RPKI Workshop

Starting ~8:45

ARIN Deep Dive

Using ARIN's Hosted RPKI Services

CHI NOG 13

27 May 2026

ARIN Deep Dive

Brad Gorman

Director of Customer Technical Services

Our Exploration Plan

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

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 3rd 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 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

ARIN Deep Dive

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

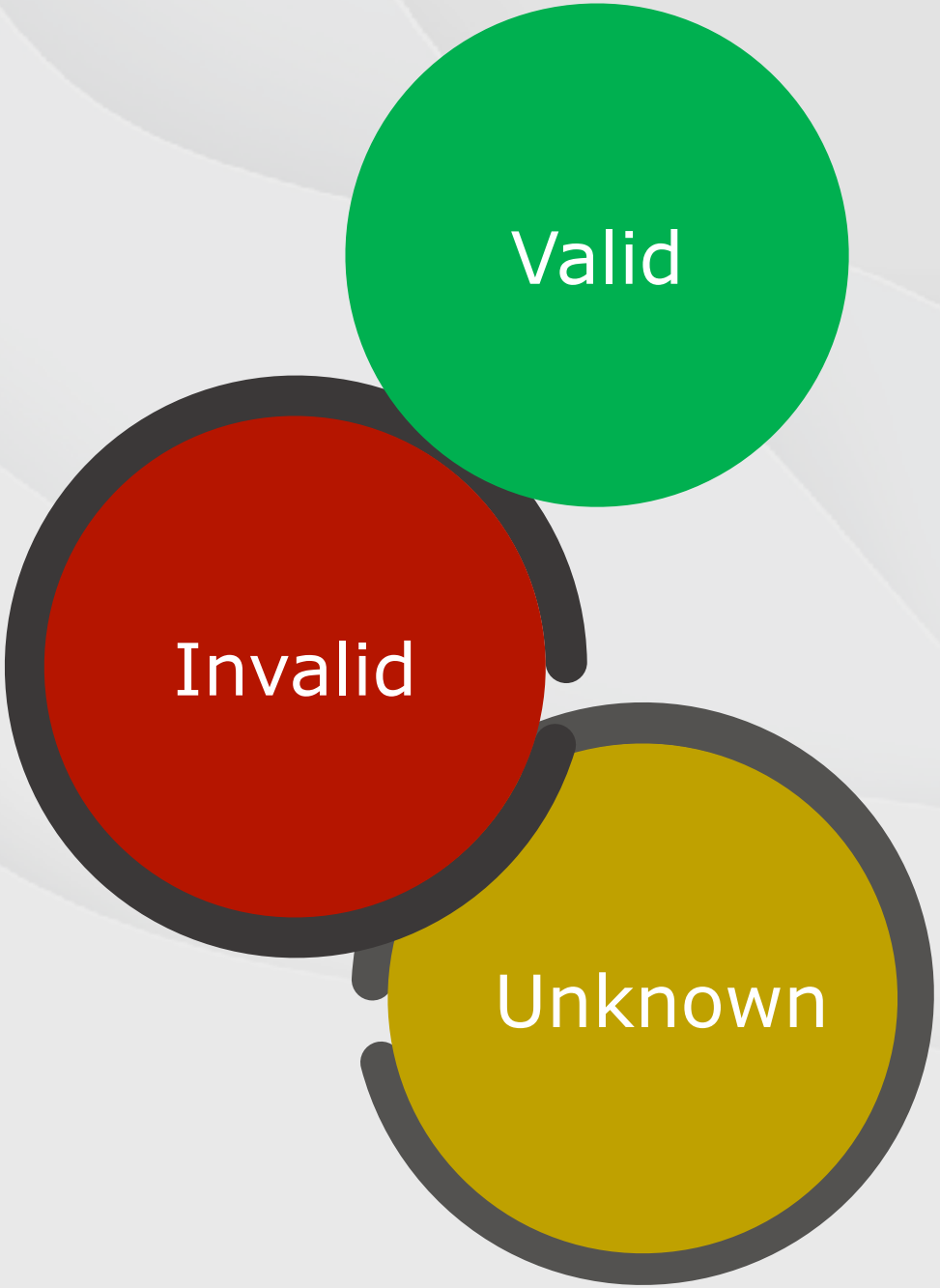
- The Origin AS in a ROA does not need to be allocated to you, only the IP prefixes.
- Bring Your Own IP (BYOIP) service providers source your IP prefix from their network. The Origin AS will be theirs — not yours — and the ROA must reflect that.
- A DDoS service provider will announce your IP prefix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

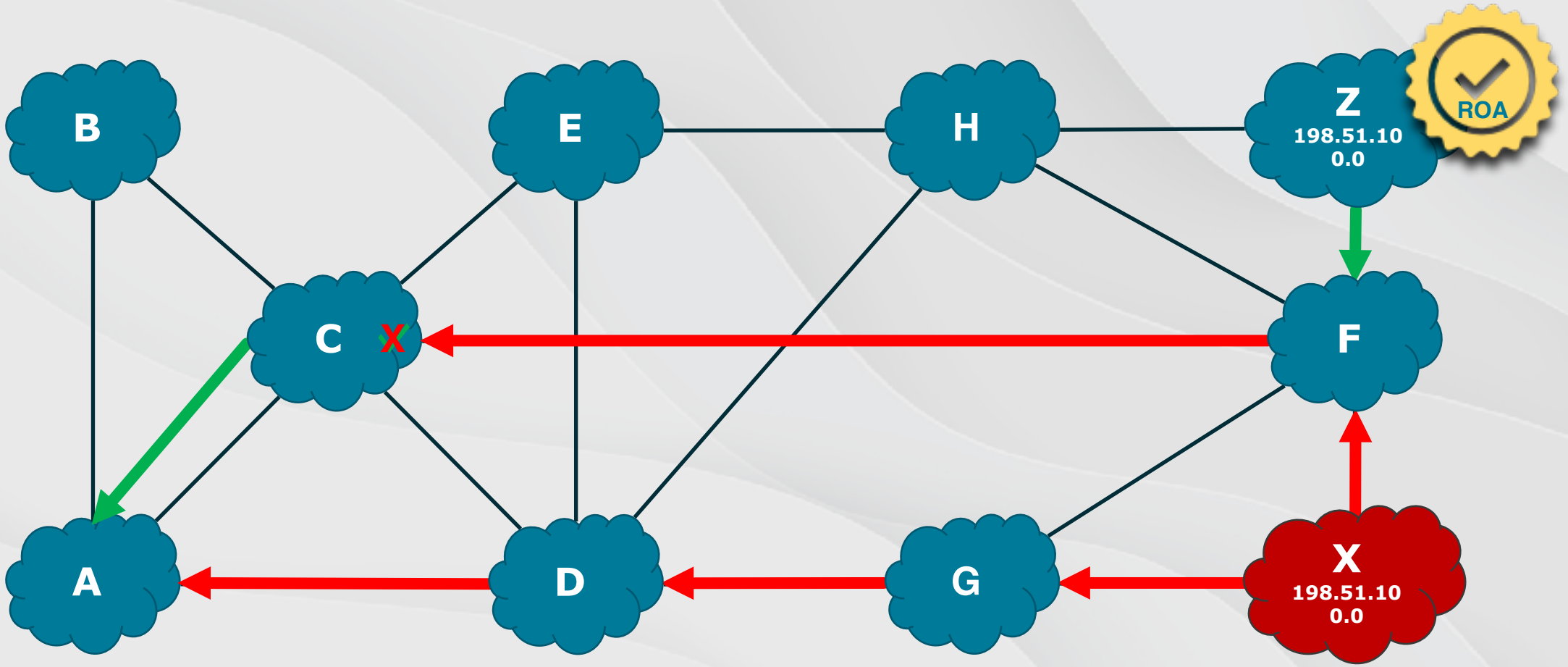
Validation

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

Action

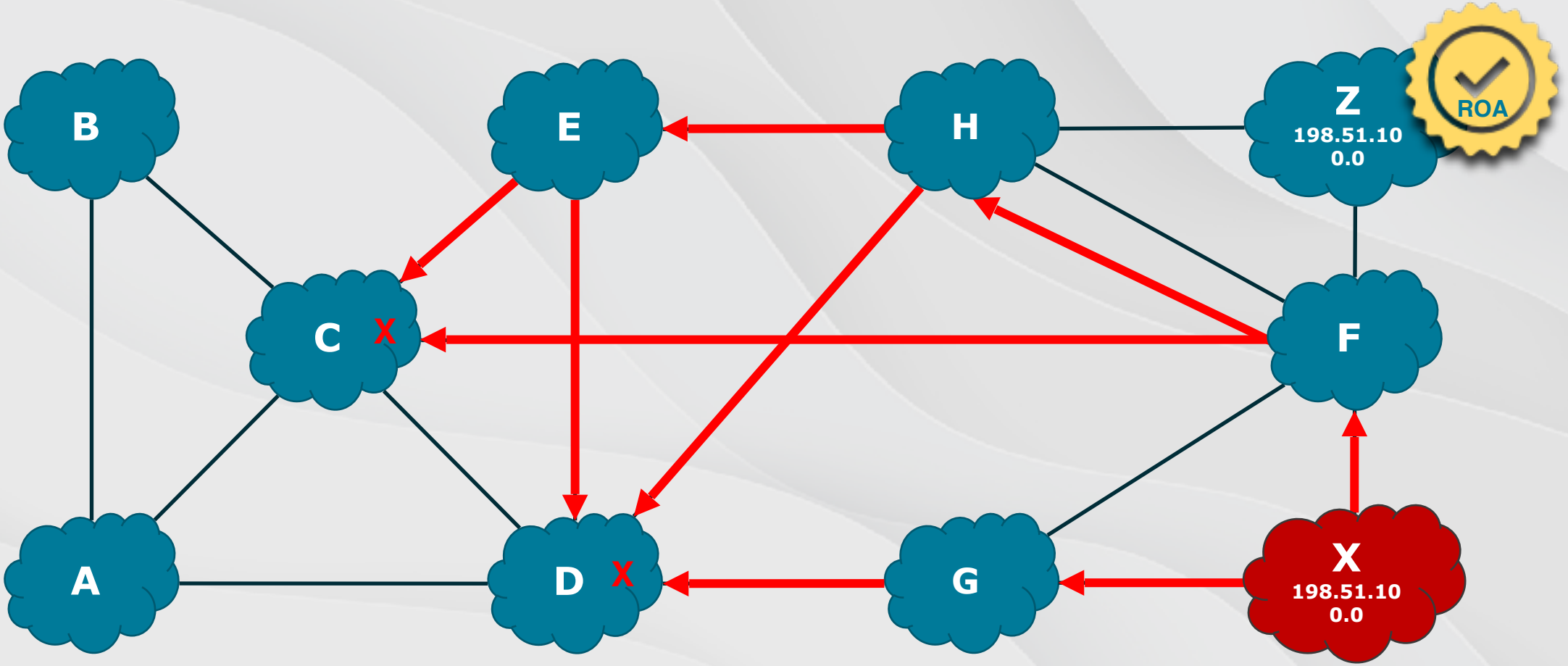
Network operators perform **ROV**, enhancing global routing security

Route Origin Validation in Action

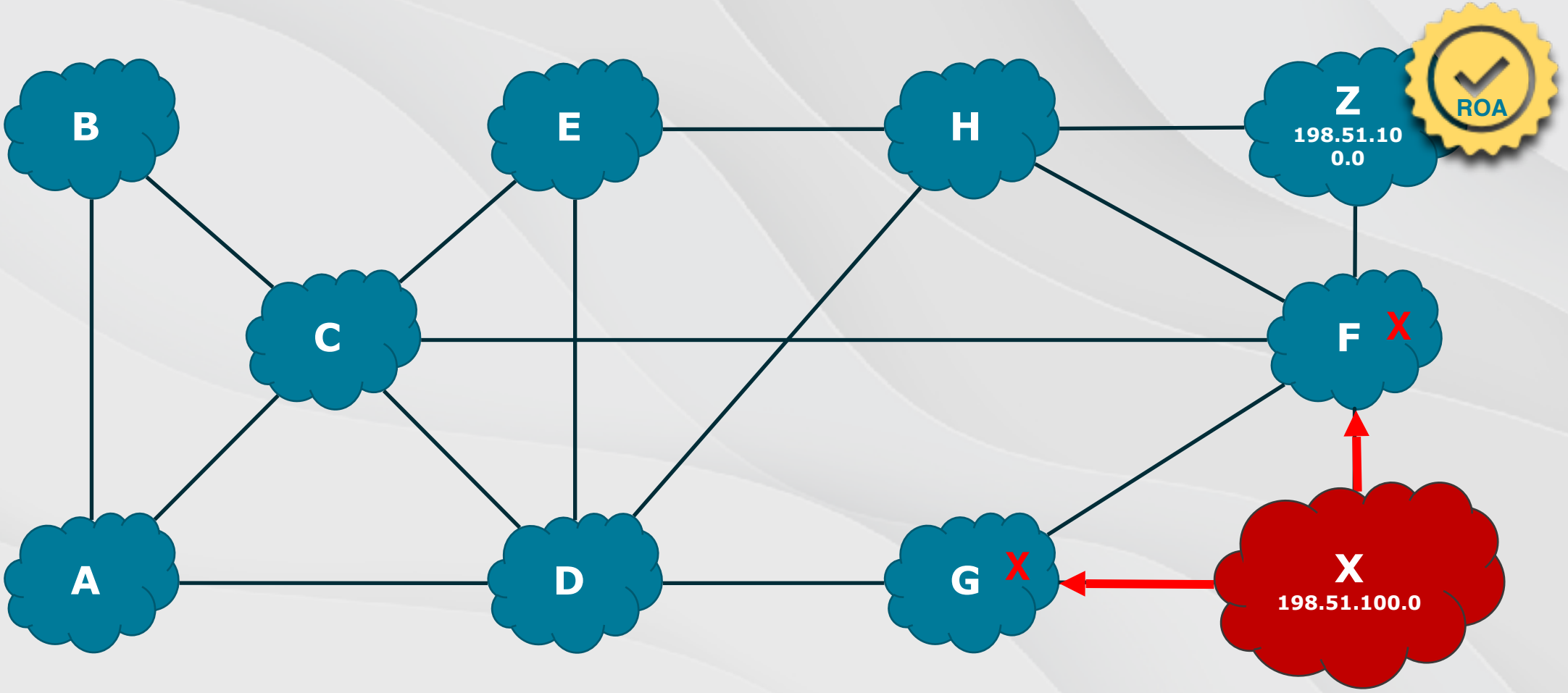


AS Z: 198.51.100.0/24
AS X: 198.51.100.0/24

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.

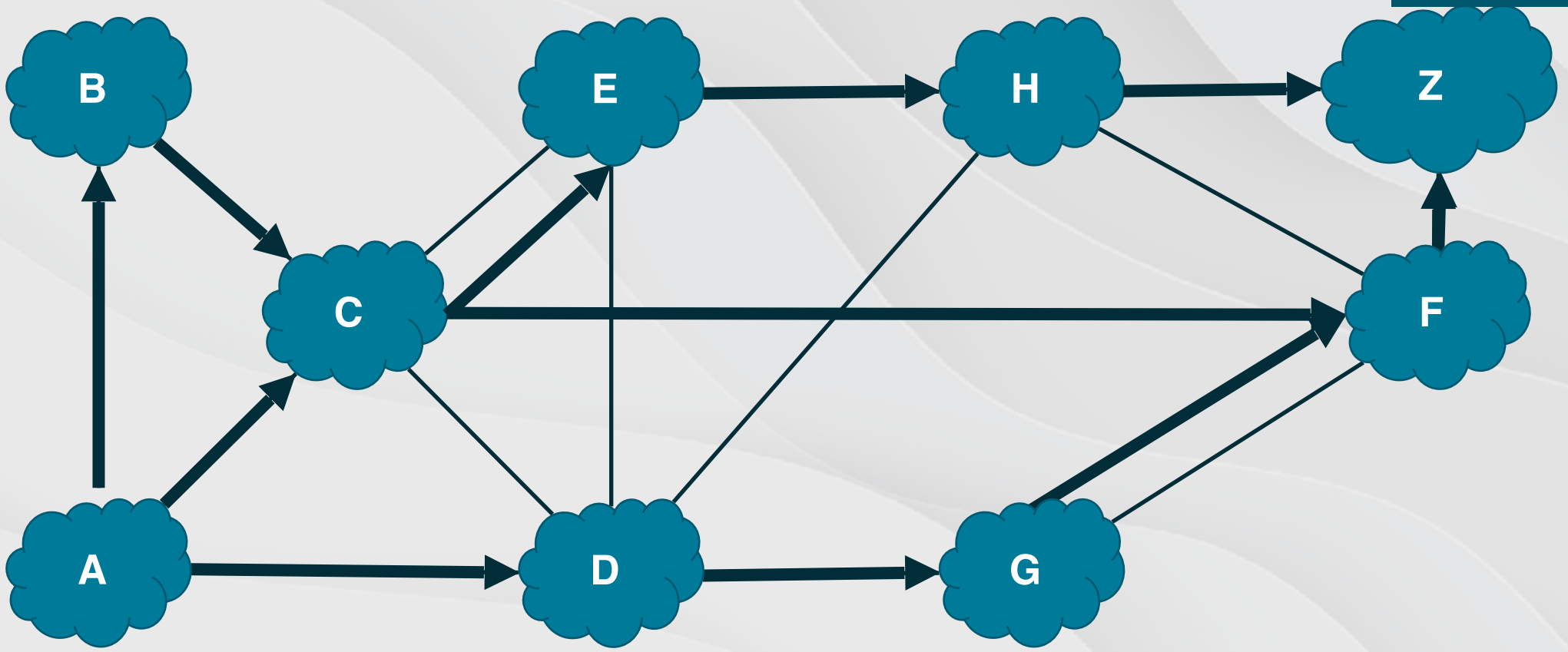
The AS0 ASPA

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.

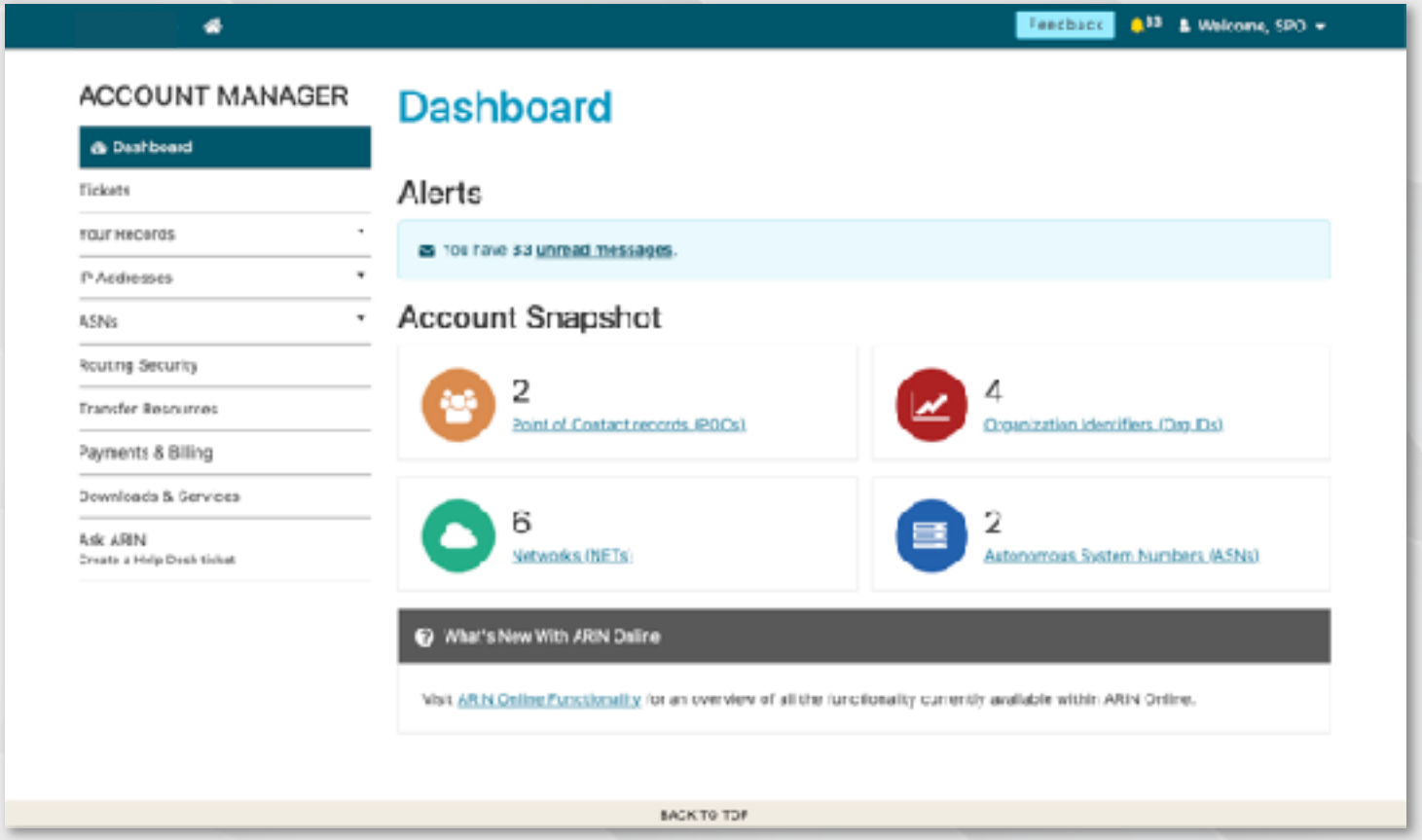
Delegated RPKI
Suggested for organizations that want/ need cryptographic control of RPKI certificates; the organization should have a deeper understanding of RPKI, routing security, and a technical staff to maintain and publish the high availability repository.

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

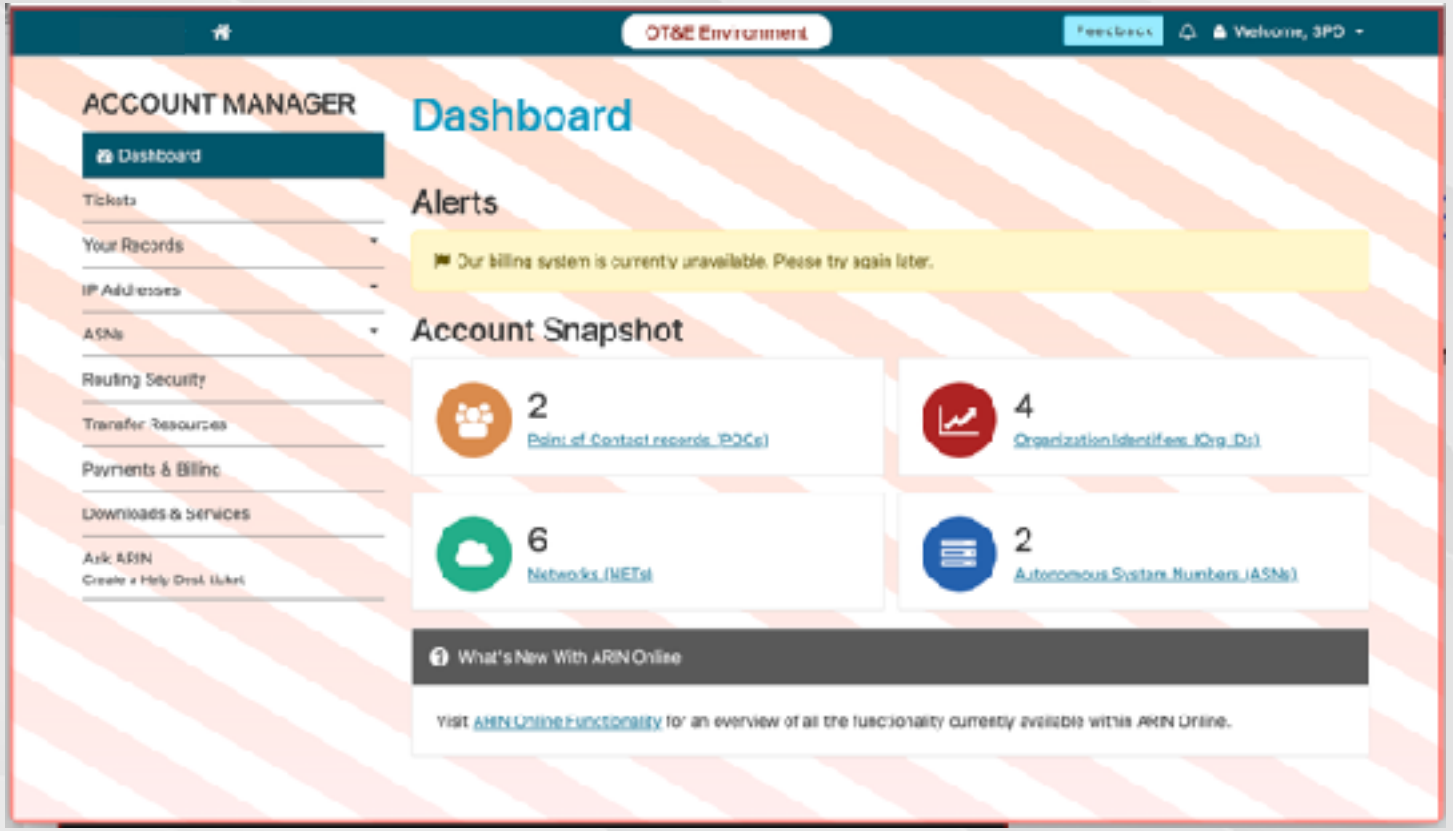


Log in at https://account.arin.net

Two RPKI Environments

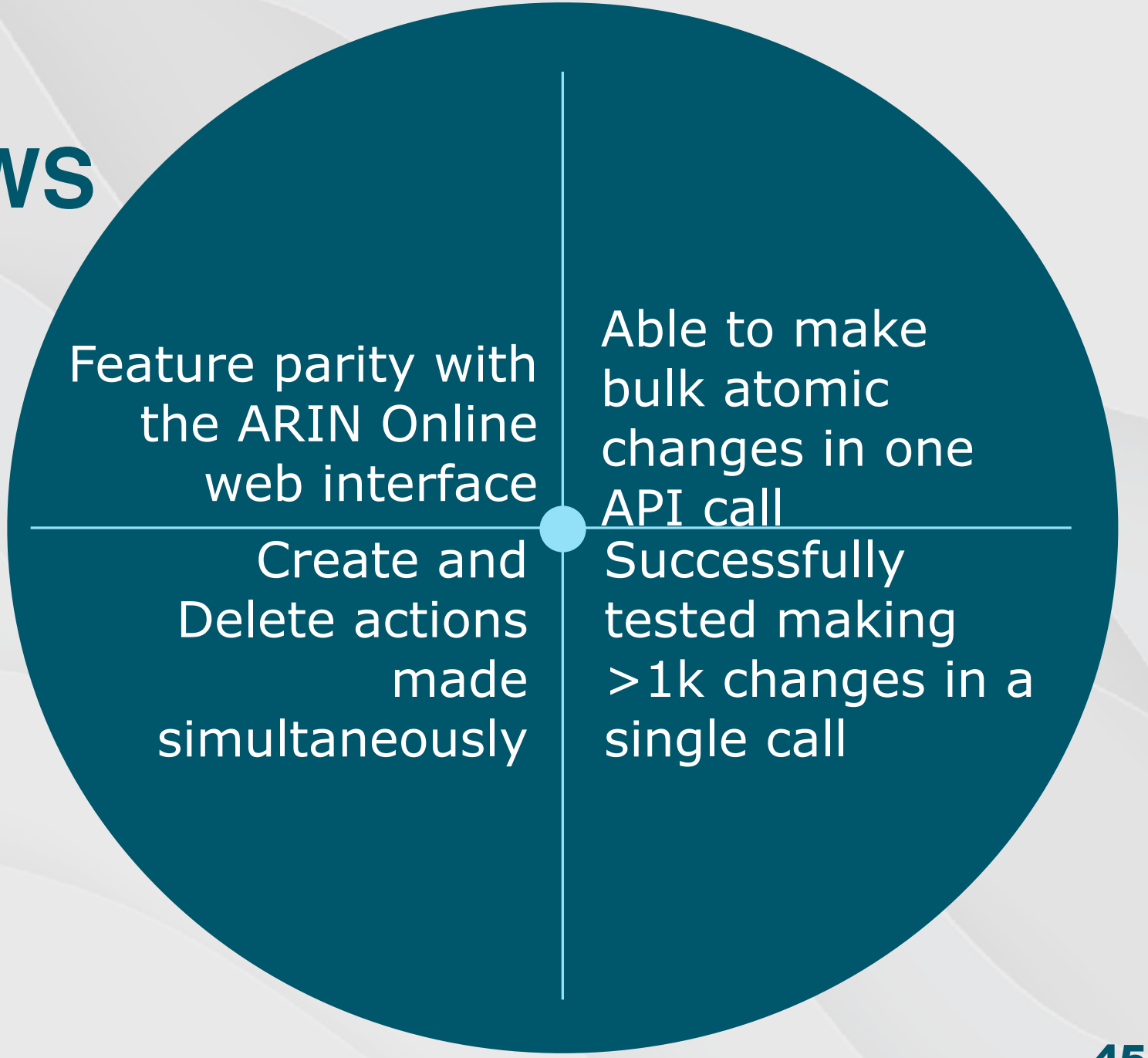
Operational Test and Evaluation (OT&E)

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

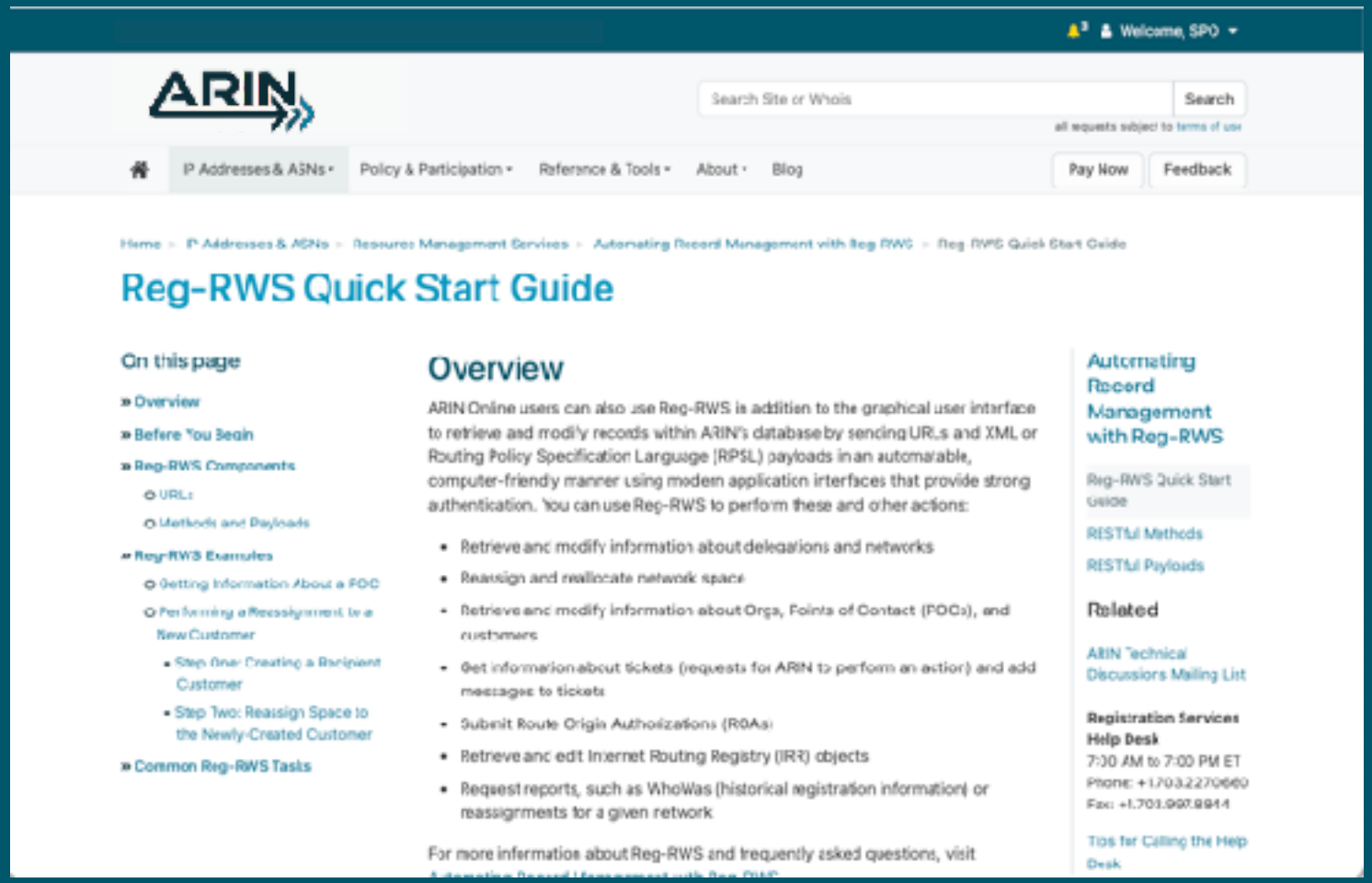


Log in at https://account.ote.arin.net

One RESTful API Endpoint — RegRWS



Reg-RWS Quick Start Guide



- 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

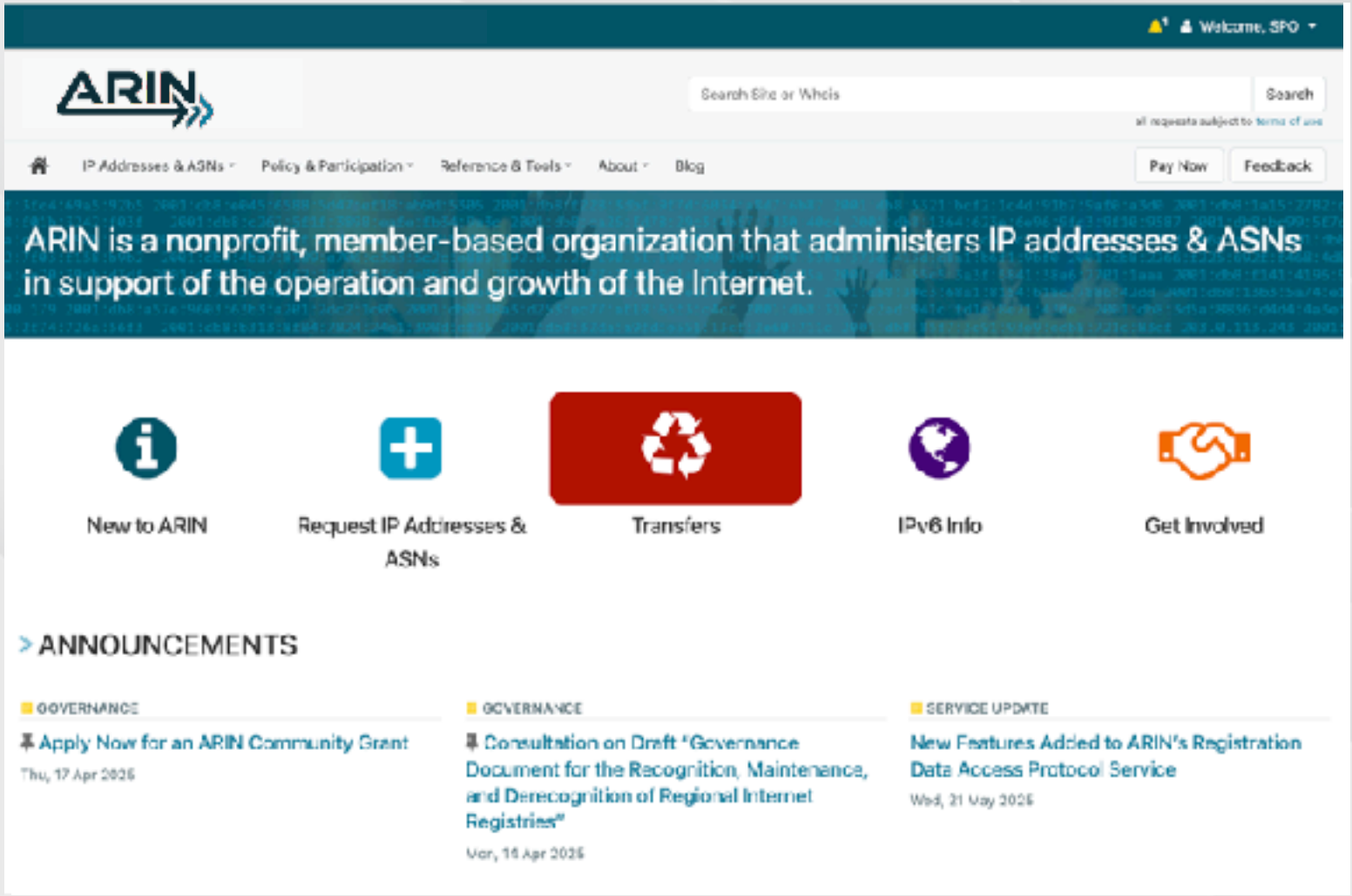
IPv4 or IPv6 number resources directly allocated to your organization by ARIN

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



- 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).

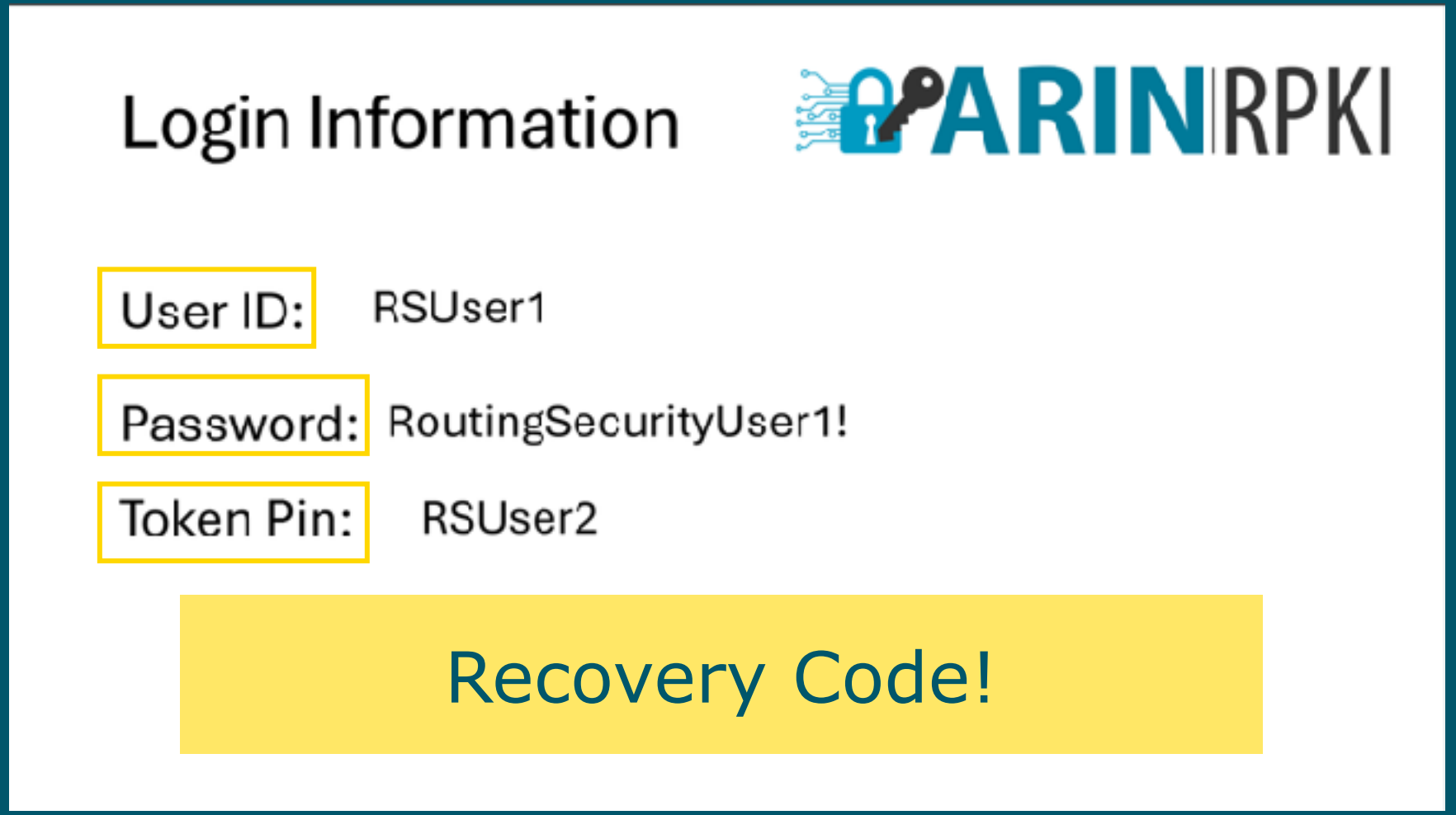
Let’s take a break

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

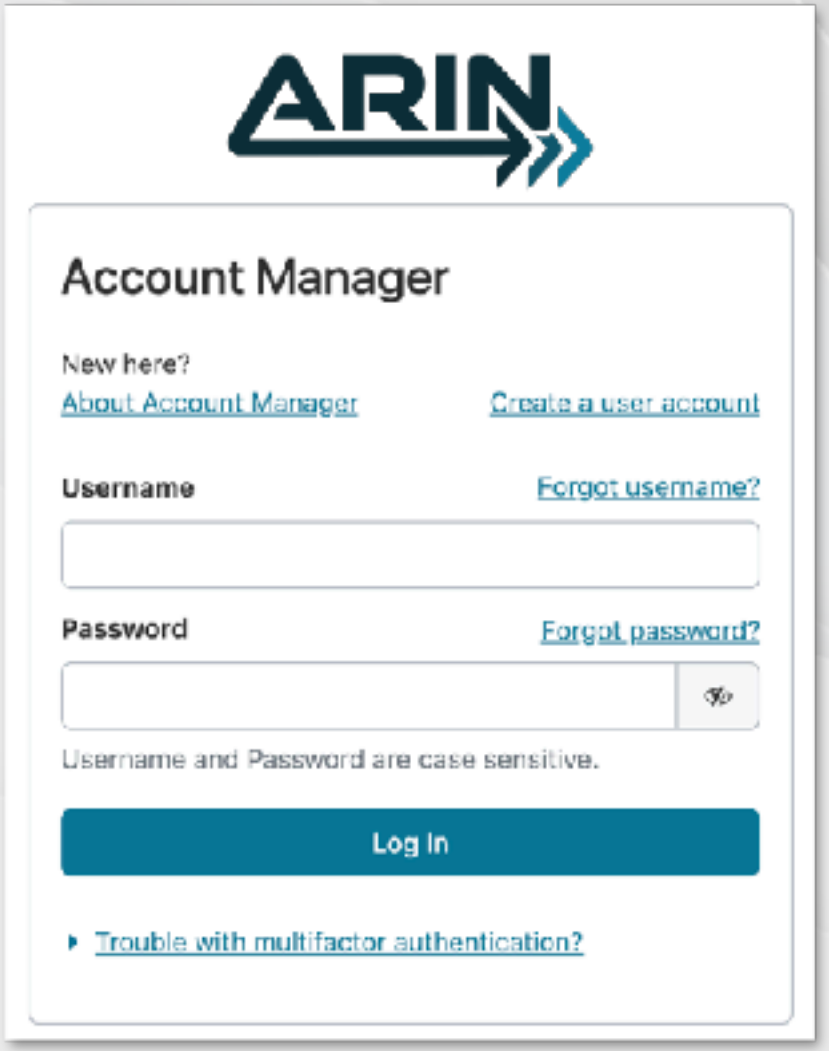



ARIN Deep Dive
Getting Started with Hosted RPKI


ARIN Deep Dive
Let's Begin

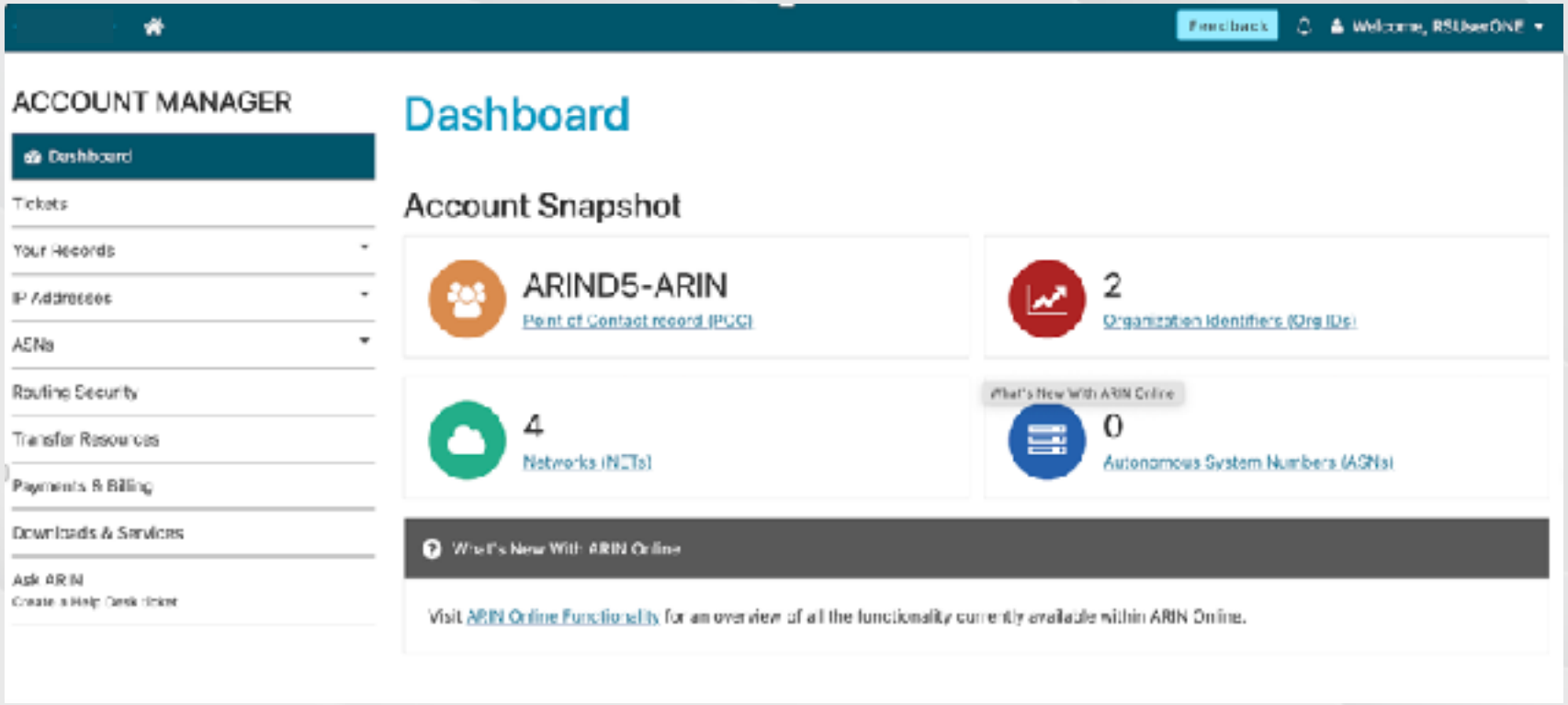
ARIN Online User Interface

Accessing ARIN Online



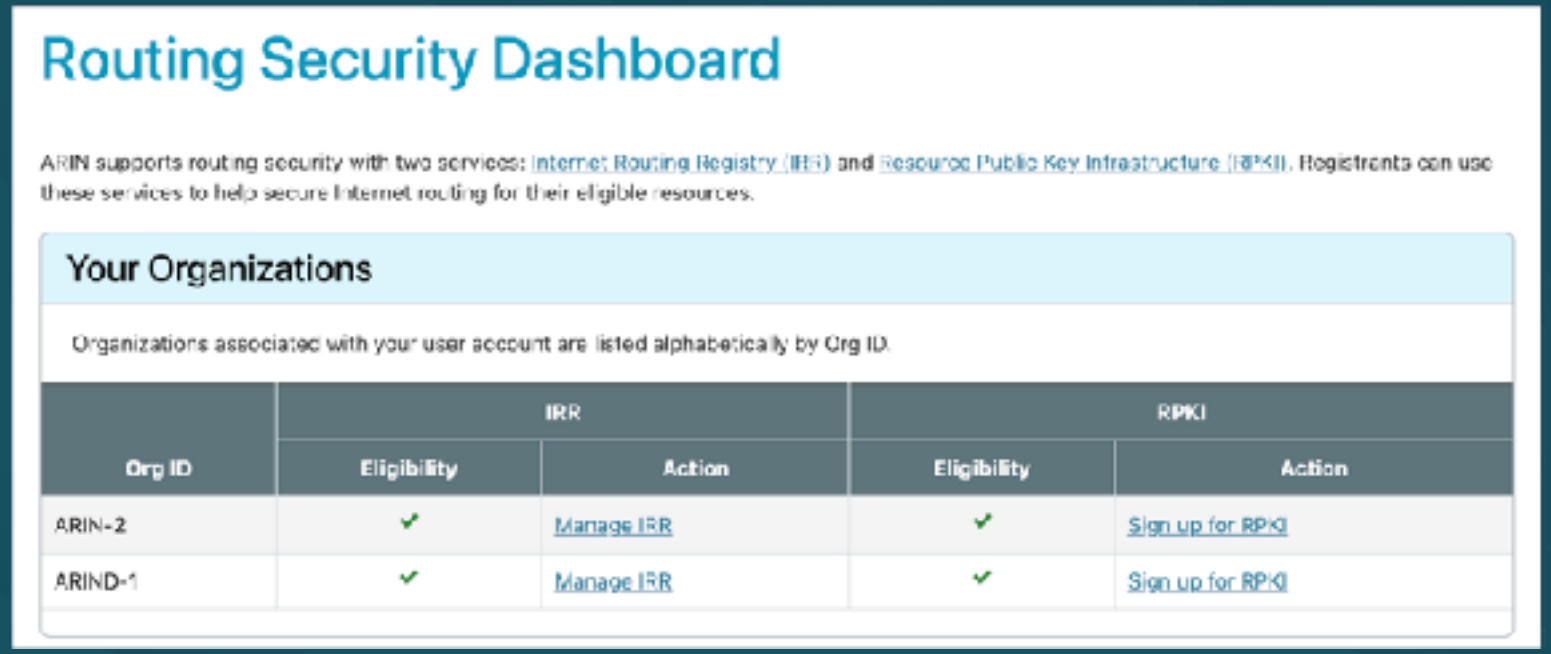
- If you are a first-time customer of ARIN, select **Create a user account**.
- Instructional videos that explain how to complete the steps above can be found at arin.net/howtovideos
- If you already have a user account, enter your credentials and select **Log In** to continue
- https://account.arin.net

ARIN Online User Dashboard



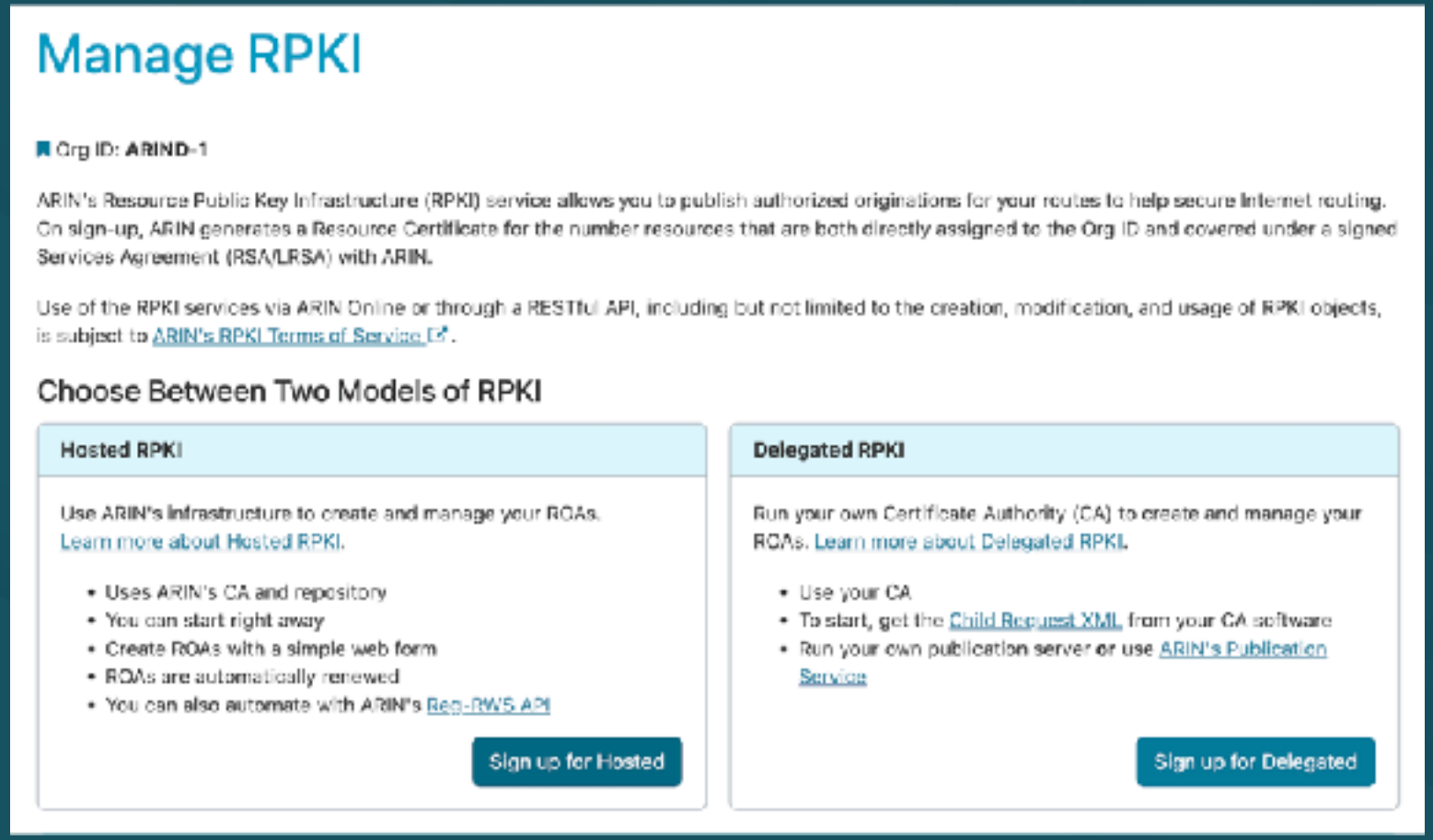
- Once logged in, a user can see information related to all linked organizations.
- Functionality and access is based on the Point of Contact the user is linked to.
- To make RPKI decisions, the user must be the Admin, Tech, or Routing Point of Contact.
- Select Routing Security in the left navigation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

Routing Security Dashboard



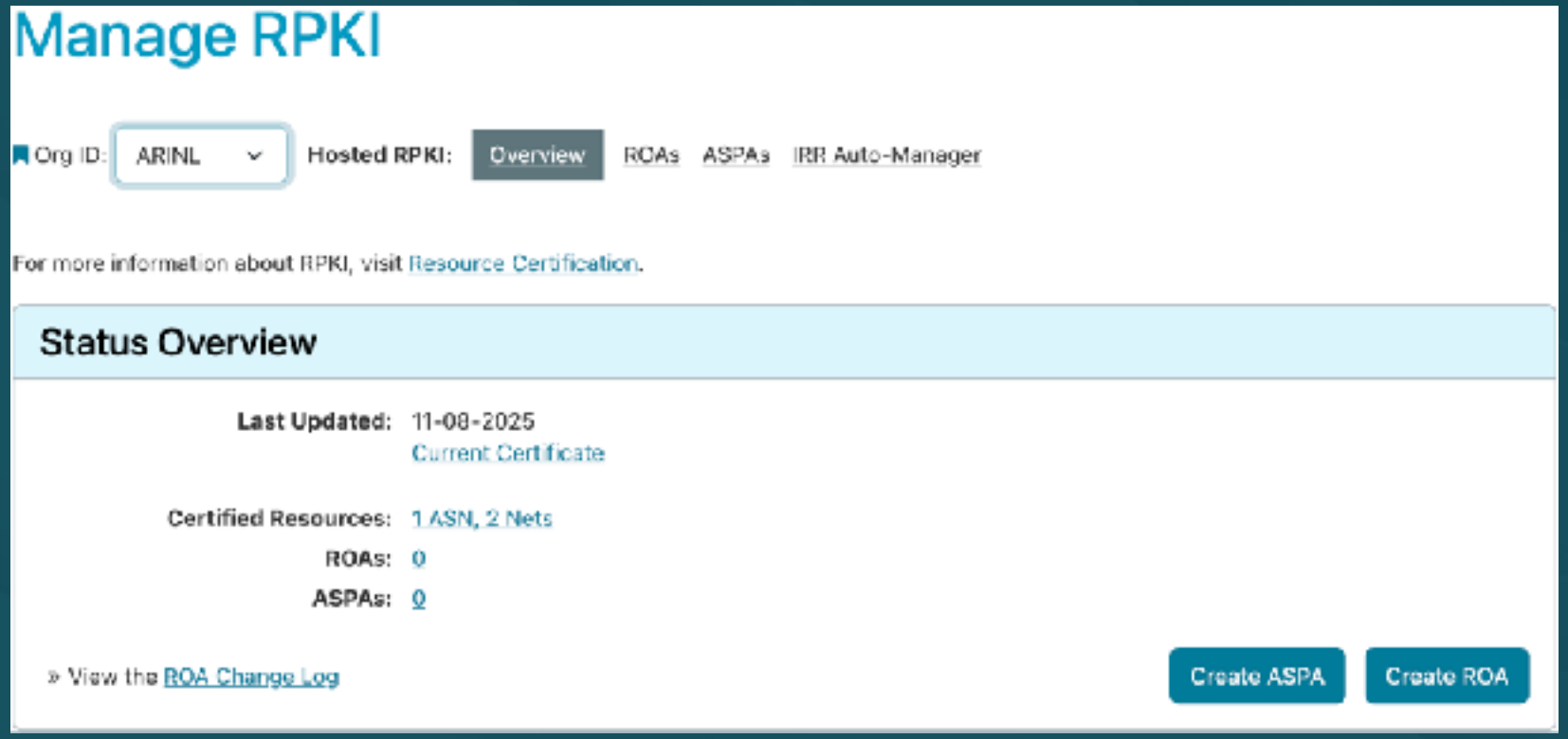
- Search for your organization on the Routing Security dashboard
- Select **Sign up for RPKI**

Manage RPKI – Selection Sign Up



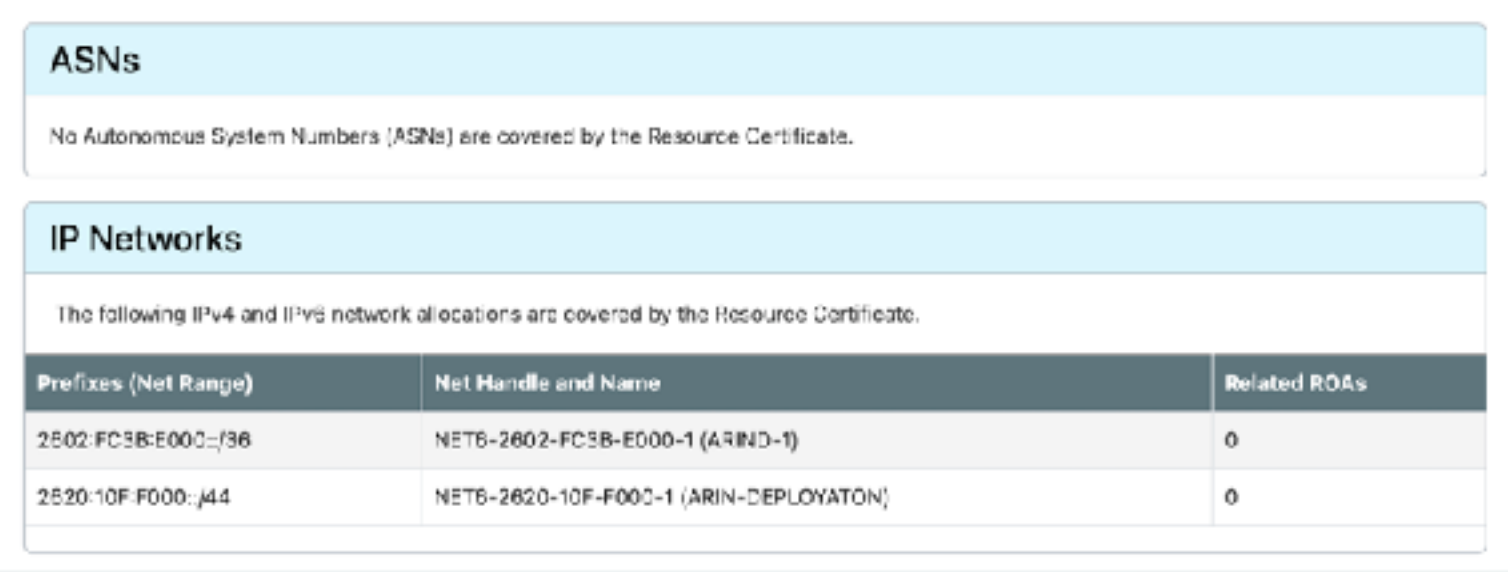
- The first time you reach the Manage RPKI page, you must pick your deployment type: **Hosted** or **Delegated**
- Hosted customers have access to RPKI tools developed by ARIN
- Delegated customers have more control of the cryptographic element, but are responsible for operating a Certificate Authority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

Manage RPKI – Status Overview



- The 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.

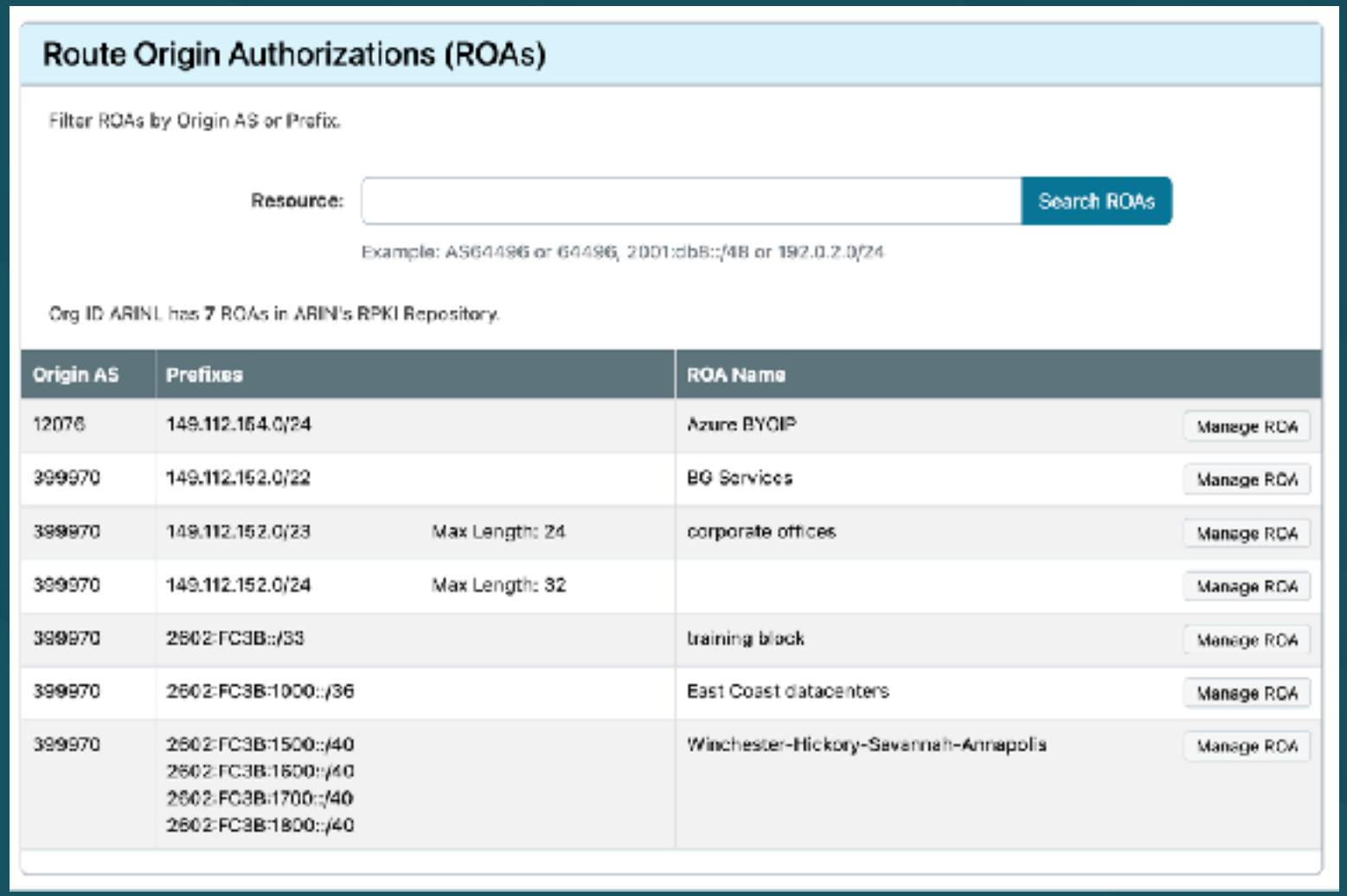
IP Networks

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

Prefixes (Net Range)	Net Handle and Name	Related ROAs
2602:FC3B:E000::/36	NET6-2602-FC3B-E000-1 (ARIN-1)	0
2620:10F:F000::/44	NET6-2620-10F-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.

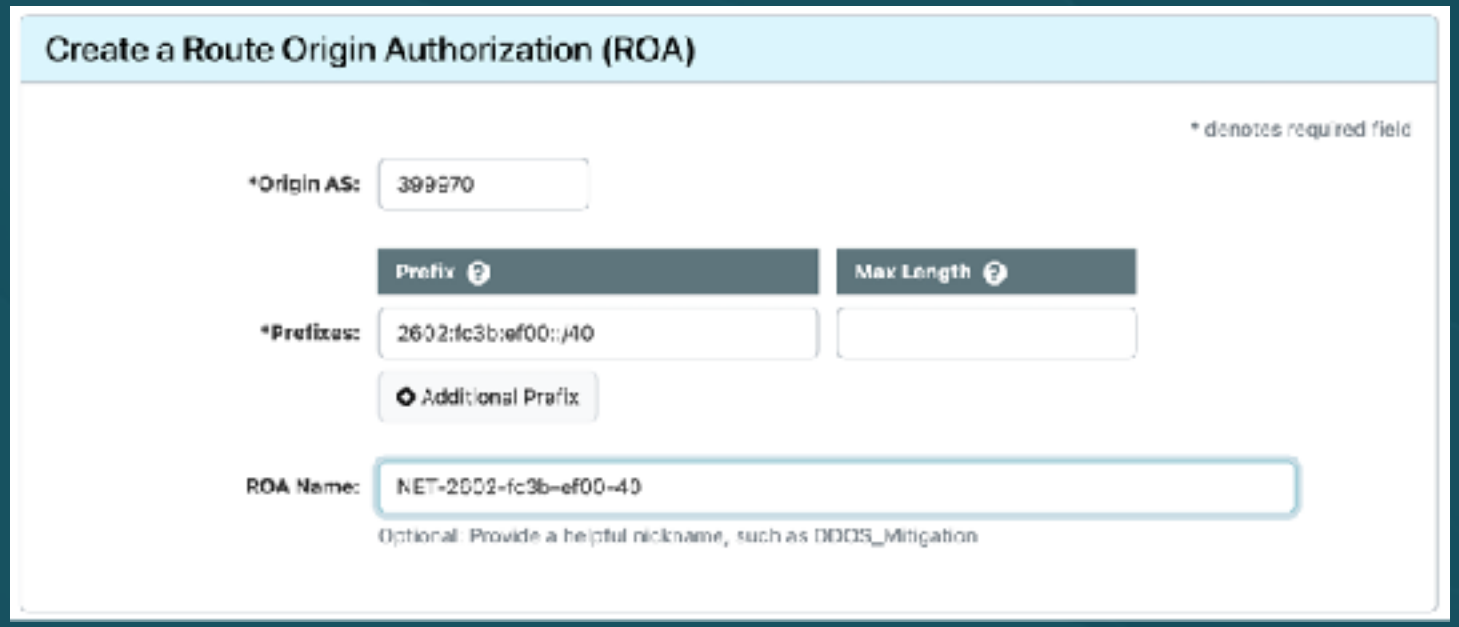
RPKI – ROA Table



- 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

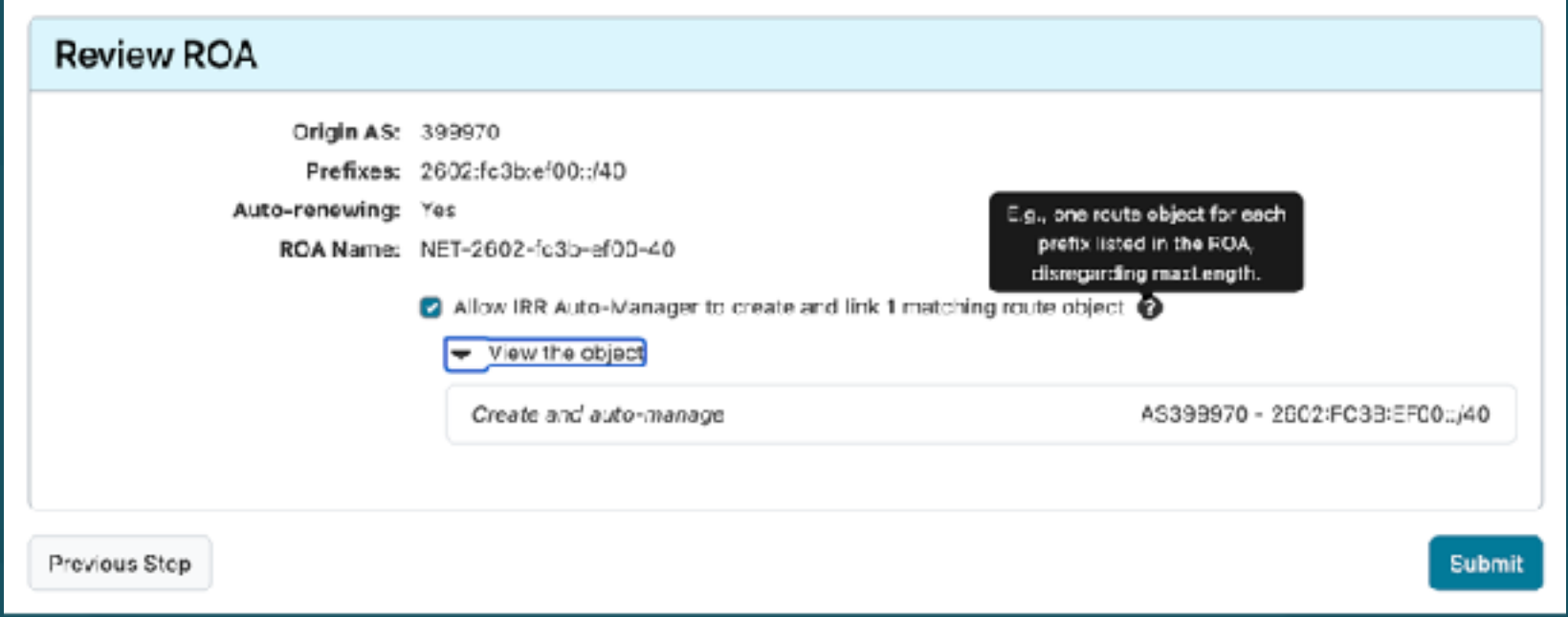
Creating ROAs

ROA Entry Form



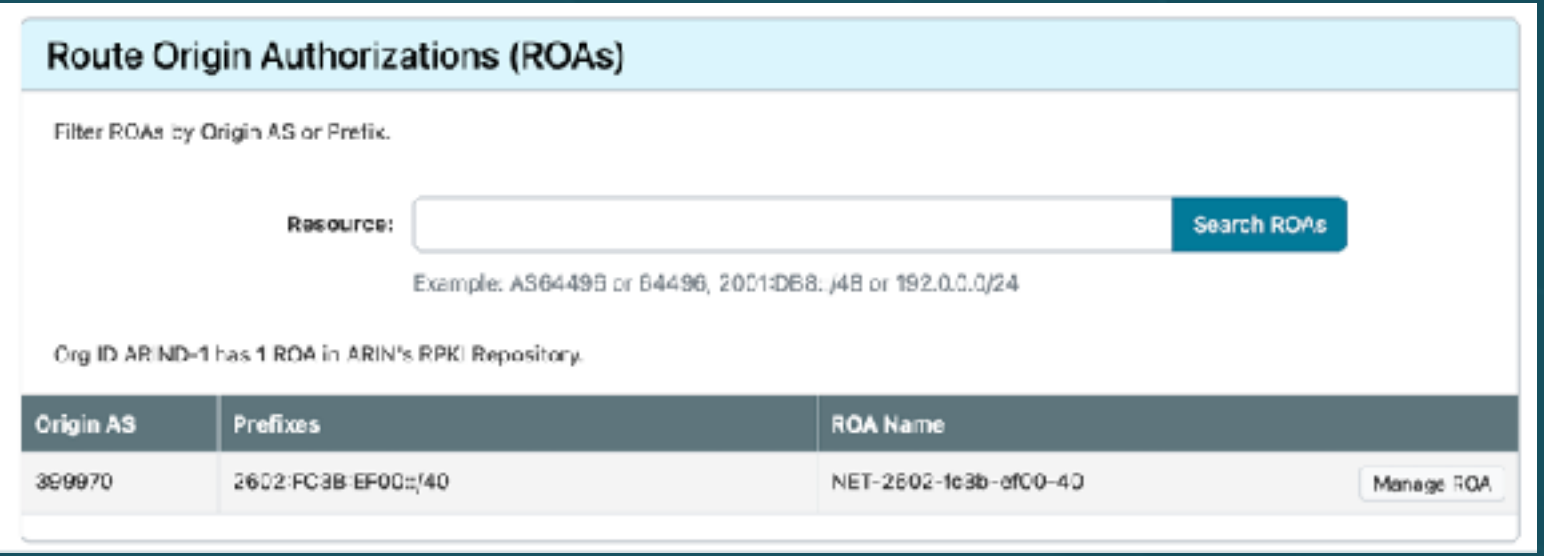
- The ROA create form has two mandatory fields: Origin AS and Prefixes
- There are two optional fields: Max Length and ROA Name
- Select the **Create ROA** button above the table to access the ROA Create form

Create ROA Review



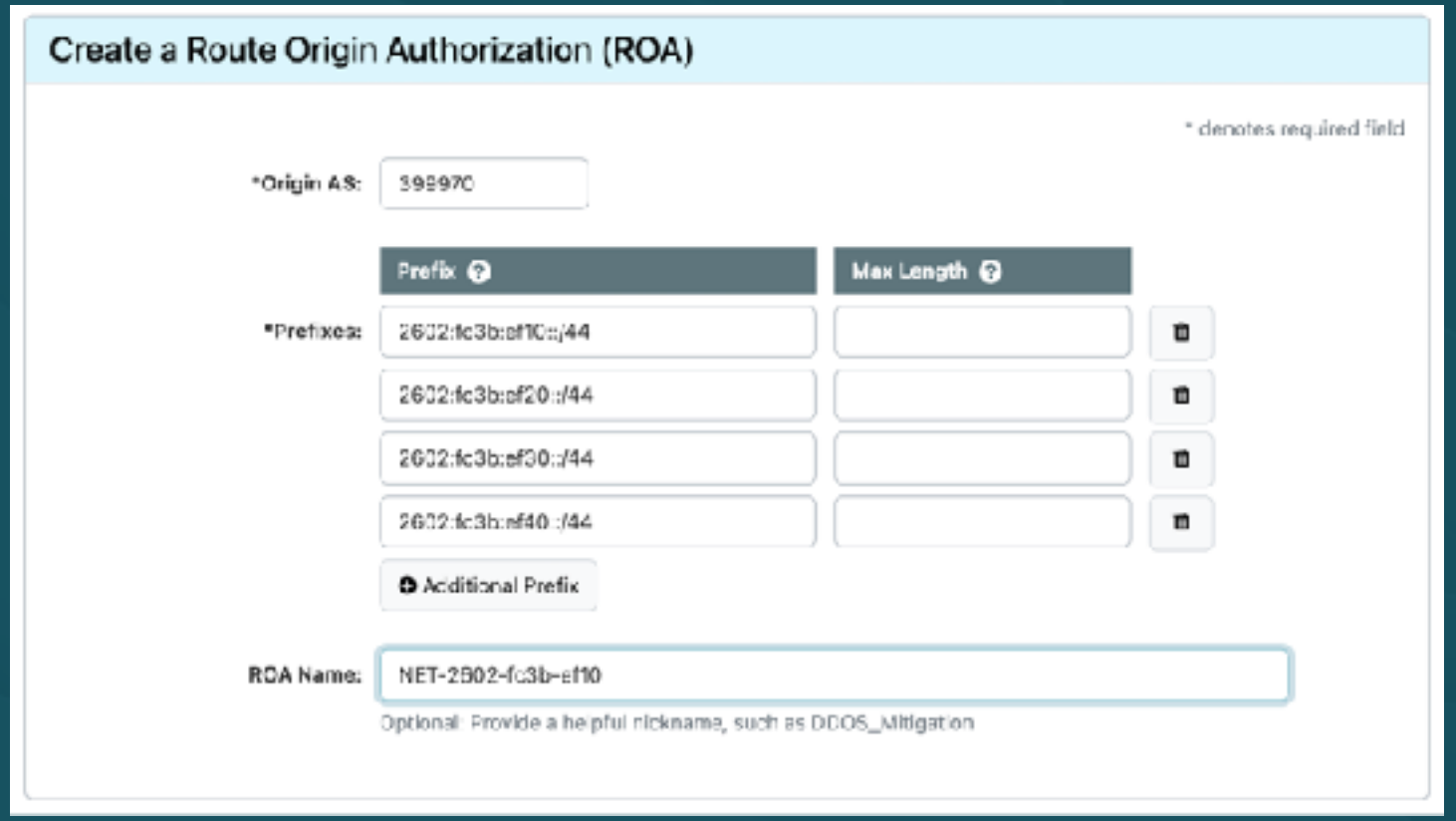
- All ROAs created using ARIN Online (or the Reg-RWS RESTful endpoint) auto-renew every 90 days.
- The IRR Auto-Manager creates an IRR route object that matches each Origin AS and prefix in the ROA.
- If you are happy with the data you entered, select **Submit**.
- Select **Previous Step** to make changes.

Create ROA Success



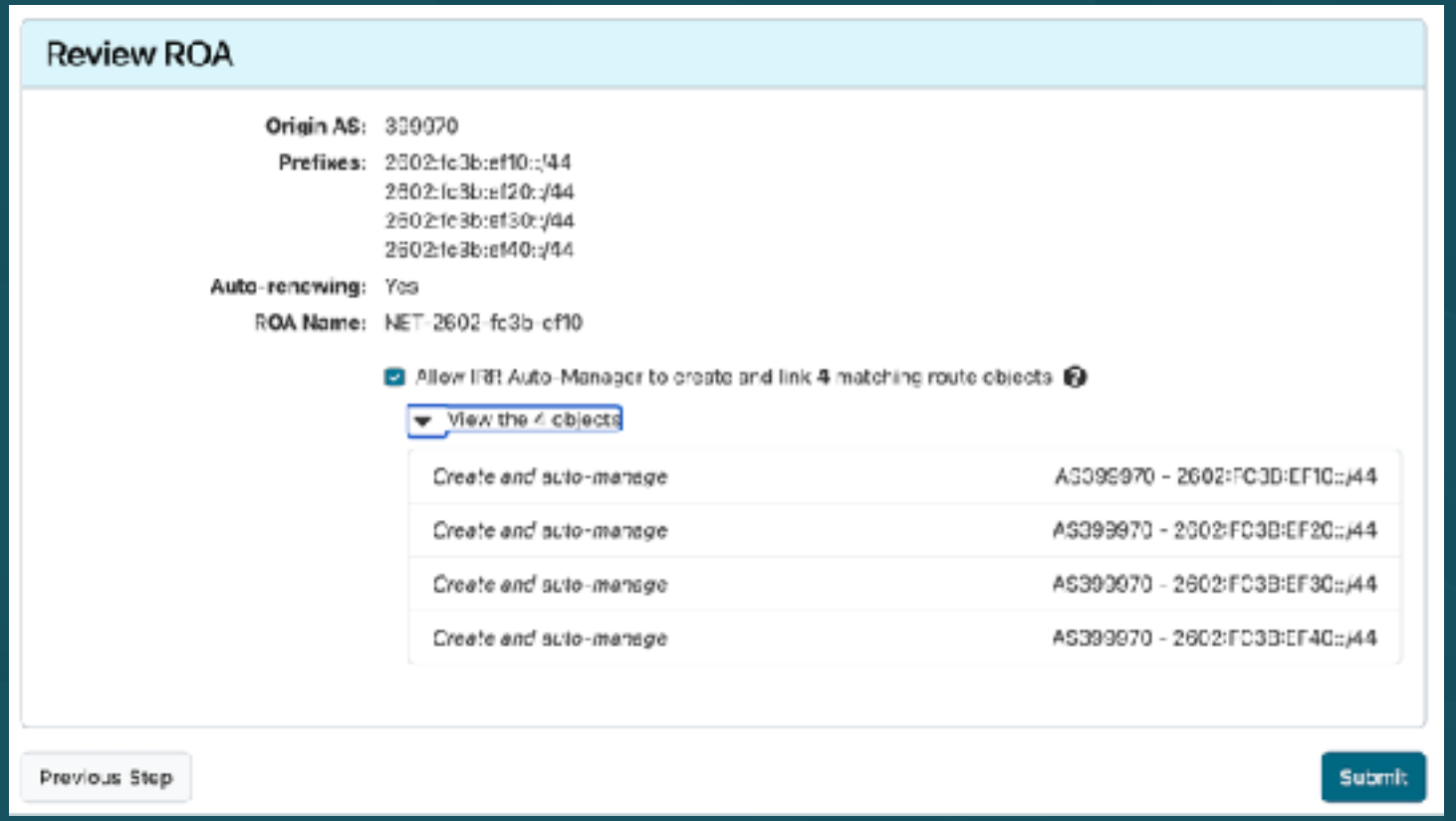
- The table now shows the newly created ROA
- You will also see a green success banner displayed above the table
- Select the **Create ROA** to continue covering your number resources

Create Multi-Prefix ROA



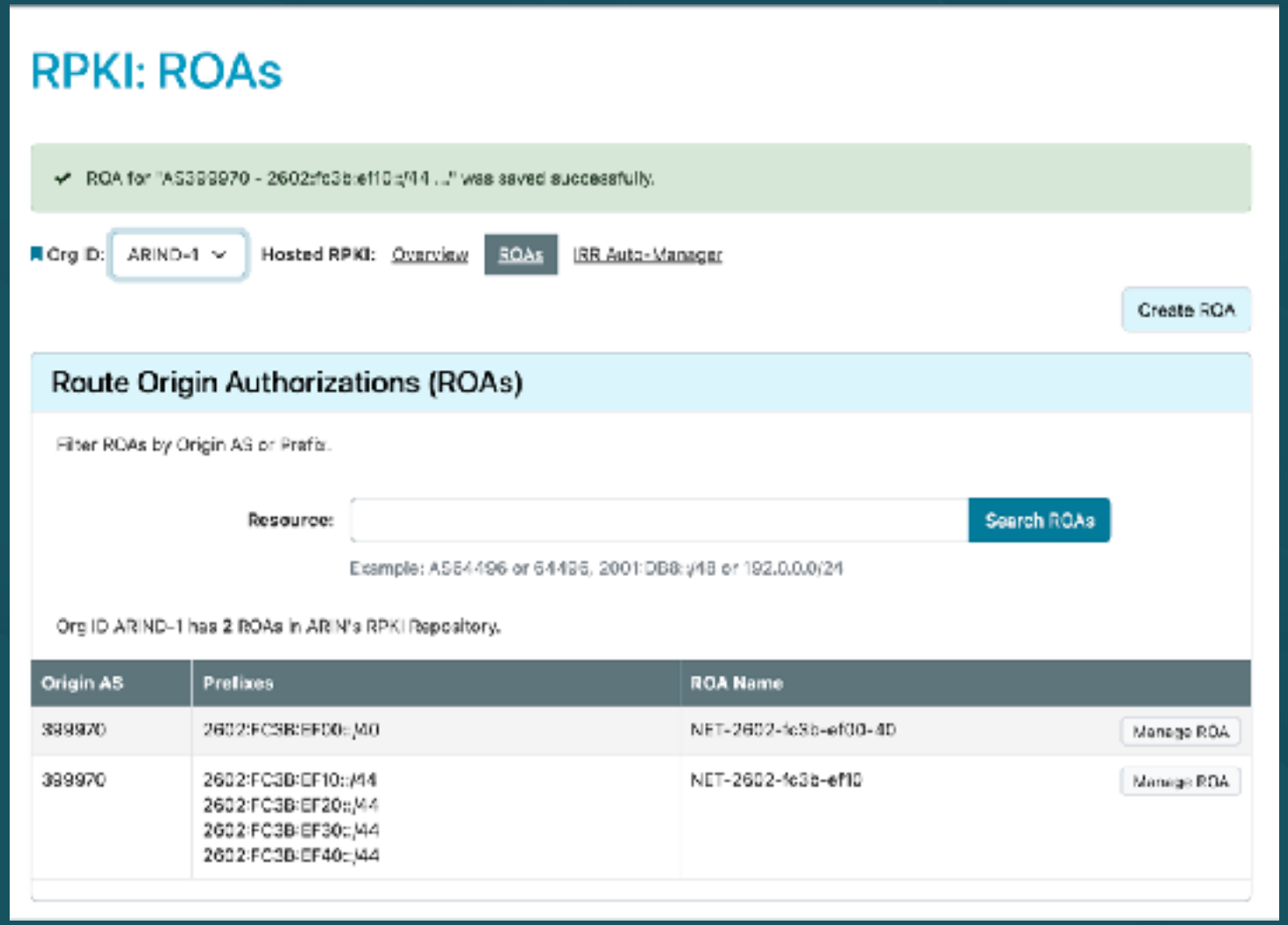
- There is no limit to the number of prefixes that can be entered into an individual ROA.
- Select the **Additional Prefix** button for every origin/prefix pair you want to add.
- Select the **Next Step** to proceed.

Create Multi-Prefix ROA Review



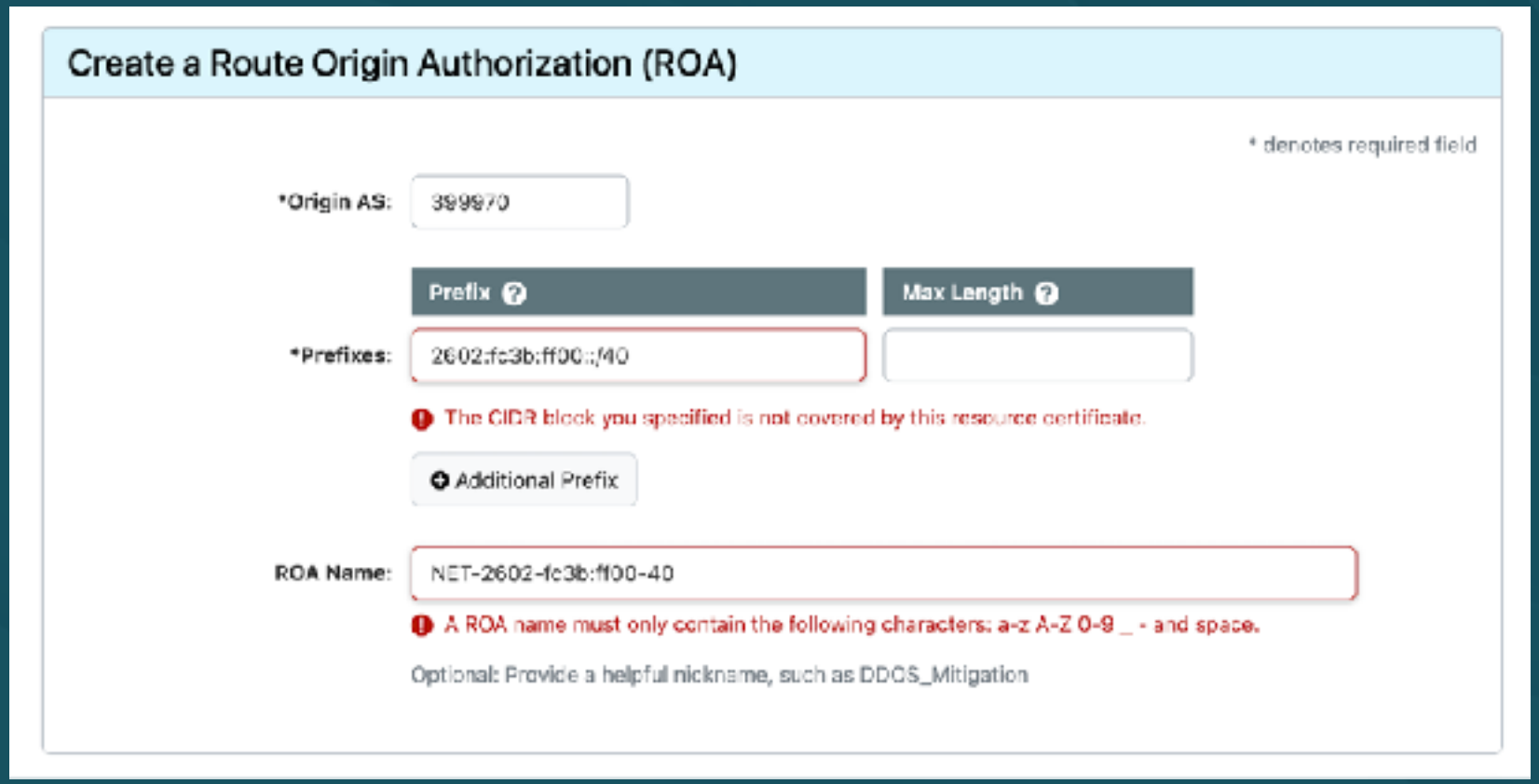
- The Review ROA table presents the same information as a single prefix ROA
- Select the **Submit** button to continue and return to the ROAs table

Create Multi-Prefix ROA Success



- 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

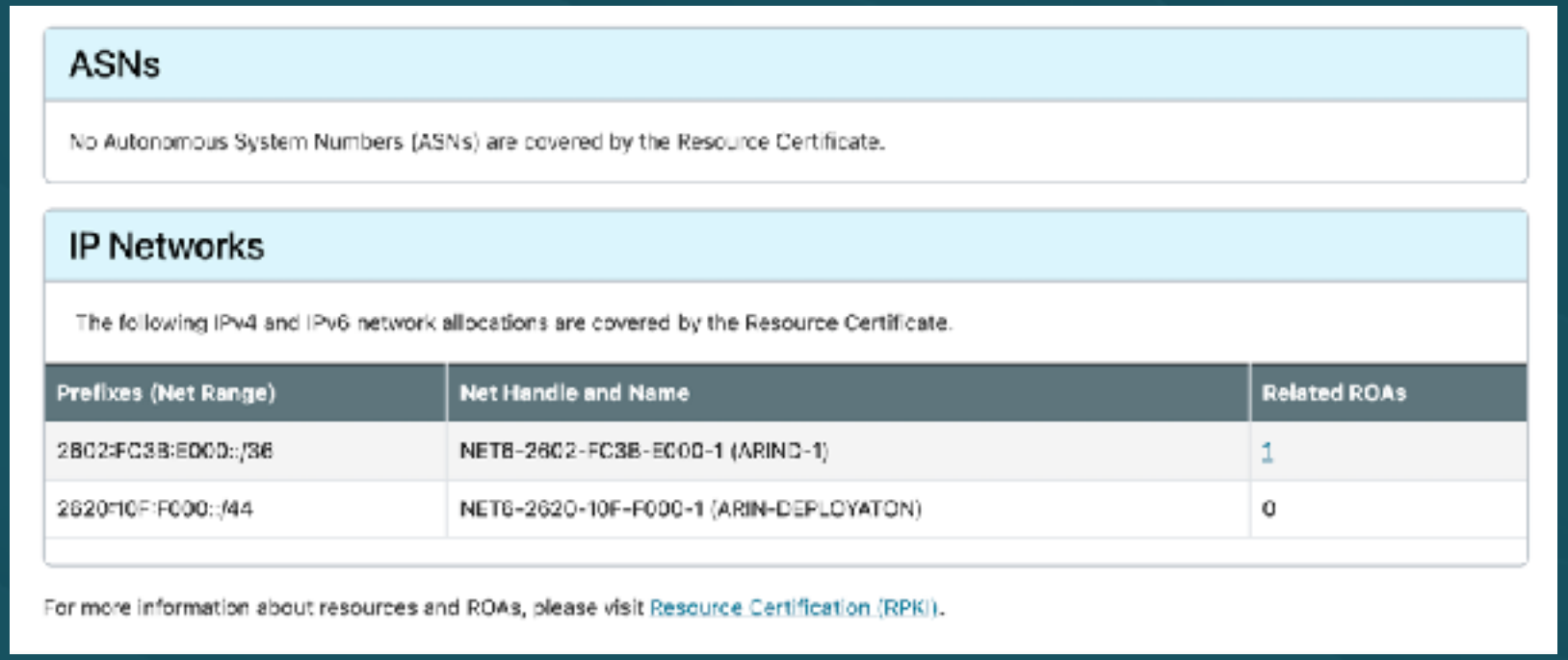
Create ROA - Failure



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 paring 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

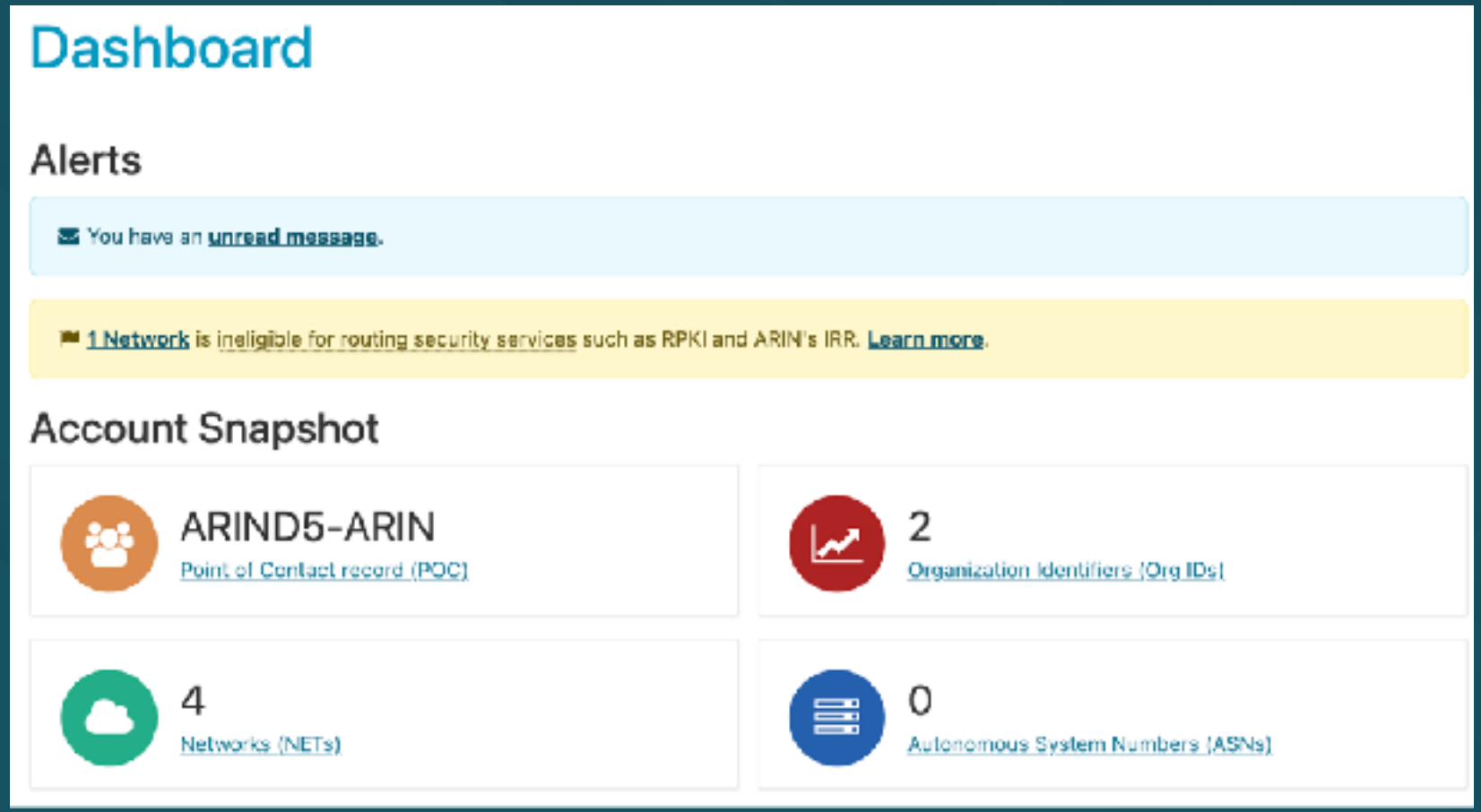
The following IPv4 and IPv6 network allocations are covered by the Resource Certificate.

Prefixes (Net Range)	Net Handle and Name	Related ROAs
2602:FC3B:E000::/36	NET6-2602-FC3B-E000-1 (ARIN-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 (RPKI).

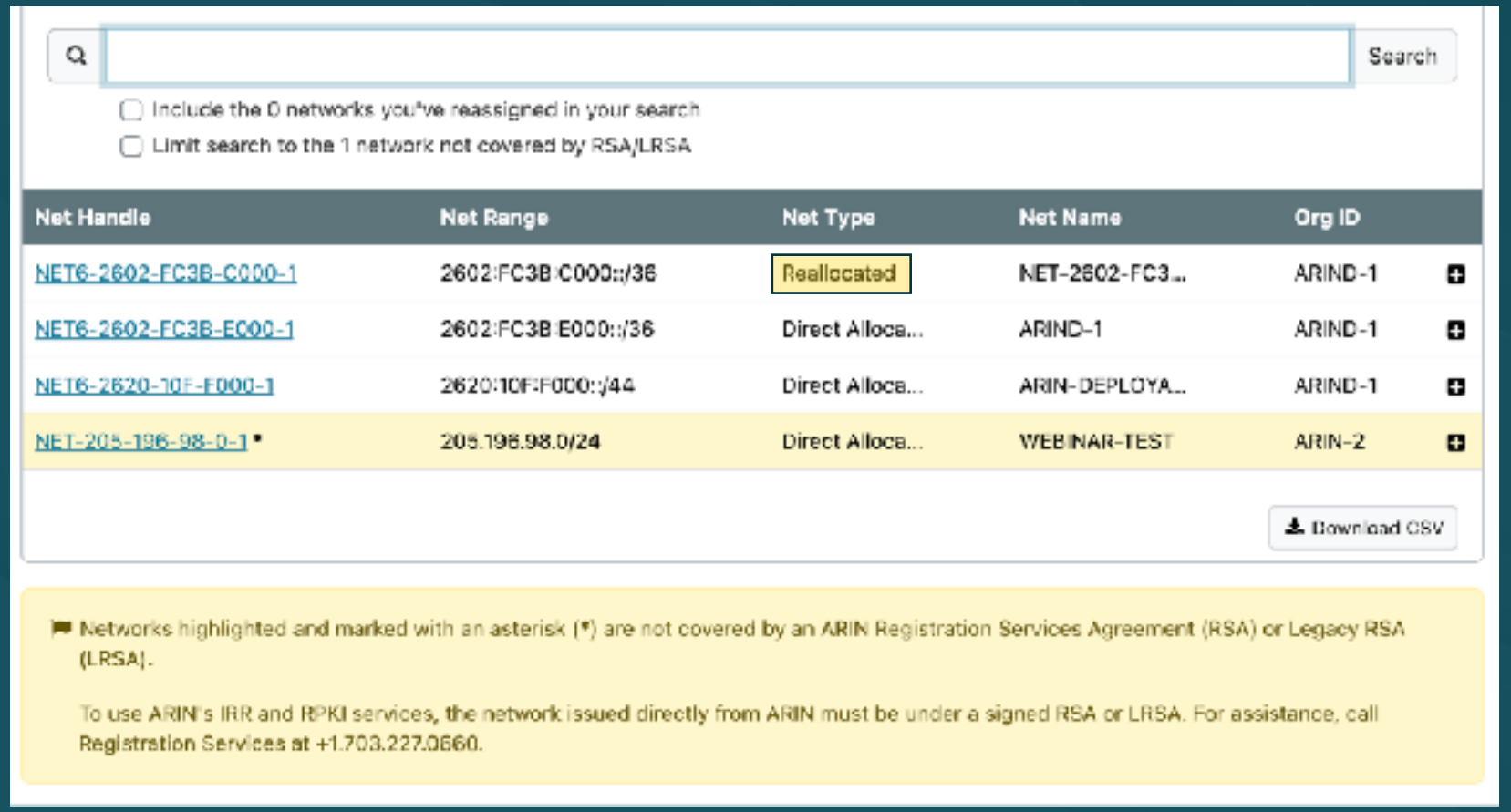
- Go back to the Overview Tab and select **Certified Resources**
- Is the IP prefix you entered on your resource certificate?
- ARIN is the authority that identifies who has been allocated resources
- No misconfiguration or a nefarious attempt at creating a ROA with your resources by others is blocked

Ineligible Resources – User Dashboard



- The 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.

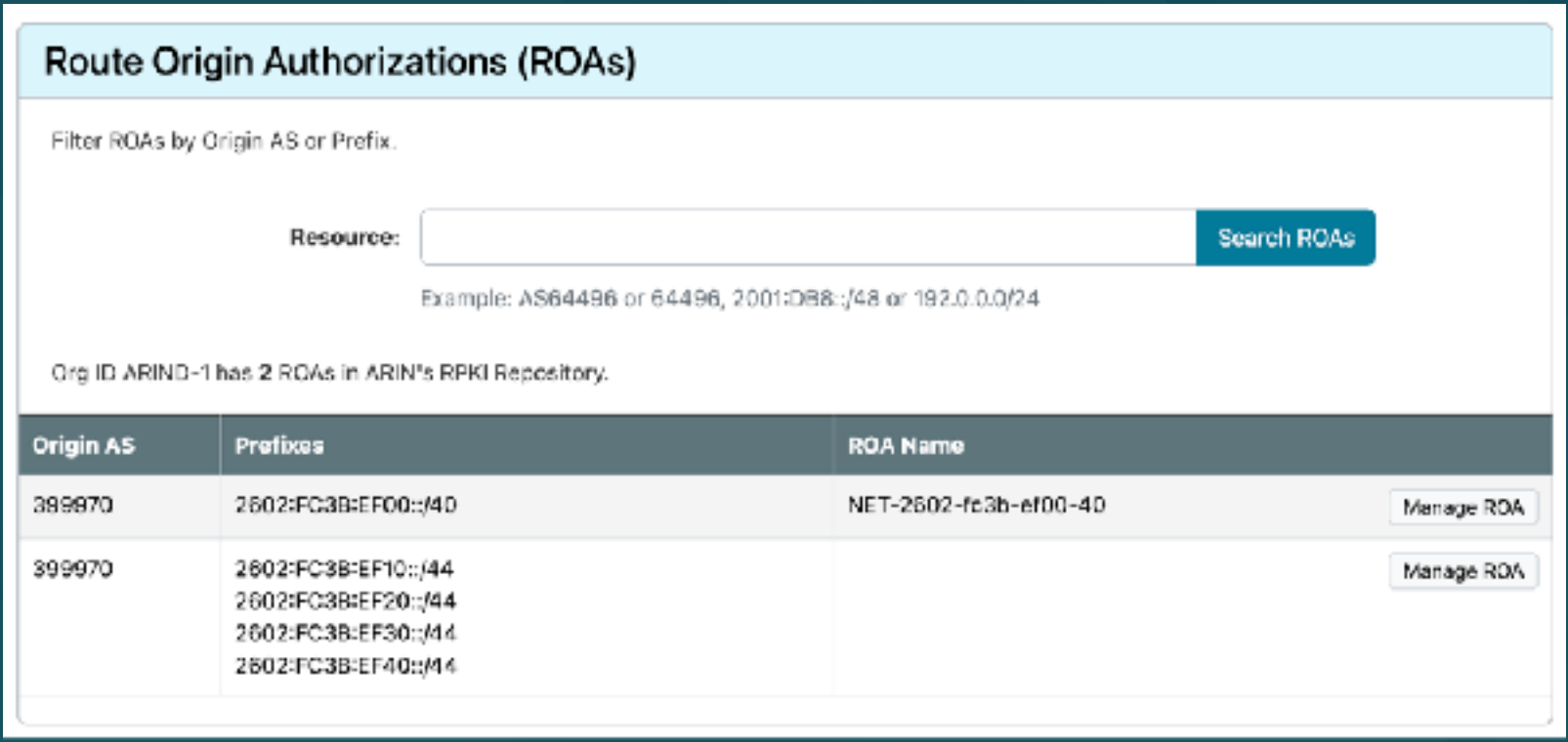
Ineligible Resources – Manage Resources



- 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

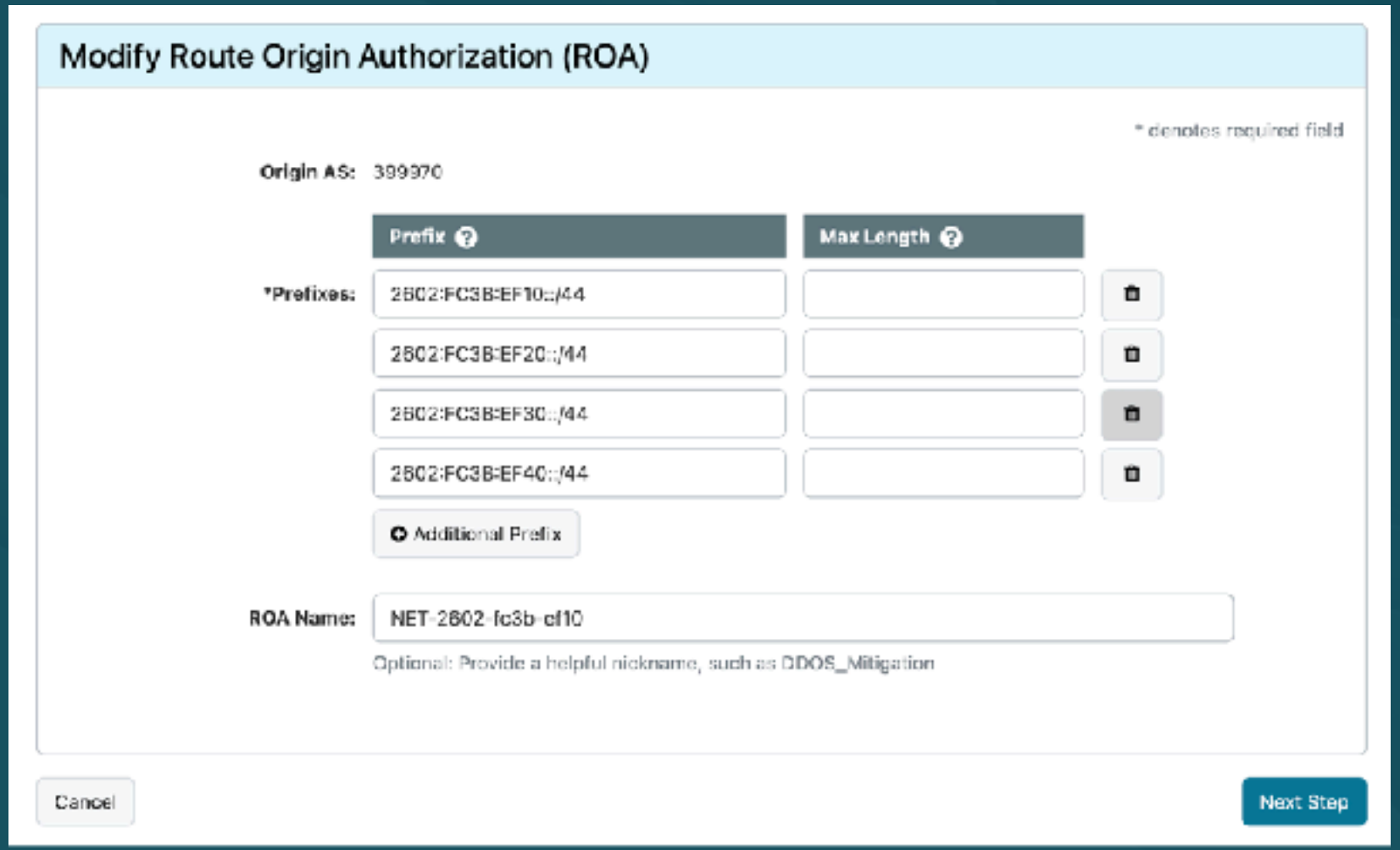
Modifying ROAs

Modify ROA



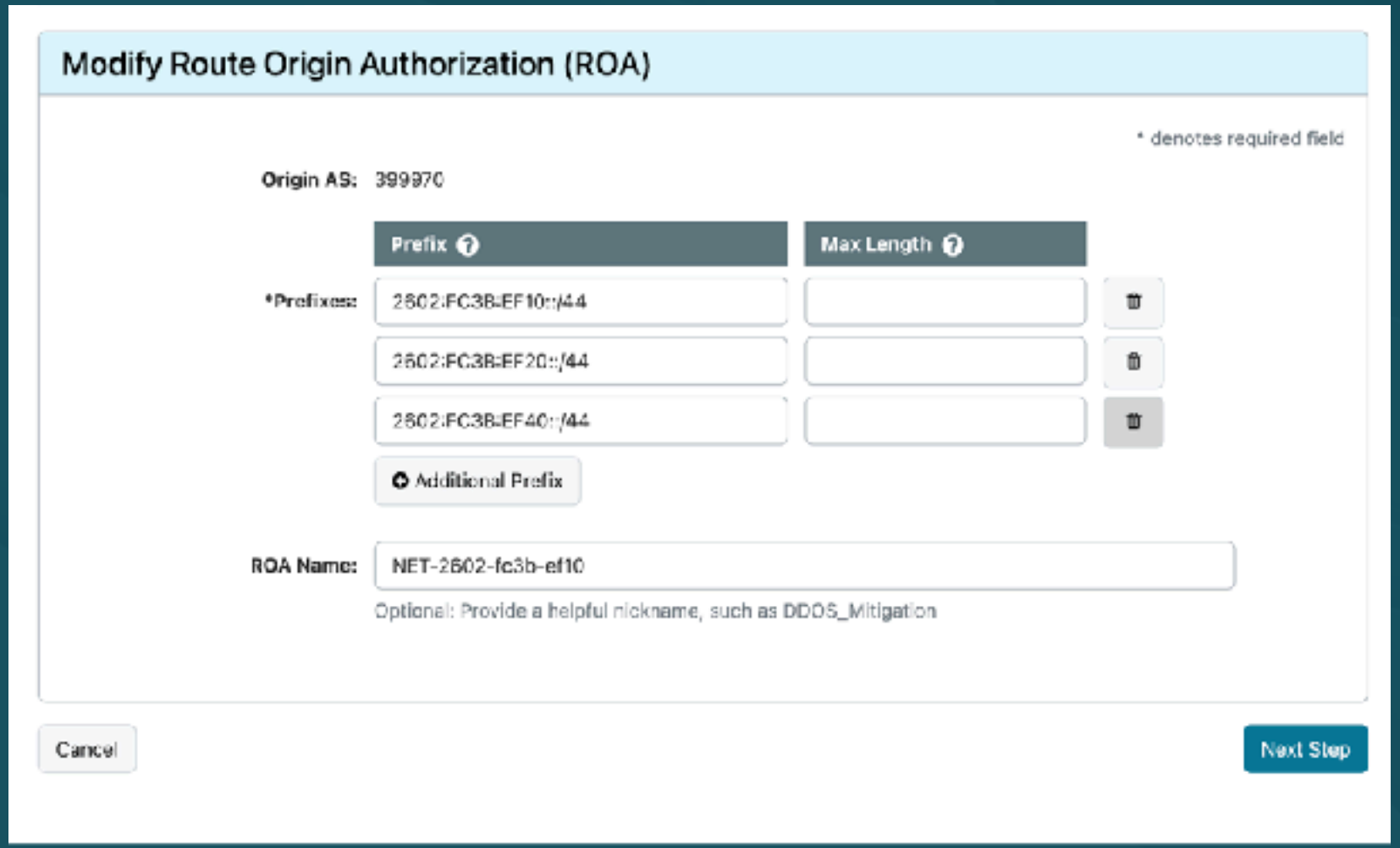
- Back to the ROA table… note the **Manage ROA** button in each row for the corresponding ROA
- Select **Manage ROA** next to the multi-prefix in the table

Modify ROA



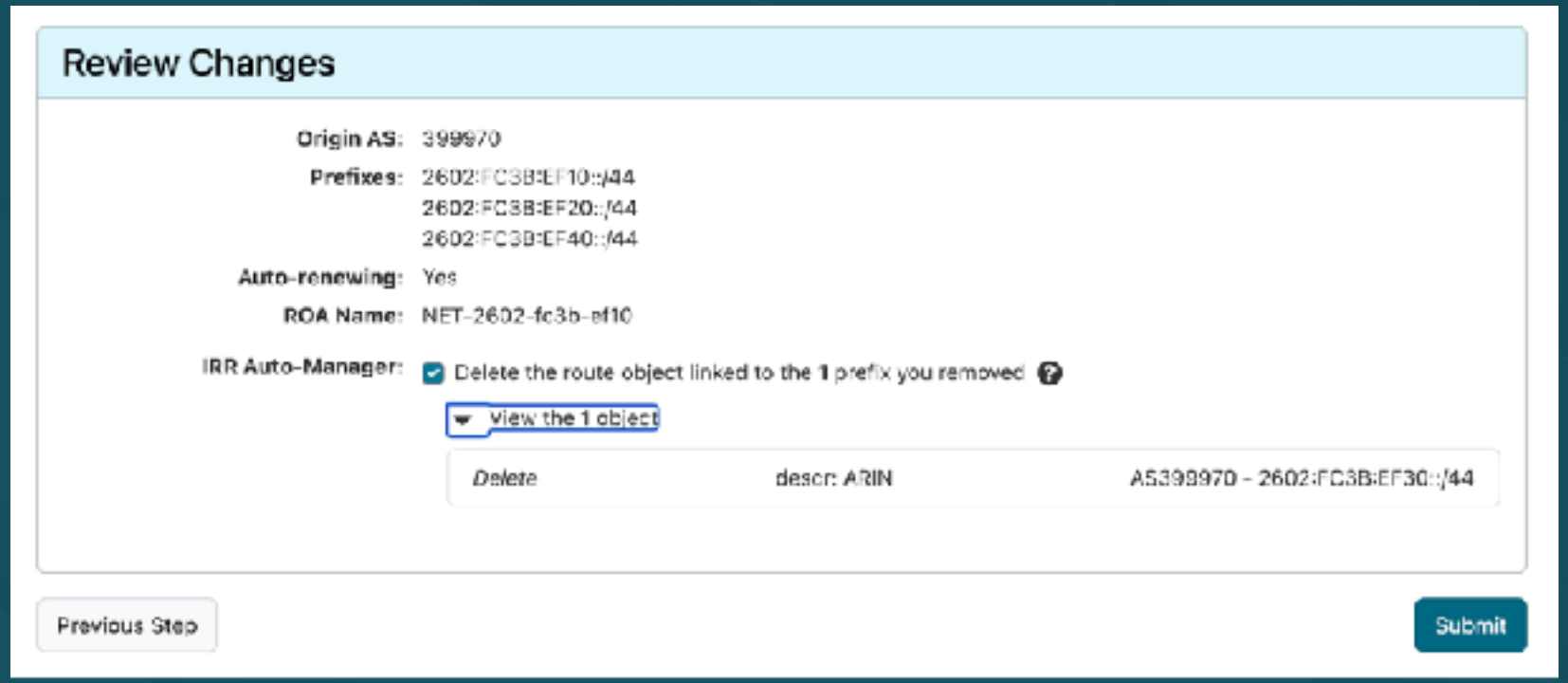
- There is a trash can icon next to each prefix contained in the ROA.
- Select the **trash can** for a prefix you want to remove from the ROA.

Modify ROA – post select change



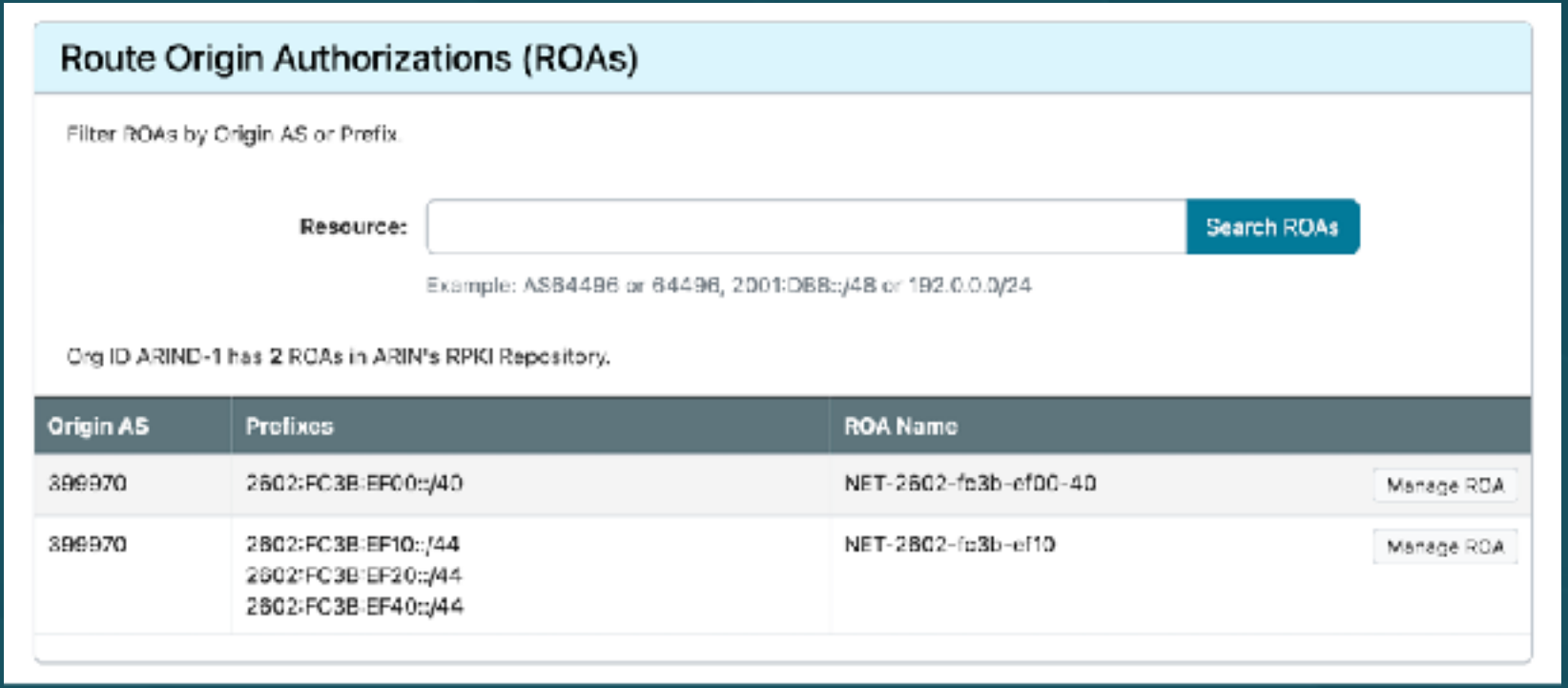
- The prefix is removed from the list
- You can add a prefix during the same modify sequence; both actions will be executed simultaneously
- Select **Next Step**

Modify ROA Review



- Review your changes
- Select **Submit**

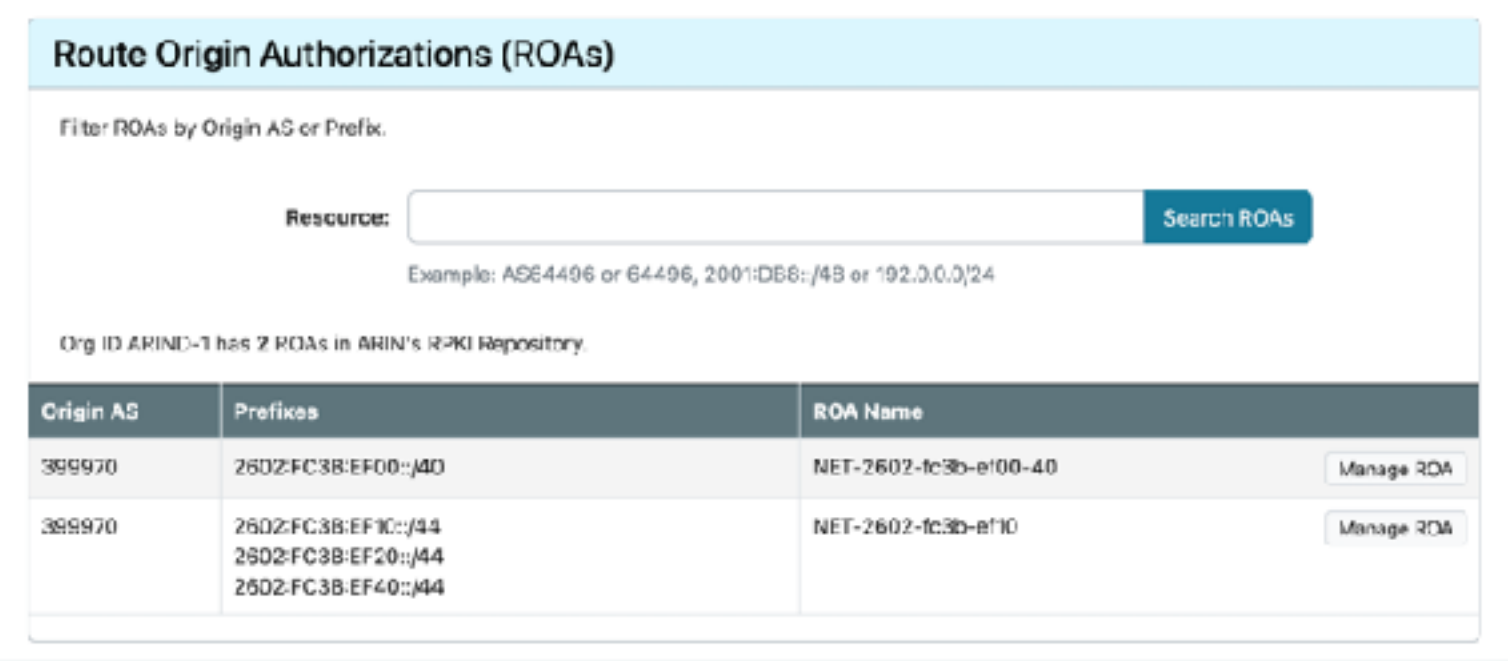
Modify ROA Success



The requested change is reflected in the ROA table.

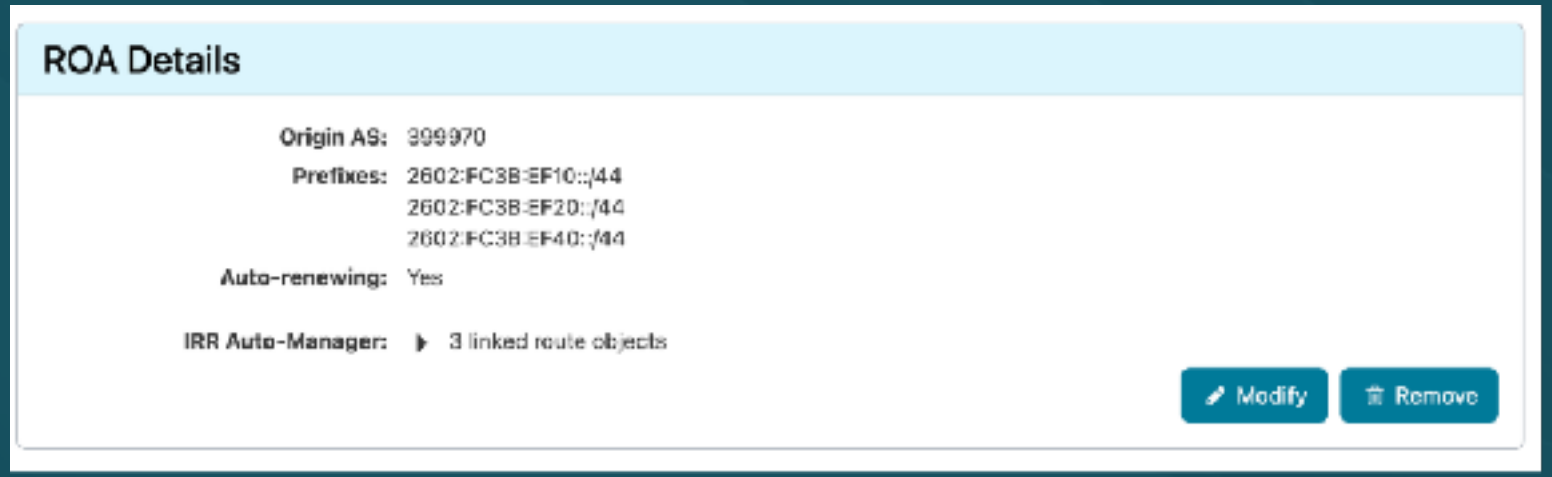
Removing ROAs

Remove ROA



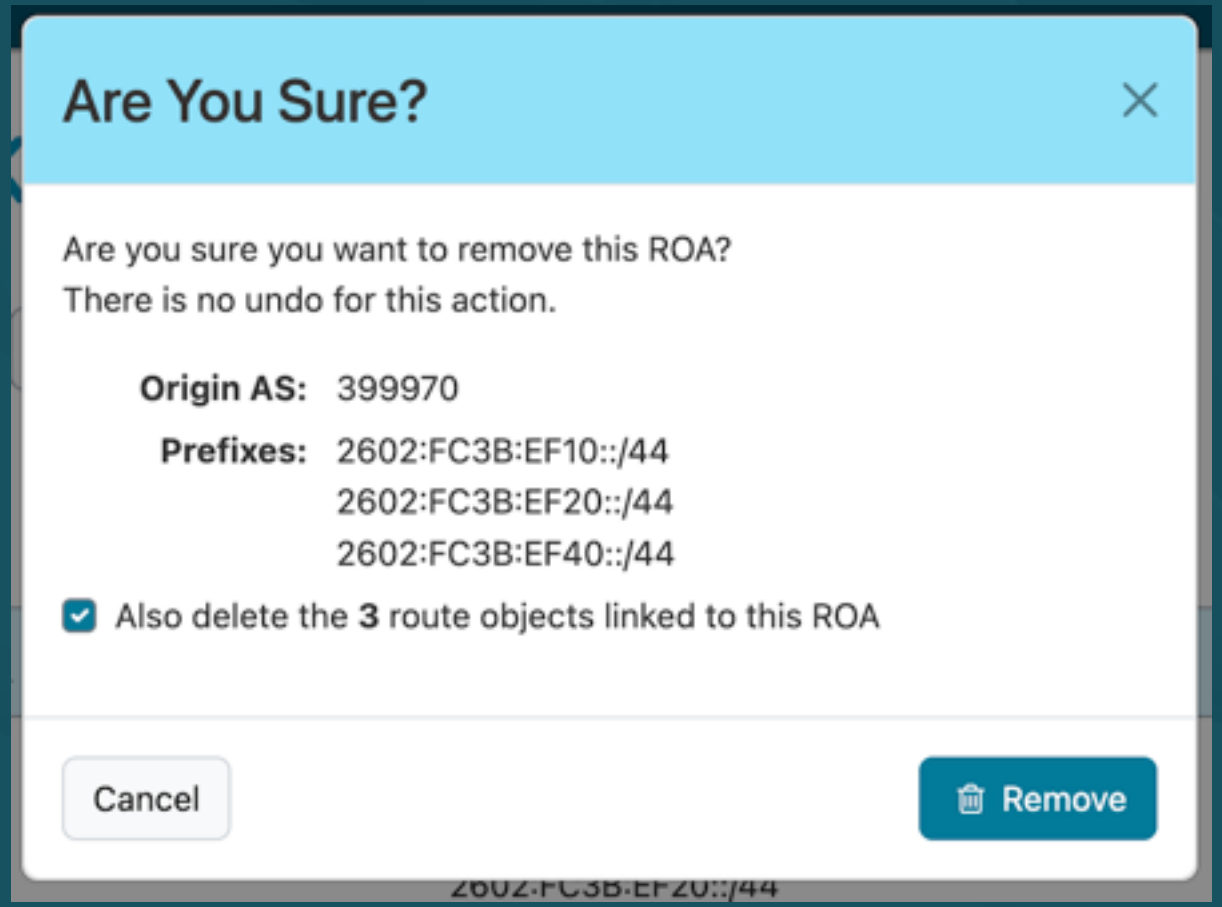
- The procedure to remove a ROA begins the same as modifying a ROA
- Return to ROAs table
- Select **Manage ROA** next to the multi-prefix ROA

Remove ROA



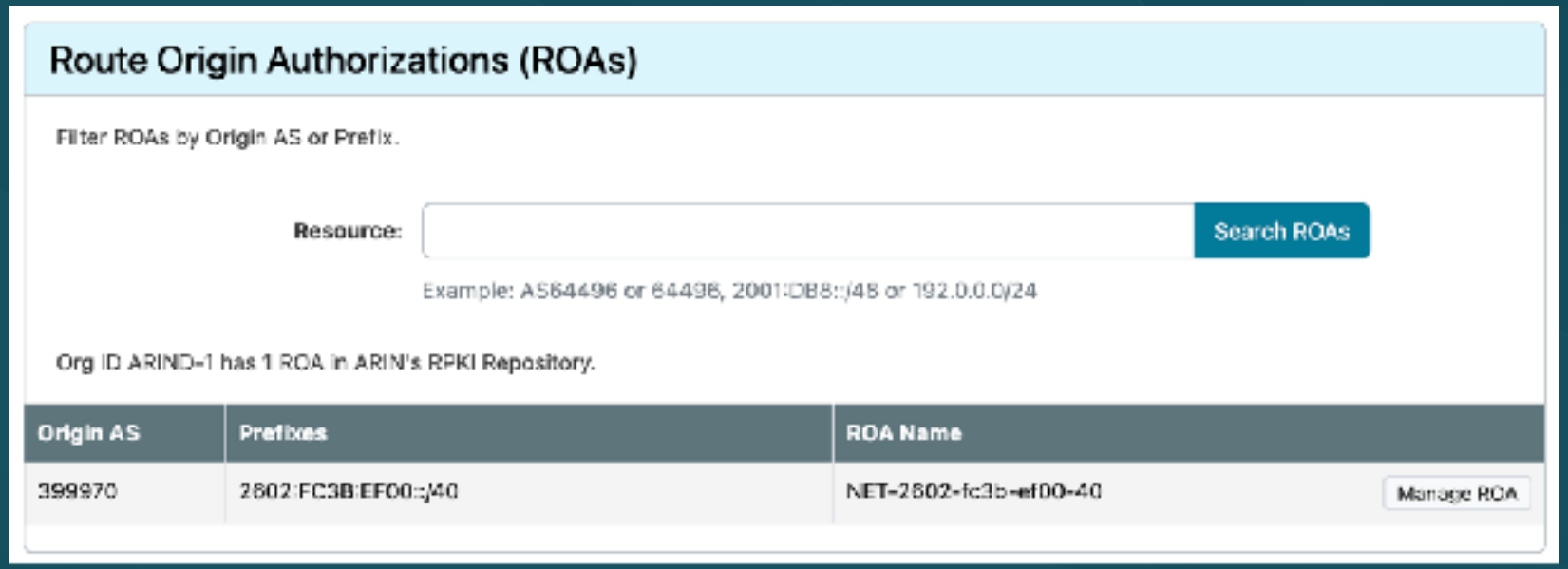
- In the ROA details window Select **Remove**

Remove ROA – Confirm Request



- 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**

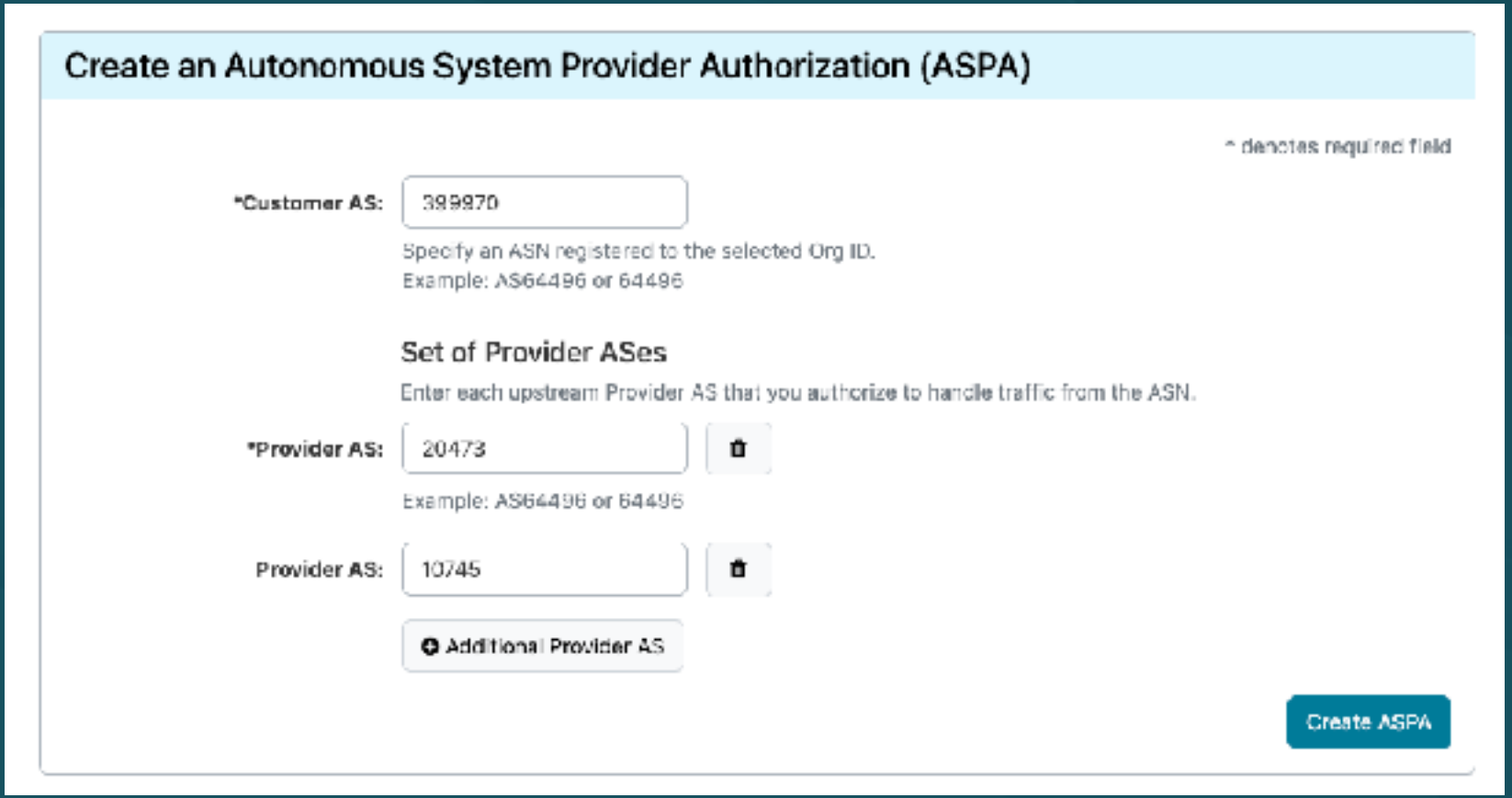
Remove ROA Success



- 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.

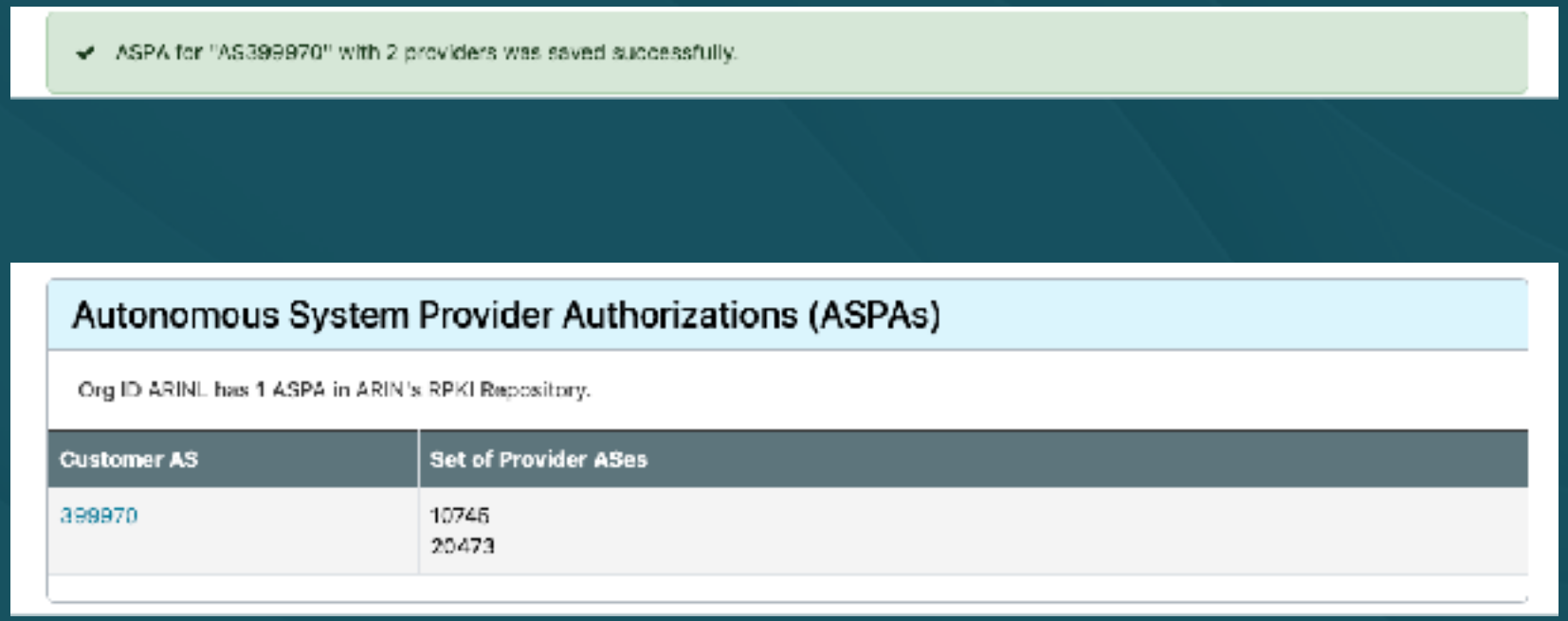
Creating ASPAs

ASPA Entry Form



- 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**

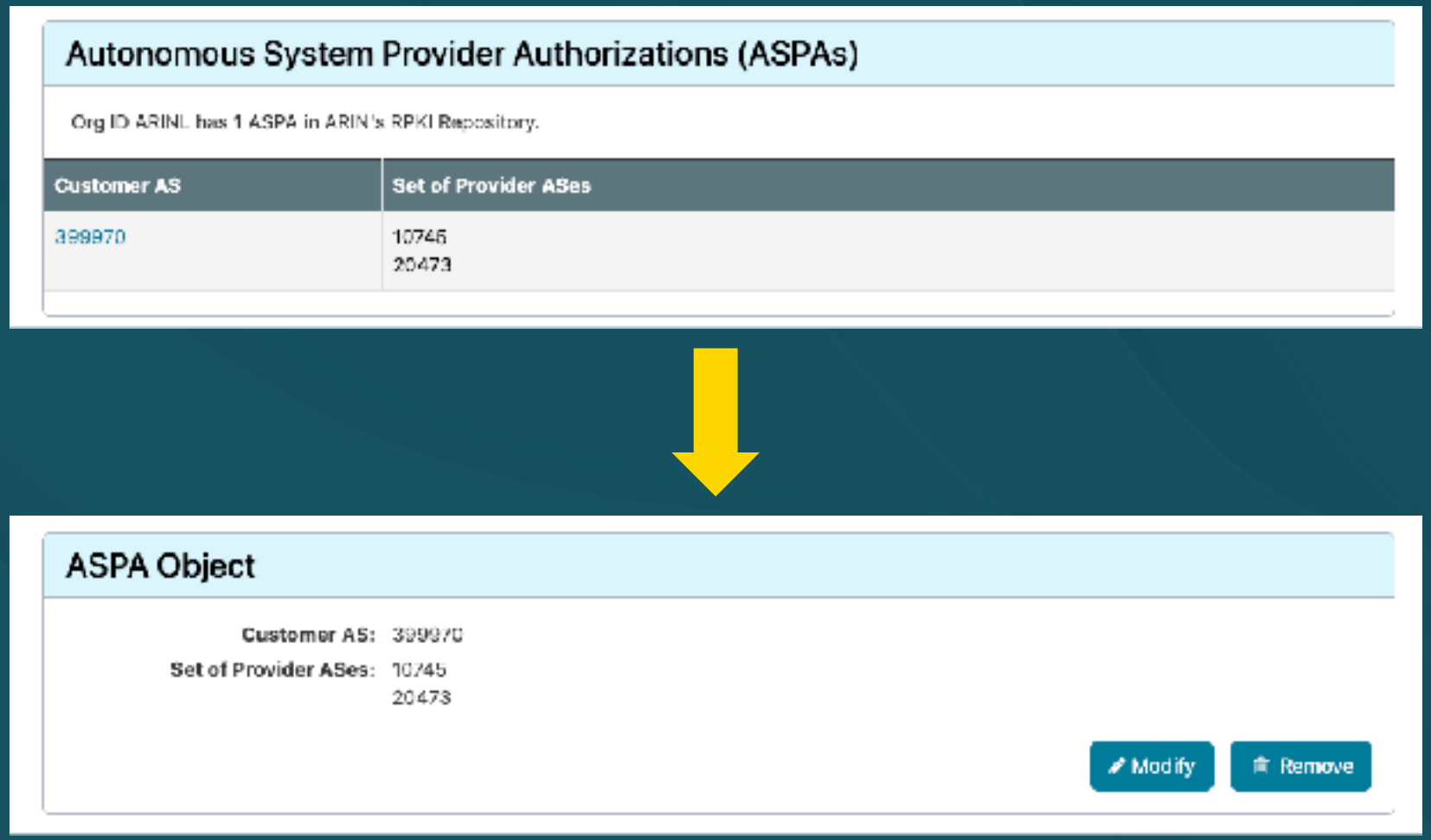
ASPA Confirmation



- 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

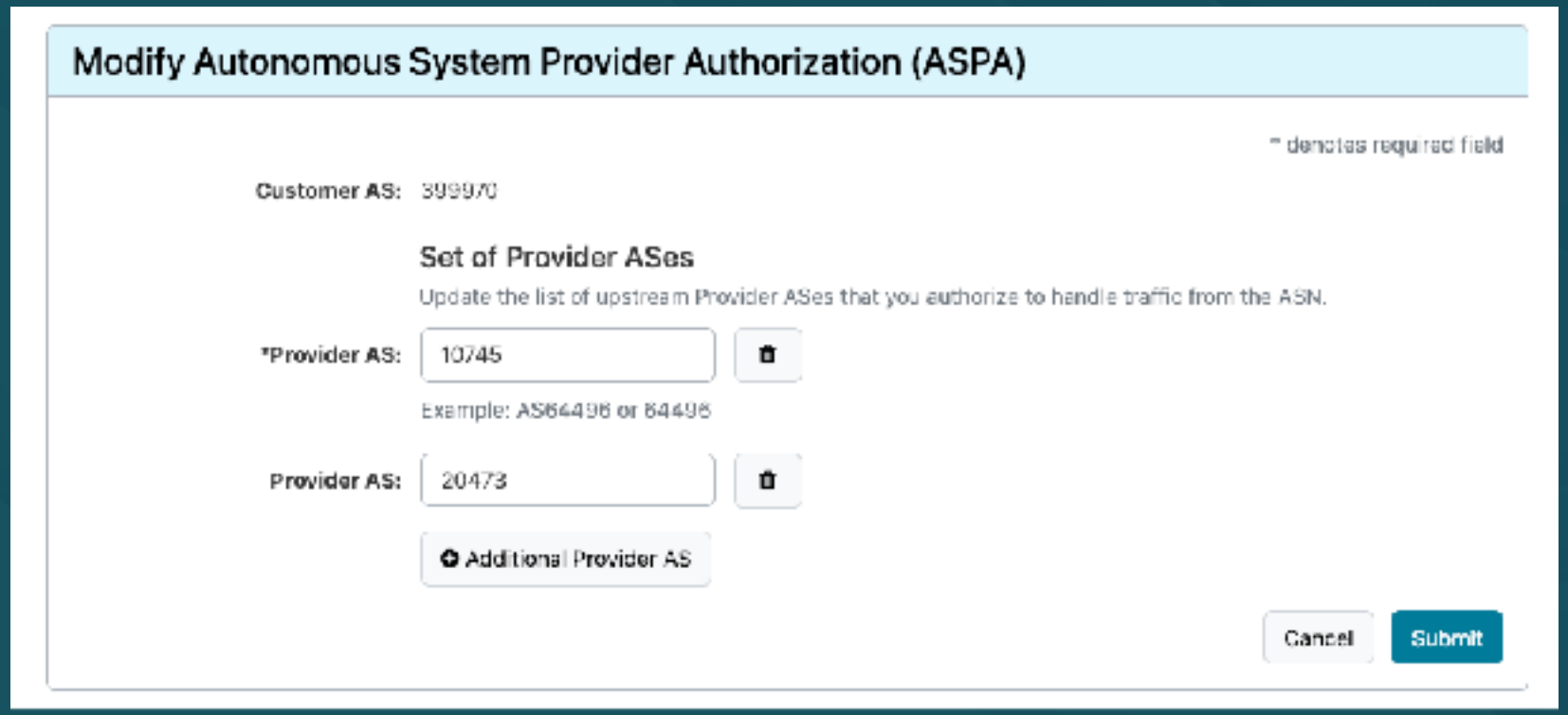
Modifying an ASPA

Modify an ASPA



- 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

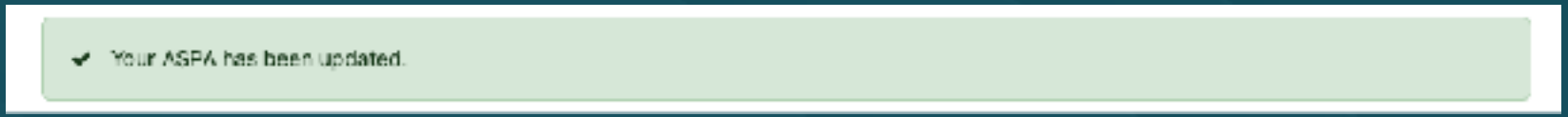


- Here you can change a provider AS number, add a new provider AS, or delete a provider AS from the ASPA
- In this example, we are going to remove a provider AS from the ASPA
- Select the **trash can icon** next to provider **AS 20473**

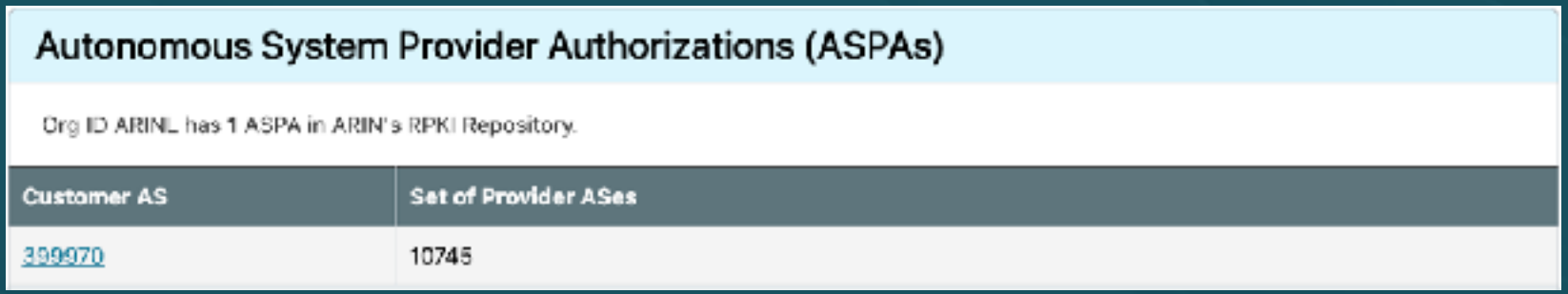
Modify an ASPA

- 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



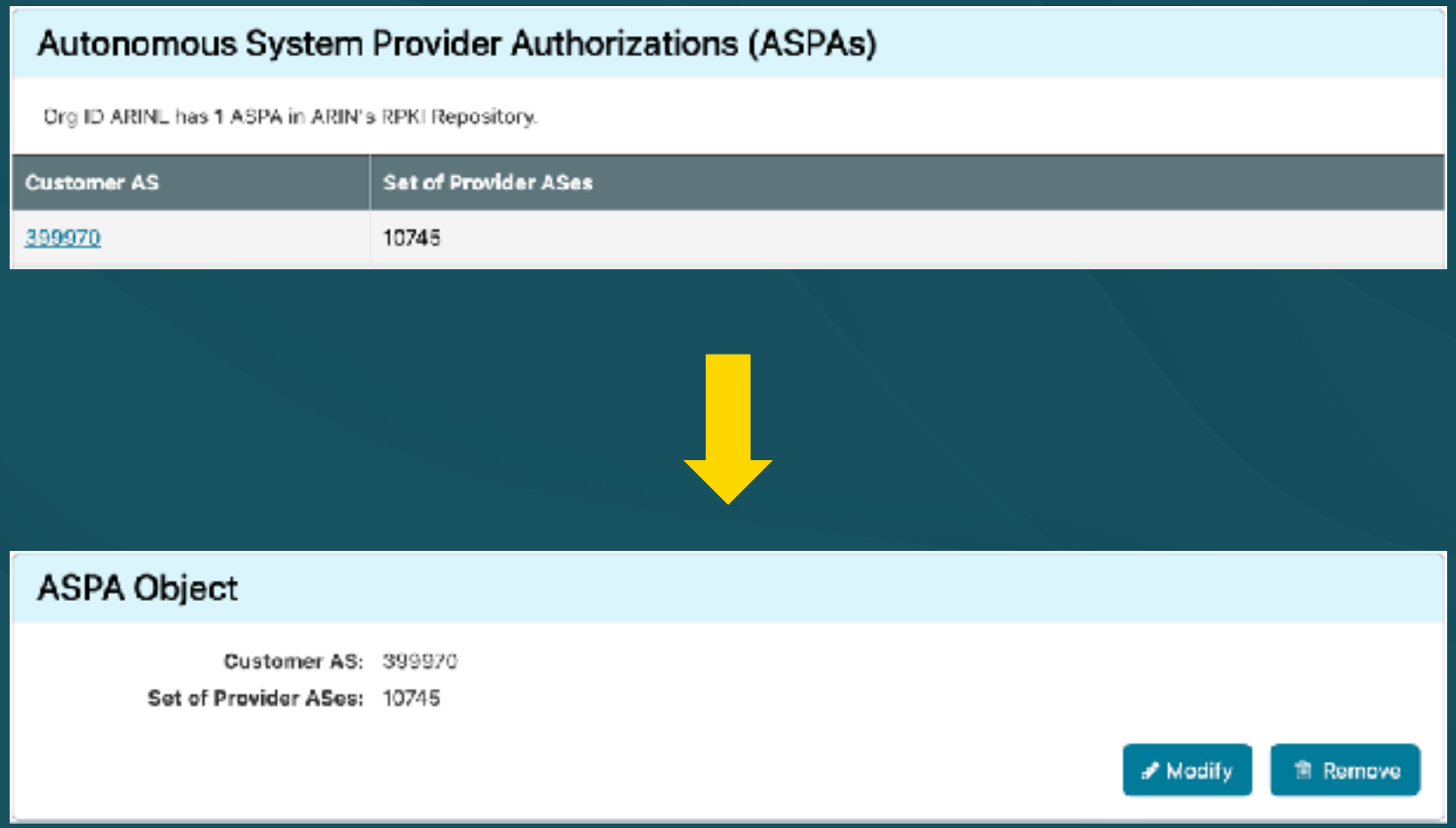
- Confirmation is received the change was successful



- The ASPA table shows the results of the modification

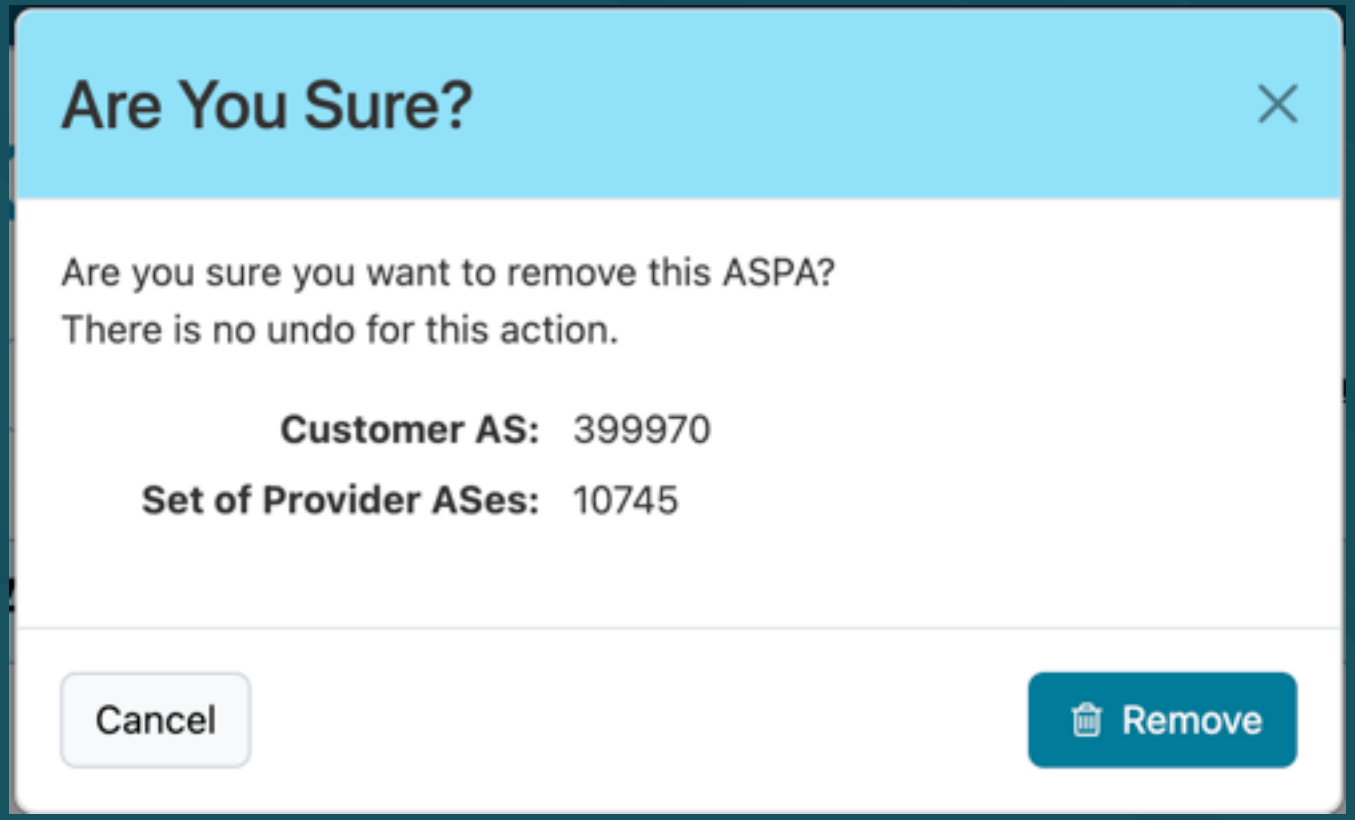
Removing an ASPA

Remove an ASPA



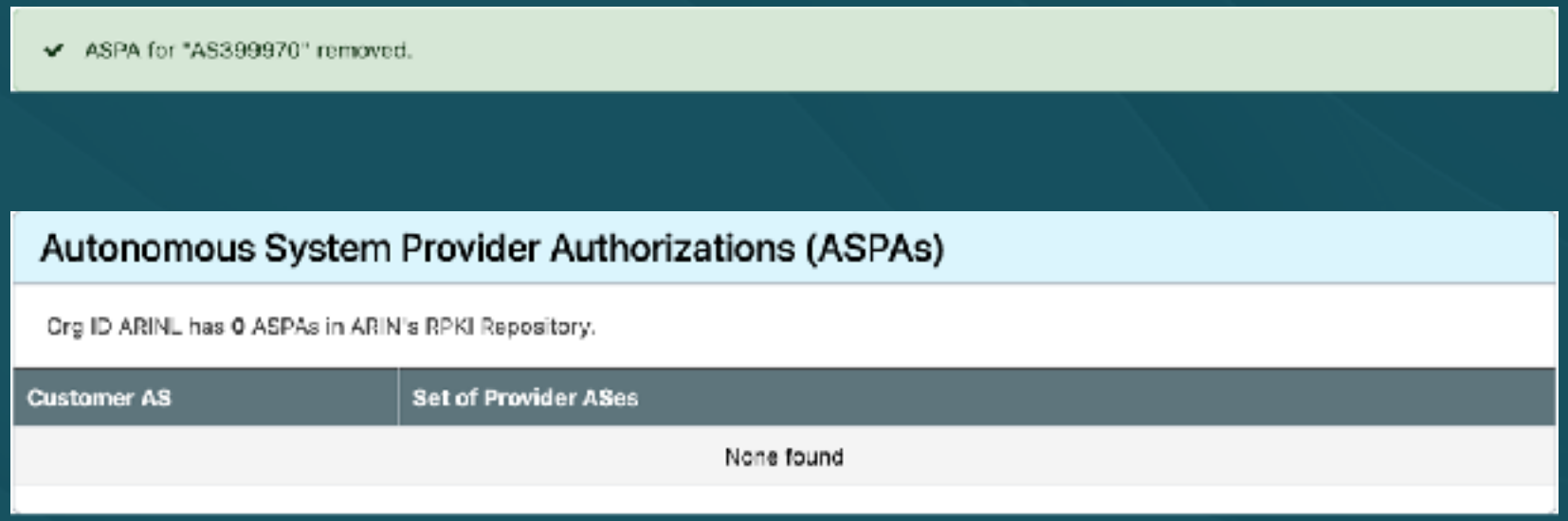
- Removing an ASPA starts the same as modifying an ASPA
- In the ASPA table, identify which object you want to remove and select the **Customer AS number**
- Select **Remove** to continue

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**

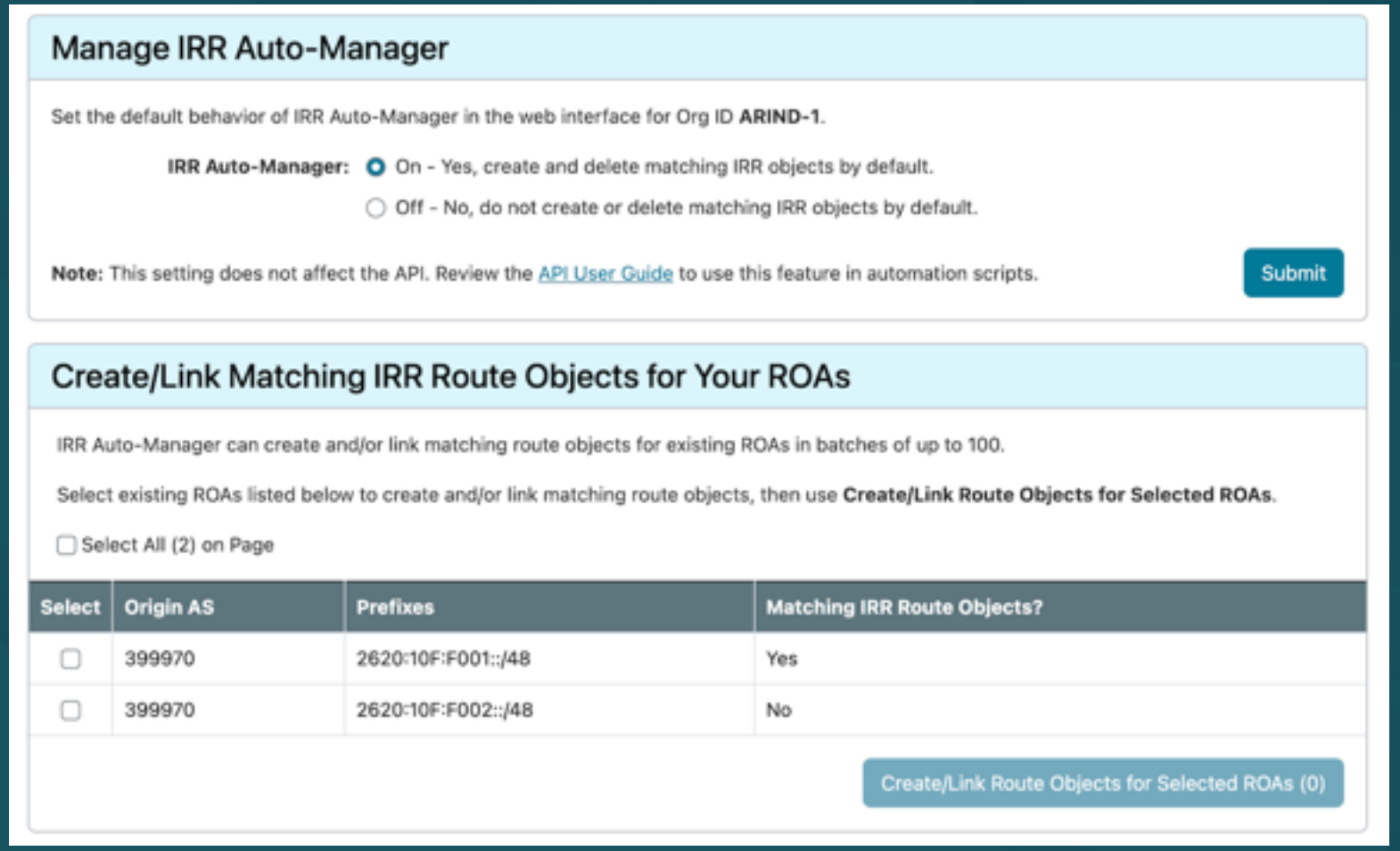
Remove an ASPA success



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

IRR Auto-Manager

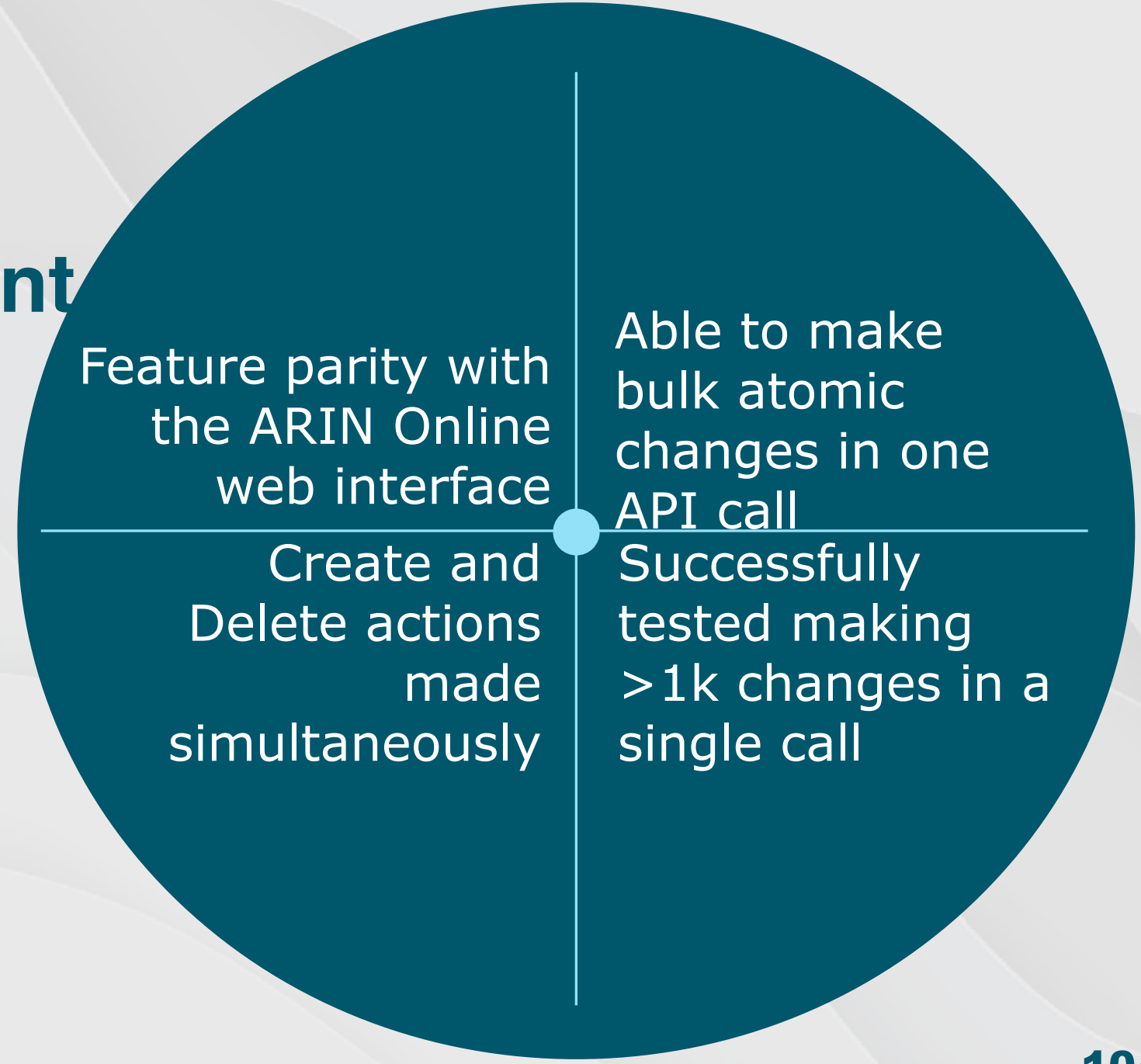
IRR Auto-Manager



- 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

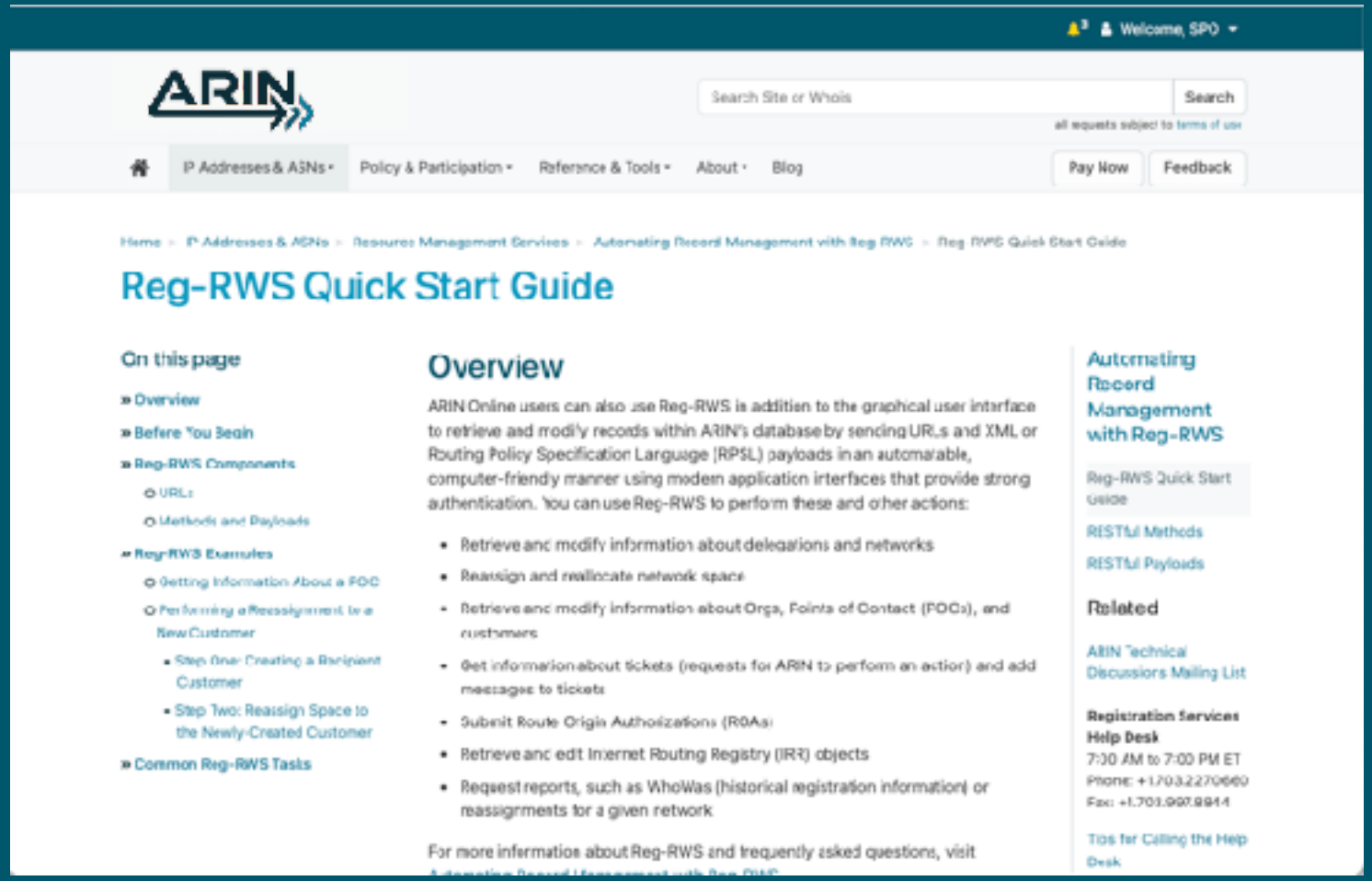
Reg-RWS – RESTful API Endpoint



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



- 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!

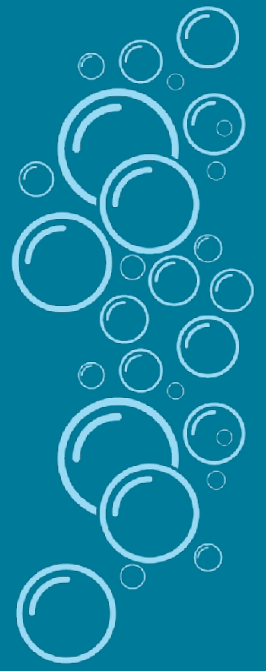
- RPKI documentation - https://rpki.readthedocs.io/en/latest/index.html
- RPKI deployment hub - https://rpkihub.au/
- IETF SIDROPS - https://datatracker.ietf.org/group/sidrops/documents/
- RPKI Community Discord board (invite) - https://discord.gg/nGvKa3Yc
- ARIN RPKI FAQ - https://www.arin.net/resources/manage/rpki/faq/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

ARIN Deep Dive

DON'T FORGET:

Take home your workbook!

Thank You



Customer Technical Services Team

routing.security@arin.net