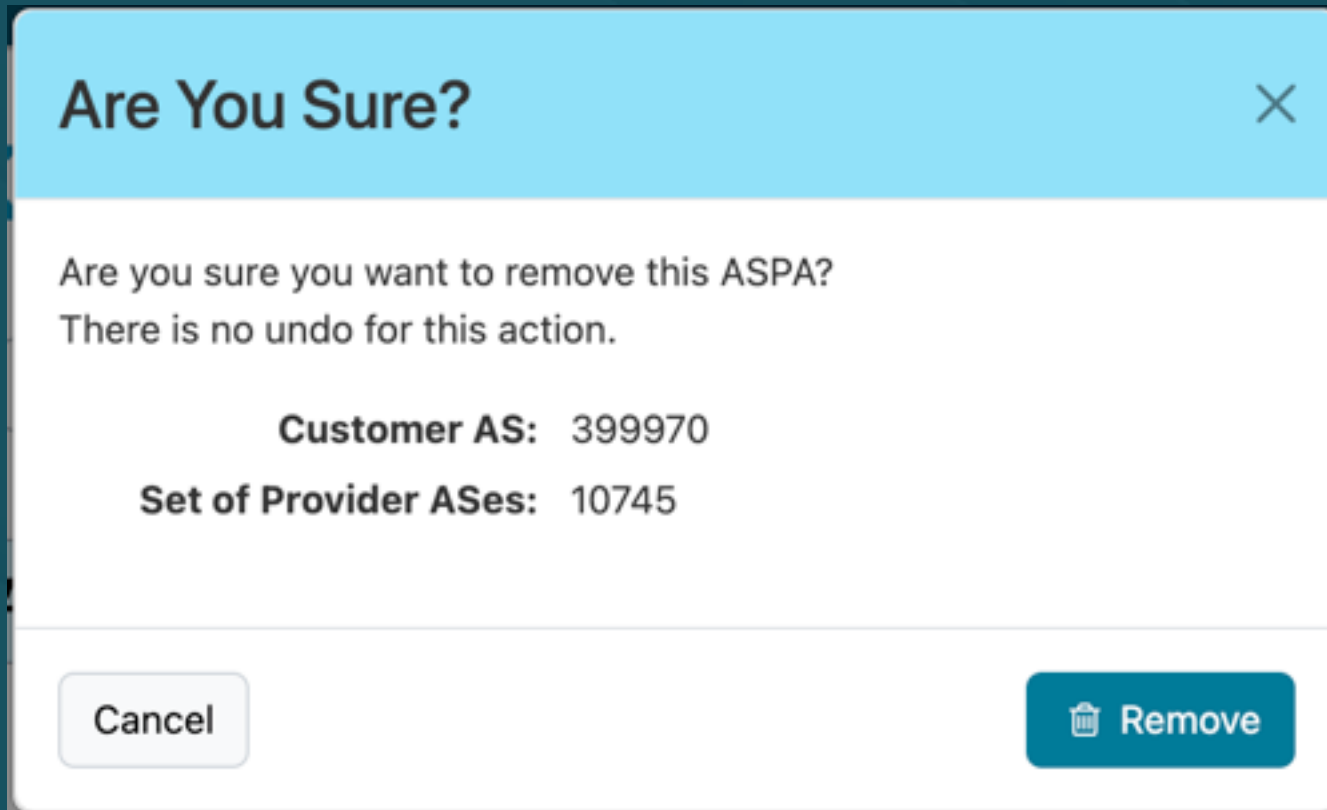
Autonomous System Provider Authorizations (ASPAs)	
Org ID ARINL has 1 ASPA in ARIN's RPKI Repository.	
Customer AS	Set of Provider ASes
<a href="#">399970</a>	10745



ASPA Object	
Customer AS:	399970
Set of Provider ASes:	10745
<a href="#">Modify</a> <a href="#">Remove</a>	

- Removing an ASPA starts the same as modifying an ASPA
- In the ASPA table, identify which object you want to remove and select the **Customer AS number**
- Select **Remove** to continue

## Remove ASPA – Confirm Request



- There is a confirmation step noting there is no undo
- You may still end the operation by selecting cancel
- Go ahead and select **Remove**

# Remove an ASPA success

✓ ASPA for "AS399970" removed.

## Autonomous System Provider Authorizations (ASPAs)

Org ID ARINL has 0 ASPAs in ARIN's RPKI Repository.

Customer AS	Set of Provider ASes
None found	

- Confirmation is received that the removal was successful
- The table shows no ASPAs for the Org ID remain in the repository

# IRR Auto-Manager

# IRR Auto-Manager

## Manage IRR Auto-Manager

Set the default behavior of IRR Auto-Manager in the web interface for Org ID **ARIND-1**.

**IRR Auto-Manager:**  On - Yes, create and delete matching IRR objects by default.  
 Off - No, do not create or delete matching IRR objects by default.

**Note:** This setting does not affect the API. Review the [API User Guide](#) to use this feature in automation scripts.

**Submit**

## Create/Link Matching IRR Route Objects for Your ROAs

IRR Auto-Manager can create and/or link matching route objects for existing ROAs in batches of up to 100.

Select existing ROAs listed below to create and/or link matching route objects, then use **Create/Link Route Objects for Selected ROAs**.

Select All (2) on Page

Select	Origin AS	Prefixes	Matching IRR Route Objects?
<input type="checkbox"/>	399970	2620:10F:F001::/48	Yes
<input type="checkbox"/>	399970	2620:10F:F002::/48	No

**Create/Link Route Objects for Selected ROAs (0)**

- The IRR Auto-Manager is intended to bring the two routing security tools (IRR and RPKI) data sets into parity.
- The IRR Auto-Manager detects ROAs that do not have matching IRR objects, or IRR objects that are not linked to matching ROAs.
- Changes can be made individually selected at once
- When no mismatches exist, the table is not displayed

# RPKI API Endpoint: Reg-RWS

# Reg-RWS – RESTful API Endpoint

Feature parity with  
the ARIN Online  
web interface

Create and  
Delete actions  
made  
simultaneously

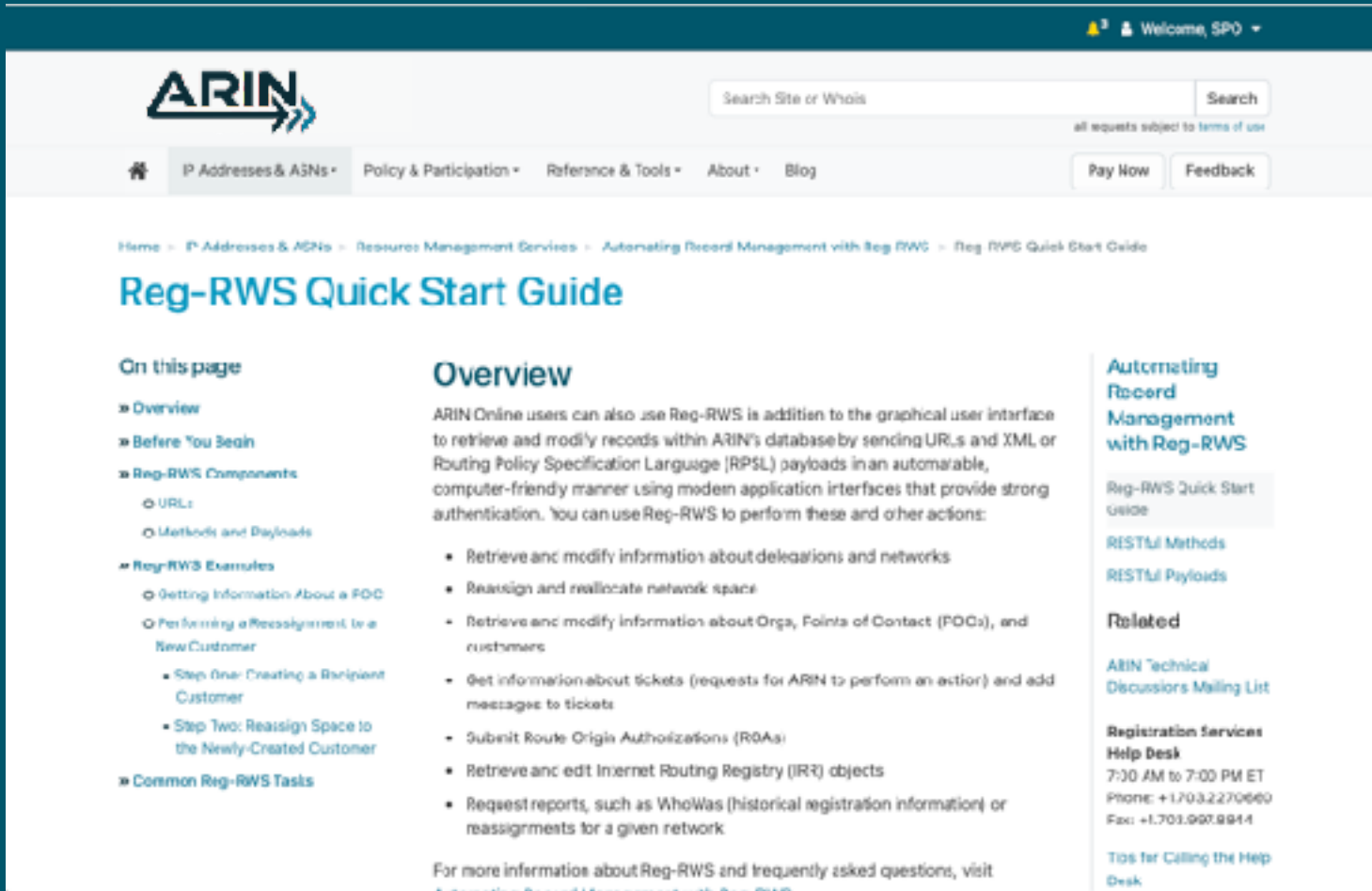
Able to make  
bulk atomic  
changes in one  
API call

Successfully  
tested making  
>1k changes in a  
single call

## Do I Need to Use the API?

- No one *needs* to the use Reg-RWS API
- Making bulk changes in the ARIN Online web interface is inefficient and time consuming
- The Reg-RWS API enables resource holders the opportunity to script RPKI updates
- No programming experience is necessary

# Reg-RWS Quick Start Guide



The screenshot shows the ARIN website interface. At the top, there is a navigation bar with the ARIN logo on the left, a search box labeled "Search Site or Whois" in the center, and a user greeting "Welcome, SPO" on the right. Below the navigation bar, there are several menu items: "IP Addresses & ASNs", "Policy & Participation", "Reference & Tools", "About", and "Blog". There are also buttons for "Pay Now" and "Feedback".

The main content area features a breadcrumb trail: "Home > IP Addresses & ASNs > Resource Management Services > Automating Record Management with Reg-RWS > Reg-RWS Quick Start Guide". The title "Reg-RWS Quick Start Guide" is prominently displayed in blue.

On the left side, there is a "On this page" section with a list of links: "Overview", "Before You Begin", "Reg-RWS Components" (with sub-links for "URLs" and "Methods and Payloads"), "Reg-RWS Examples" (with sub-links for "Getting Information About a POC", "Performing a Reassignment to a New Customer", "Step One: Creating a Recipient Customer", and "Step Two: Reassign Space to the Newly-Created Customer"), and "Common Reg-RWS Tasks".

The main content area has an "Overview" section. It states: "ARIN Online users can also use Reg-RWS in addition to the graphical user interface to retrieve and modify records within ARIN's database by sending URLs and XML or Routing Policy Specification Language (RPSL) payloads in an automatable, computer-friendly manner using modern application interfaces that provide strong authentication. You can use Reg-RWS to perform these and other actions:"

- Retrieve and modify information about delegations and networks
- Reassign and reallocate network space
- Retrieve and modify information about Orgs, Points of Contact (POCs), and customers
- Get information about tickets (requests for ARIN to perform an action) and add messages to tickets
- Submit Route Origin Authorizations (ROAs)
- Retrieve and edit Internet Routing Registry (IRR) objects
- Request reports, such as WhoWas (historical registration information) or reassignments for a given network

At the bottom of the overview section, it says: "For more information about Reg-RWS and frequently asked questions, visit Automating Record Management with Reg-RWS".

On the right side, there is a "Automating Record Management with Reg-RWS" section. It includes a link for "Reg-RWS Quick Start Guide" (which is highlighted), "RESTful Methods", and "RESTful Payloads". Below this is a "Related" section with a link for "ARIN Technical Discussions Mailing List". At the bottom right, there is a "Registration Services Help Desk" section with contact information: "7:00 AM to 7:00 PM ET", "Phone: +1.703.227.0660", "Fax: +1.703.007.8914", and a link for "Tips for Calling the Help Desk".

- <https://www.arin.net/resources/manage/regrws/quickstart/>
- <https://www.arin.net/resources/manage/regrws/methods/>

# What Did Your RPKI Changes Do?

# Links to a few helpful and free RPKI tools

- RPKI ROA Planner - <https://roa-planner.internet2.edu/>
- NIST RPKI Monitor - <https://rpki-monitor.antd.nist.gov/ROV>
- Hurricane Electric Super Looking Glass - <https://bgp.he.net/super-lg/>
- IRR Explorer - <https://irrexplorer.nlnog.net/>
- Routinator web UI - <https://rpki-validator.ripe.net/ui/>
- Cloudflare RPKI portal - <https://rpki.cloudflare.com/?view=validator>
- RPKI ASPA Planner - <https://rootbeer.testing.ns.internet2.edu/aspa>
- PacketVis BGP/RPKI Monitoring - <https://packetvis.com/>
- rpki-client console - <https://console.rpki-client.org/>



# Yes, documentation is a tool too!

- **RPKI documentation** - <https://rpki.readthedocs.io/en/latest/index.html>
- **RPKI deployment hub** - <https://rpkihub.au/>
- **IETF SIDROPS** - <https://datatracker.ietf.org/group/sidrops/documents/>
- **RPKI Community Discord board (invite)** - <https://discord.gg/nGvKa3Yc>
- **ARIN RPKI FAQ** - <https://www.arin.net/resources/manage/rpki/faq/>
- **ARIN Suggestions** - <https://www.arin.net/participate/community/acsp/>
- **BGP Filter Guide** - [https://bgpfilterguide.nlnog.net/guides/reject\\_invalids/](https://bgpfilterguide.nlnog.net/guides/reject_invalids/)

**DON'T FORGET:**  
**Take home**  
**your workbook!**



**ARIN RPKI** | A step-by-step guide to using RPKI with ARIN

**Why is RPKI important?**

- Making statements about your resources benefits you, your network, and other users by providing a clear and consistent view of your resources.
- Resources are not shared unless you have a valid RPKI signature for them.
- A growing number of Internet Service Providers (ISPs) require you to provide RPKI for your resources, which is required for routing your traffic.
- There are many tools to help you with RPKI, including our tools and our courses for RPKI.

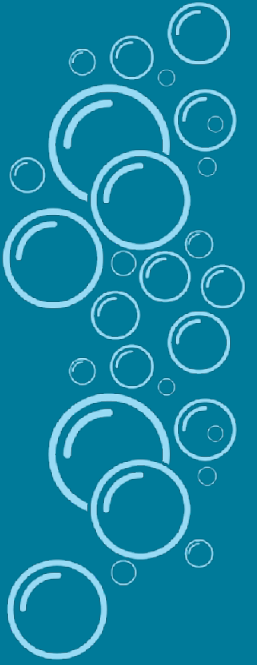
**Download our free Evaluation Workbook**  
A step-by-step guide to using RPKI with ARIN.

**OTER**  
It is important to be alert for and aware of the operational and security risks of RPKI. Always use the latest and best practices for RPKI. It is important to be aware of the risks of RPKI, ARIN, and our tools.

A copy of your screen dashboard and resources list is available for taking screenshots.

Learn more about OTER in the ARIN RPKI course.

# Thank You



Customer Technical Services  
Team

[routing.security@arin.net](mailto:routing.security@arin.net)