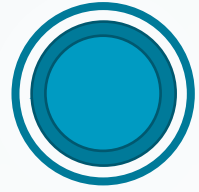




Stand up for your Routes!

Using the Resource Public Key Infrastructure (RPKI)

Brad Gorman, Product Owner Routing Security
American Registry for Internet Numbers (ARIN)
June 20, 2023



What's Being Covered Today

- Security of the Early Internet
- The Goal of the RPKI
- Current RPKI Deployment
- Using ARIN's RPKI Services

A faint, light blue network diagram is visible in the background, consisting of several interconnected nodes and lines, suggesting a network topology. The nodes are represented by small circles, and the connections are thin lines. The overall style is clean and technical.

Security of the Early Internet



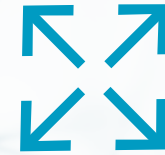
BGP Enabled the Internet We Know Today



Made it easy to establish peering sessions with neighboring networks



Transitioned from information sharing to a commercial platform



Scaled beyond where best effort sharing of routing policy was reliable

Routing Policy Specification Language (RPSL)

- RPSL is a standard language used by Internet Service Providers to build security policy on network devices
- Internet Routing Registry (IRR) is an ecosystem where operators share information about their policies
- ARIN authenticates entries in our database, confirming the resource holder created the objects
- We don't discourage using a 3rd party IRR for redundancy, however, information cannot be verified

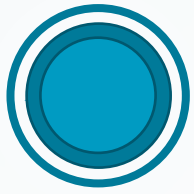
The background of the slide features a faint, light blue network diagram consisting of interconnected nodes and lines, suggesting a complex system or data structure. A solid teal horizontal bar spans the width of the slide, containing the main title. Below the teal bar, a thin grey horizontal line is visible, ending in a small dark grey circle on the right side.

The Goal of the RPKI

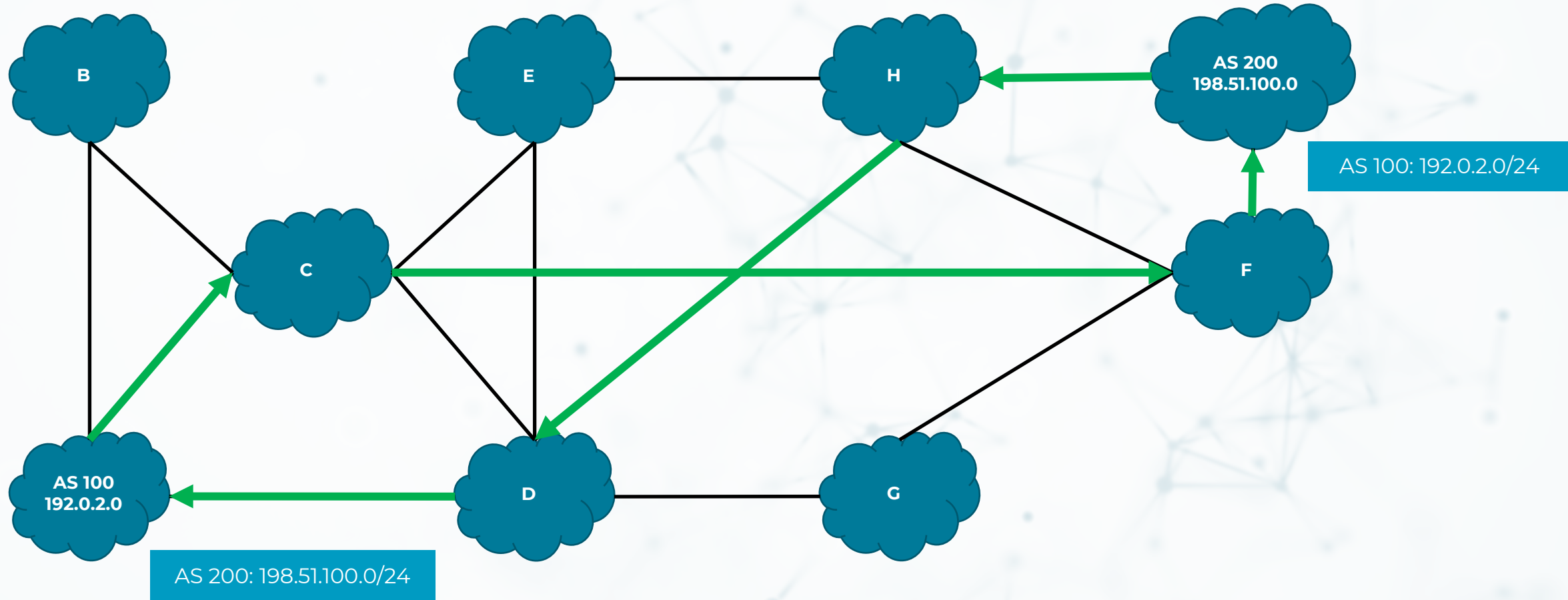
The Goal of the RPKI

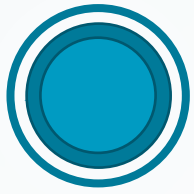
Provide a cryptographically signed method for an Internet number resource holder, allowing them to make an authoritative statement about the origin of a prefix(s) announced on to the Internet (Route Origin Authorization, ROA)

- RPKI gives operators another data set to make more informed routing decisions (Route Origin Validation, ROV)
- Protect resource holders from impact resulting from human error or nefarious activity
- Reduce the overall attack vector for attempted hijacks on the greater Internet

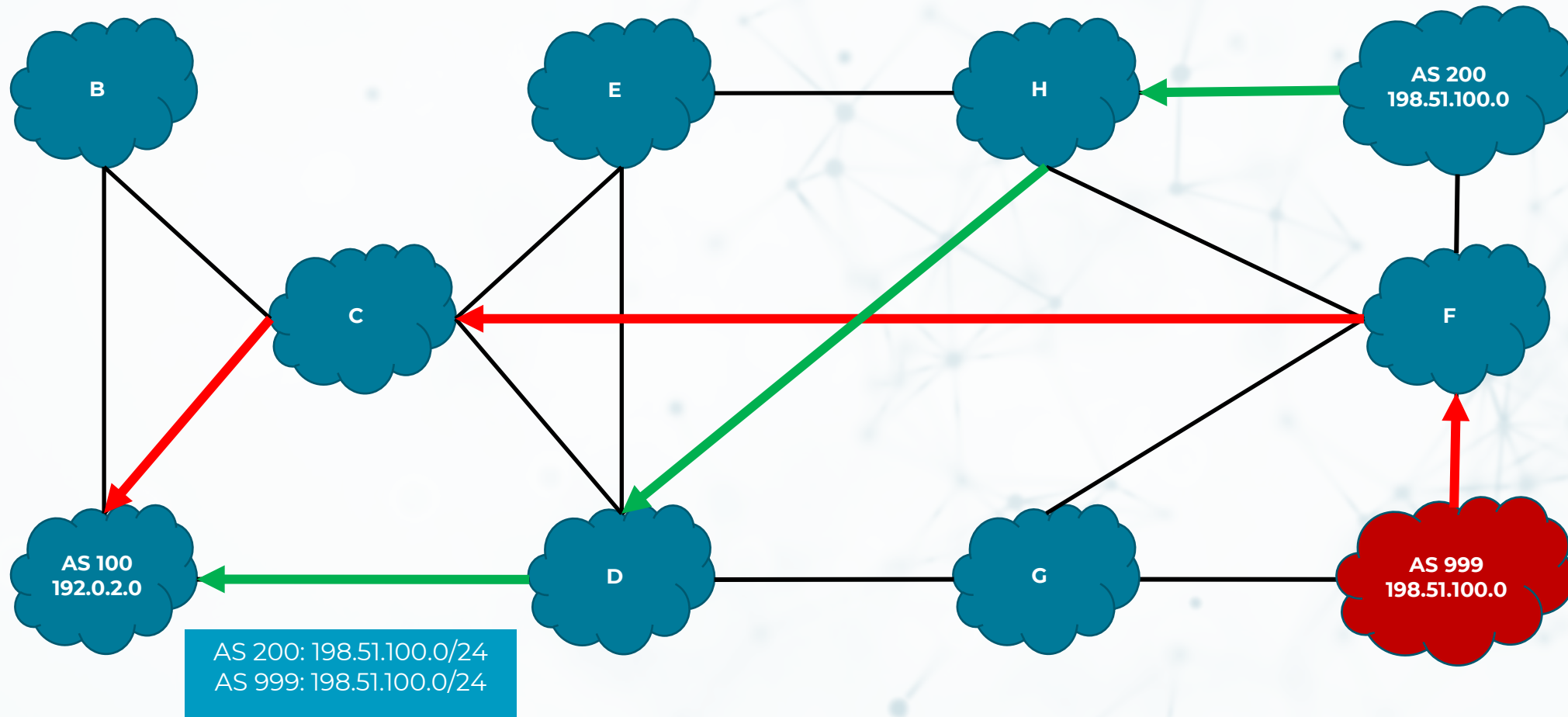


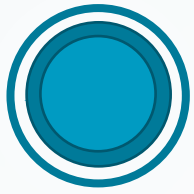
Internet is More Complex Today



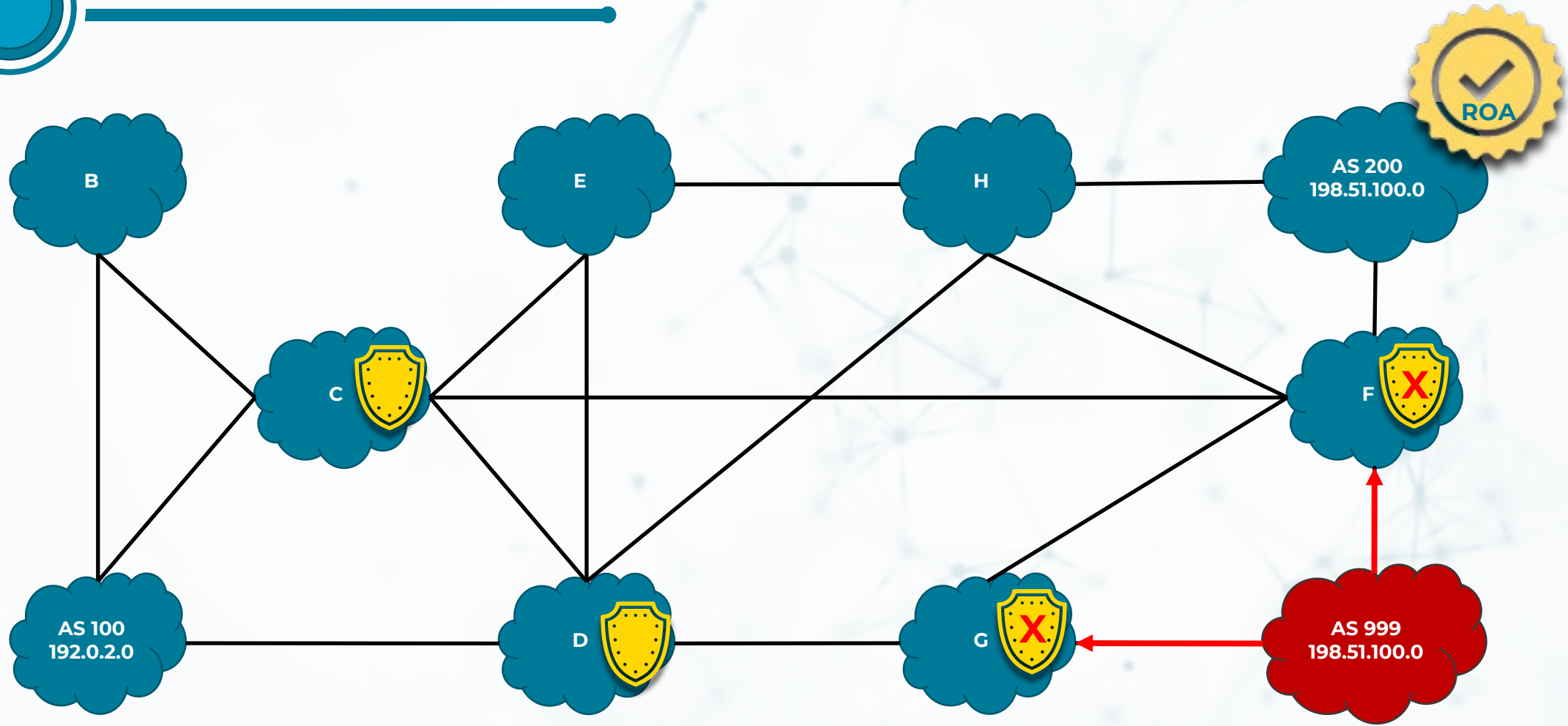


Bad Actors Will Find a Way





RPKI in Action



A faint, light blue network diagram is visible in the background, consisting of several interconnected nodes and lines, suggesting a network topology. The diagram is centered horizontally and spans most of the vertical height of the slide.

Current RPKI Deployment

RPKI Adoption – Org Participation

- Only **19.5%** of Orgs registered to use ARIN's RPKI services
 - Hosted – **3,201**
 - Delegated – **80**
 - Repository Service (RPS) – **31**

45.3% of eligible* ARIN IP resources announced are marked as RPKI valid**

- 508M (eligible) / 1.12B (allocated to ARIN)
- 5.0% increase year-over-year

* Resources must be covered by a valid (L)RSA agreement to be eligible for RPKI services at ARIN

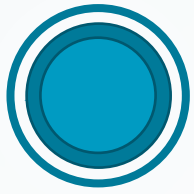
** To be considered RPKI valid there must be a VRP that exactly matches an existing route announcement in the global BGP table



We can do better!

A faint, light blue network diagram is visible in the background, consisting of several interconnected nodes and lines, suggesting a network topology. The diagram is centered horizontally and spans most of the vertical height of the slide.

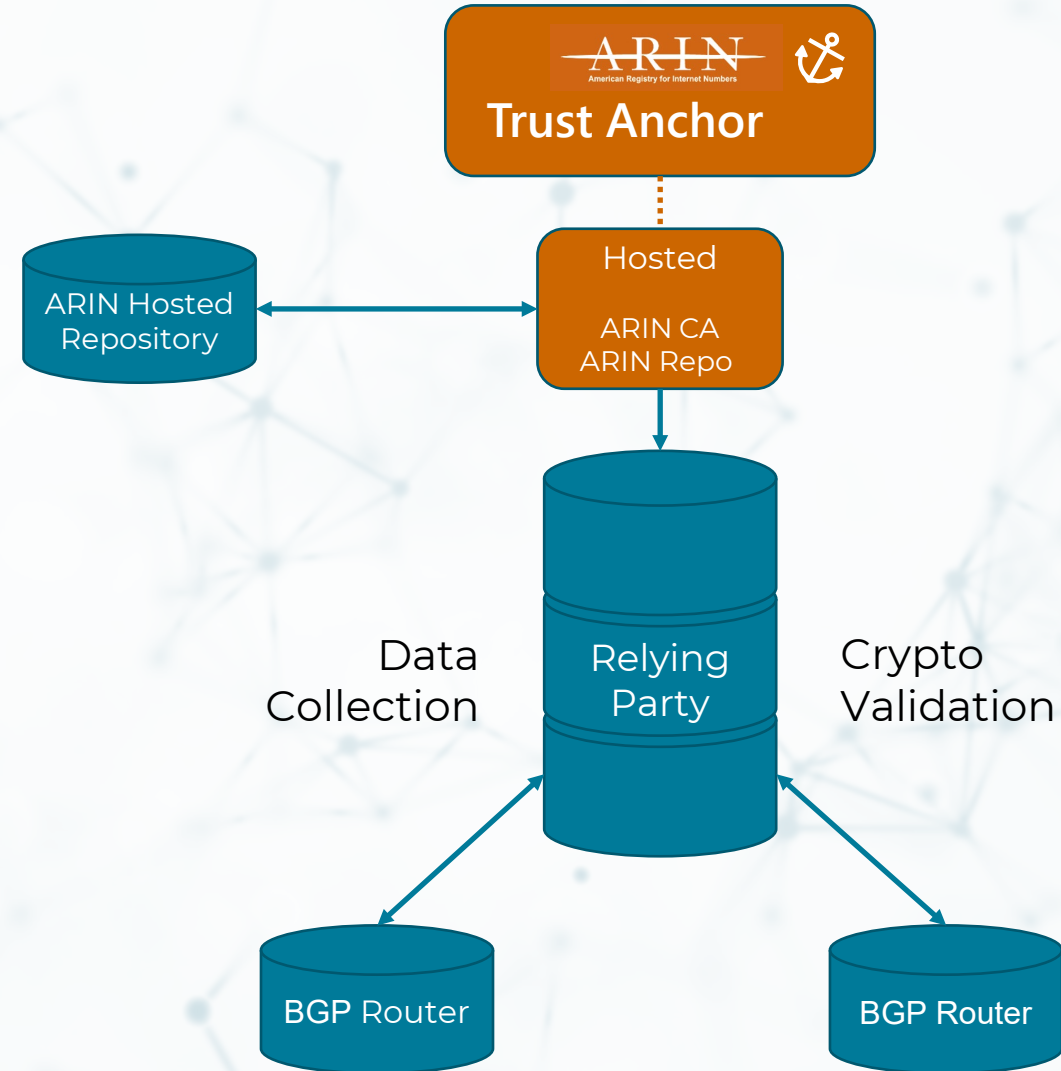
Using ARIN's RPKI Services



Hosted RPKI Service

- Certificate Authority (CA) managed by ARIN
- Repository and Publication services run by ARIN
- Org creates and maintains their ROAs
- Accessed via ARIN Online portal or the RESTful API

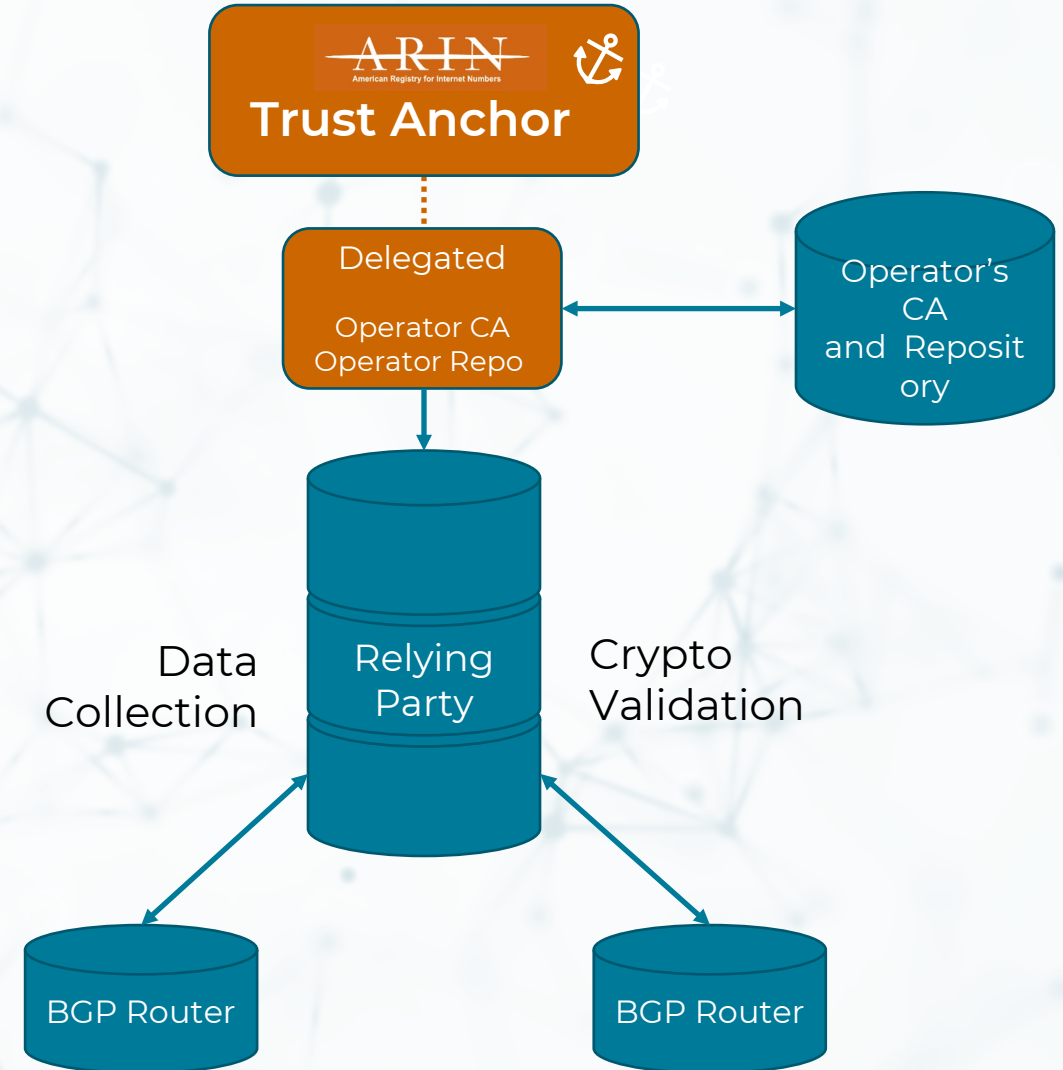
* **Easiest to use;** Recommended for most organizations just getting started with RPKI. Nearly 98% of ARIN participants use Hosted RPKI.





Delegated RPKI Service

- The organization has more control and independence
 - Runs their own CA to manage object signing
 - Separation of the publication of cryptographic functions
- * **Highest responsibility and uptime requirement**; only organizations with in-depth knowledge of RPKI and resources to run a Certificate Authority (CA) and a publication server, should select Delegate RPKI.

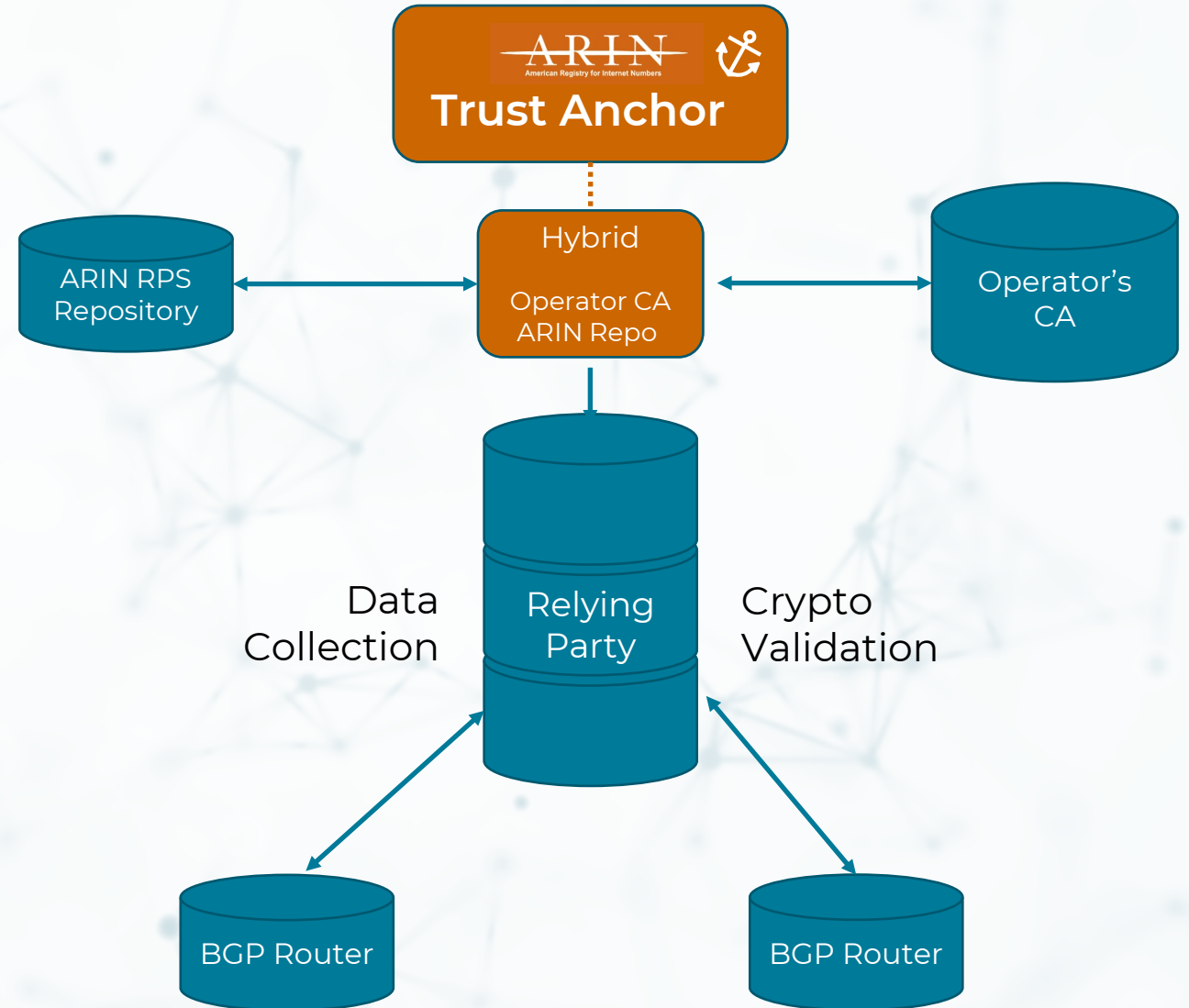




Repository Publication Service (Hybrid RPKI)

- Maintain control and independence of Delegated RPKI
- Runs their own CA to manage object signing
- Off-load Repository and Publication services to ARIN

* Suggested for organizations that wish to retain cryptographic control, and do not want to maintain the high availability repository and publication functions





Before Getting Started



IPv4 or IPv6 number resources allocated to your organization by ARIN



Autonomous System Number



A signed RSA or LRSA (RPKI Terms of Service if needed)



Your user account needs to be associated with the org as the Admin, Tech, or Routing Point of Contact (POC)



RPKI Feature Improvements

No ROA signing requirement

- No more keys
- Simplified input
- Streamlined process

ROA auto-renew

- ROAs do not expire
- 90-day lifespan, renew at 10 days remaining
- True for Web IU and New API ROAs

New RESTful API

- 'Atomic' updates
- Multiple add/delete actions in one API call
- Legacy API still supported
- **Legacy API ROAs do not auto-renew**

A faint, light blue network diagram is visible in the background, consisting of several interconnected nodes and lines, resembling a constellation or a data network. The nodes are small circles, and the lines are thin, connecting them in a non-linear fashion.

Stand Up For Your Routes!

Stand Up for Your Routes!

Creating ROAs for your resources benefits more than just you but also operators who make decisions based on RPKI validity state

There are documented cases where RPKI has been proven to interrupt hijack attempts before they become impactful

Growing number service providers require you to create ROAs for your resources before a business relationship is established

Ongoing standards work in the IETF is defining new features and use cases for the RPKI

RPKI Questions For ARIN?

Call the ARIN Helpdesk

+1.703.227.0660

From the User Dashboard

- Select Ask ARIN
- "Chat with us!"

Routing Security Team
routing.security@arin.net

ANY QUESTIONS

?

Thank You



Simplified Navigation

ARIN [Feedback](#) 14 Welcome, SPO

ACCOUNT MANAGER

- Dashboard**
- Tickets
- Your Records
- IP Addresses
- ASNs
- Routing Security**
- RPKI
Get Resource Certificate or Manage ROAs
- IRR
Manage Your Objects
- Transfer Resources
- Payments & Billing
- Downloads & Services
- Ask ARIN
Create a help desk ticket

Dashboard

Alerts

You have **14 unread messages.**

Account Snapshot

2 Point of Contact records (POCs)	2 Organization Identifiers (Org IDs)
3 Networks (NETs)	2 Autonomous System Numbers (ASNs)

What's New With ARIN Online

Visit [ARIN Online Functionality](#) for an overview of all the functionality currently available within ARIN Online.

- Routing Security dropdown
- Fewer clicks to RPKI



Simplified Navigation

ARIN [Feedback](#) 3 Welcome, SPO

ACCOUNT MANAGER

- Dashboard
- Tickets
- Your Records
- IP Addresses
- ASNs
- Routing Security
- RPKI**
Get Resource Certificate or Manage ROAs
- IRR
Manage Your Objects
- Transfer Resources
- Payments & Billing
- Downloads & Services
- Ask ARIN
Create a help desk ticket

Manage RPKI

ARIN's Resource Public Key Infrastructure (RPKI) service allows users to publish authorized routes for their certified Internet number resources to help secure Internet routing.

For more information about RPKI, visit [Resource Certification](#).

Your Organizations

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

Org ID	Certification Status	Action
ARIN-2	No Direct Resources	Ask ARIN
ARINL	Eligible	Sign up for RPKI

ARIN's RPKI Trust Anchor Locator (TAL)

Relying party software (validator) must incorporate the ARIN TAL to fetch data from ARIN's RPKI repository.

[Access RPKI TAL](#)

- List of all Linked Orgs
- Certification Status



Hosted or Delegated RPKI

ARIN [Feedback](#) 3 Welcome, SPO

ACCOUNT MANAGER

- Dashboard
- Tickets
- Your Records
- IP Addresses
- ASNs
- Routing Security
 - RPKI**
Get Resource Certificate or Manage ROAs
 - IRR
Manage Your Objects
- Transfer Resources
- Payments & Billing
- Downloads & Services
- Ask ARIN
Create a help desk ticket

Manage RPKI

Org ID: **ARINL**

ARIN's Resource Public Key Infrastructure (RPKI) service allows you to publish authorized originations for your routes to help secure Internet routing.

Choose Between Two Models of RPKI

Hosted RPKI

Use ARIN's infrastructure to create and manage your ROAs. [Learn more about Hosted RPKI.](#)

- Uses ARIN's CA and repository
- You can start right away
- Create ROAs with a simple web form
- ROAs are automatically renewed
- You can also automate with ARIN's [Reg-RWS API](#)

[Sign up for Hosted](#)

Delegated RPKI

Run your own Certificate Authority (CA) to create and manage your ROAs. [Learn more about Delegated RPKI.](#)

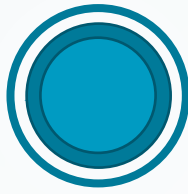
- Use your CA
- To start, get the [Child Request XML](#) from your CA software
- Run your own publication server **or** use [ARIN's Publication Service](#)

[Sign up for Delegated](#)

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.

For more information about RPKI, visit [Resource Certification](#).

- Formerly a ticketed process
- Required RSD action to complete



One-Step Signup

ARIN [Feedback](#) 3 Welcome, SPO

ACCOUNT MANAGER

- Dashboard
- Tickets
- Your Records
- IP Addresses
- ASNs
- Routing Security
- RPKI**
Get Resource Certificate or Manage ROAs
- IRR
Manage Your Objects
- Transfer Resources
- Payments & Billing
- Downloads & Services
- Ask ARIN
Create a help desk ticket

Manage RPKI

✓ Success! Your organization is now enrolled in RPKI.

Org ID: Hosted RPKI: [Overview](#) [ROAs](#) [Certified Resources](#)

Choose the item you want to access, or create a new Route Origin Authorization (ROA).
For more information about RPKI, visit [Resource Certification](#).

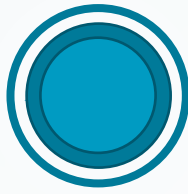
Status Overview

Last Updated: 04-25-2023
[Current Certificate](#)

Certified Resources: [2 ASNs](#), [3 Nets](#)
ROAs: [0](#)

[Create ROA](#)

- Resource certificate is automatically created (covered by RSA/LRSA)
- Ready to create ROAs



Create Your ROA By Fill In The Blank

ARIN [Feedback](#) 3 Welcome, SPO

ACCOUNT MANAGER

- Dashboard
- Tickets
- Your Records
- IP Addresses
- ASNs
- Routing Security
- RPKI**
Get Resource Certificate or Manage ROAs
- IRR
Manage Your Objects
- Transfer Resources
- Payments & Billing
- Downloads & Services
- Ask ARIN
Create a help desk ticket

RPKI: Create ROA

Org ID: ARINL Hosted RPKI: [Overview](#) [ROAs](#) [Certified Resources](#)

Create route origin authorizations (ROAs) for the resources covered by your RPKI certificate.

Create a Route Origin Authorization (ROA)

* denotes required field

*Origin AS:

	Prefix	Max Length
*Prefixes:	<input type="text" value="149.112.152.0/24"/>	<input type="text" value="24"/>
	<input type="button" value="+ Additional Prefix"/>	

ROA Name:

Optional: Provide a helpful nickname, such as DDOS_Mitigation

Next Step

- No Validity Dates
- No ROA signing keys



ROAs are Evergreen

ARIN [Feedback](#) 3 Welcome, SPO

ACCOUNT MANAGER

- Dashboard
- Tickets
- Your Records
- IP Addresses
- ASNs
- Routing Security
- RPKI**
Get Resource Certificate or Manage ROAs
- IRR
Manage Your Objects
- Transfer Resources
- Payments & Billing
- Downloads & Services
- Ask ARIN
Create a help desk ticket

RPKI: Create ROA

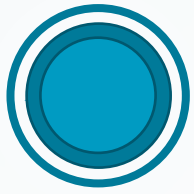
Org ID: ARINL Hosted RPKI: [Overview](#) [ROAs](#) [Certified Resources](#)

Review ROA

Origin AS: 399970
Prefixes: 149.112.152.0/24 Max Length 24
Auto-renewing: Yes

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

- Auto Renewing ROAs!
- All ROAs created in UI switch to auto-renew



Create More ROAs

ARIN [Feedback](#) 3 Welcome, SPO

ACCOUNT MANAGER

- Dashboard
- Tickets
- Your Records
- IP Addresses
- ASNs
- Routing Security
- RPKI**
Get Resource Certificate or Manage ROAs
- IRR
Manage Your Objects
- Transfer Resources
- Payments & Billing
- Downloads & Services
- Ask ARIN
Create a help desk ticket

RPKI: ROAs

✓ ROA for 'AS399970 149.112.152.0/24 Max Length 24' was saved successfully. It will be available in ARIN's publication repository within 24 hours.

Org ID: Hosted RPKI: [Overview](#) **ROAs** [Certified Resources](#)

The Org ID has the following Route Origin Authorizations (ROAs) in ARIN's RPKI Repository.

Route Origin Authorizations

Filter ROAs by Origin AS or Prefix.

Resource: [Search ROAs](#)

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

[Create ROA](#)

Origin AS	Prefixes	ROA Name
399970	149.112.152.0/24 Max Length: 24	Manage ROA

- Confirm ROA creation
- Direct return to ROA list
- One click to create more ROAs