

Stand Up For Your Routes!

Using the Resource Public Key Infrastructure (RPKI)

Brad Gorman

Senior Product Owner, Routing Security - ARIN

What's Being Covered Today

- Security of the Early Internet
- The Goal of the RPKI
- Current RPKI Deployment
- RPKI Services and Development

Security of the Early Internet

BGP Routing on the 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)

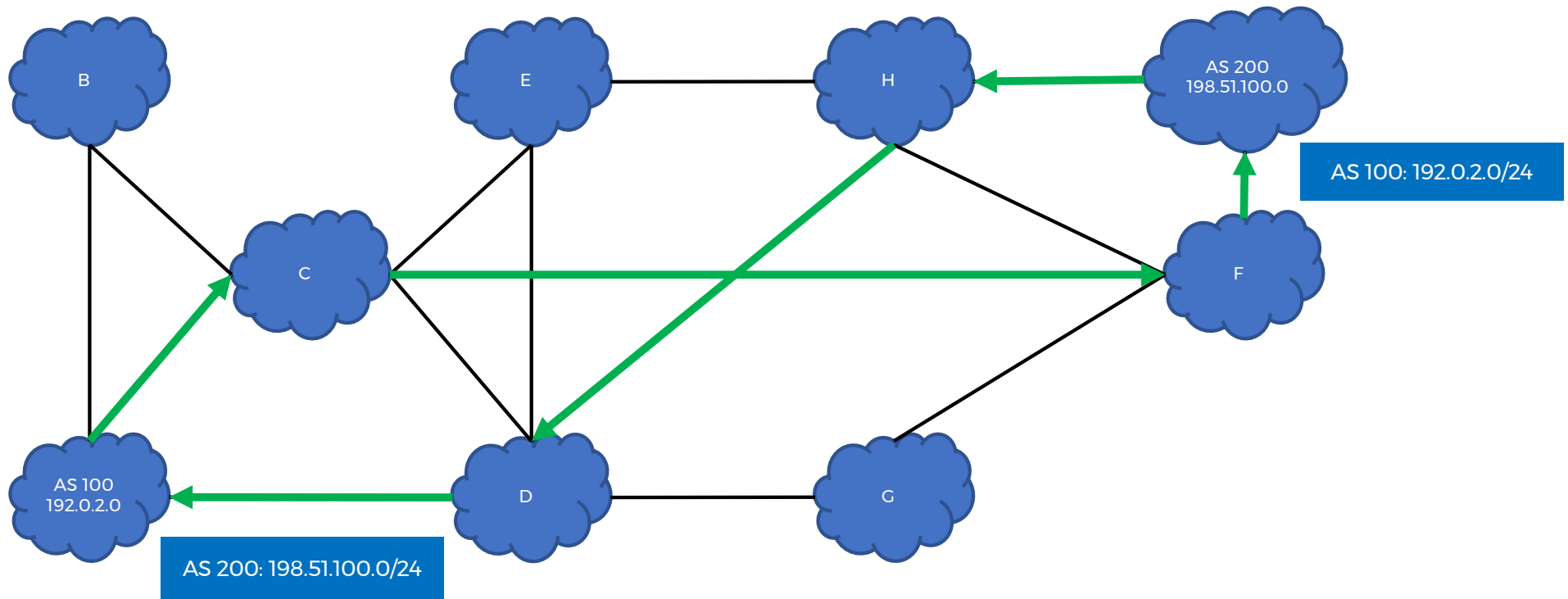
- RPSL is a standard language used by Internet Service Providers to build security policy on network devices
- Internet Routing Registry (IRR) is an ecosystem of databases where operators can share information about their policies
- ARIN authenticates entries in our database, confirming the rightful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

The Goal of the RPKI

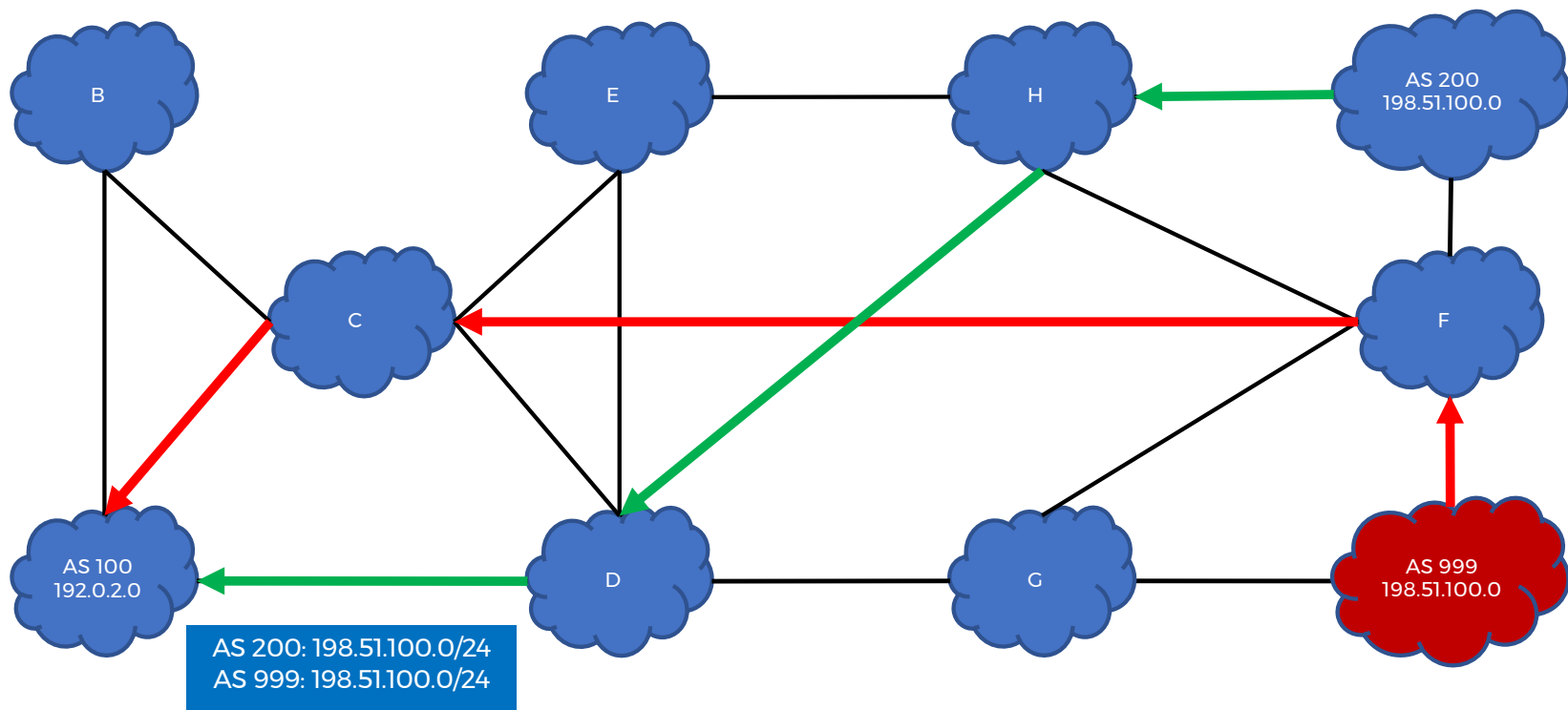
The Goal of the RPKI

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

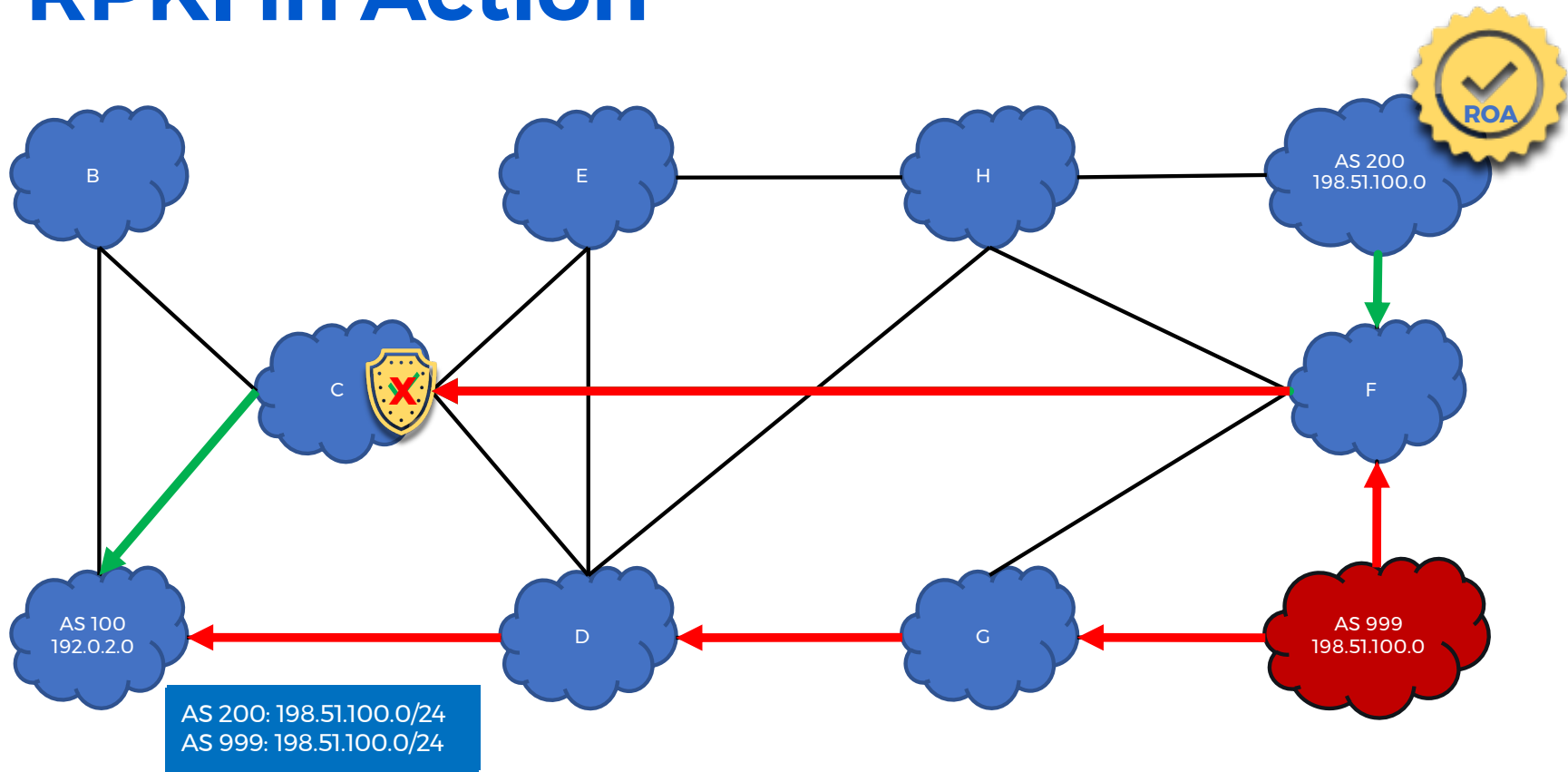
Internet is More Complex Today



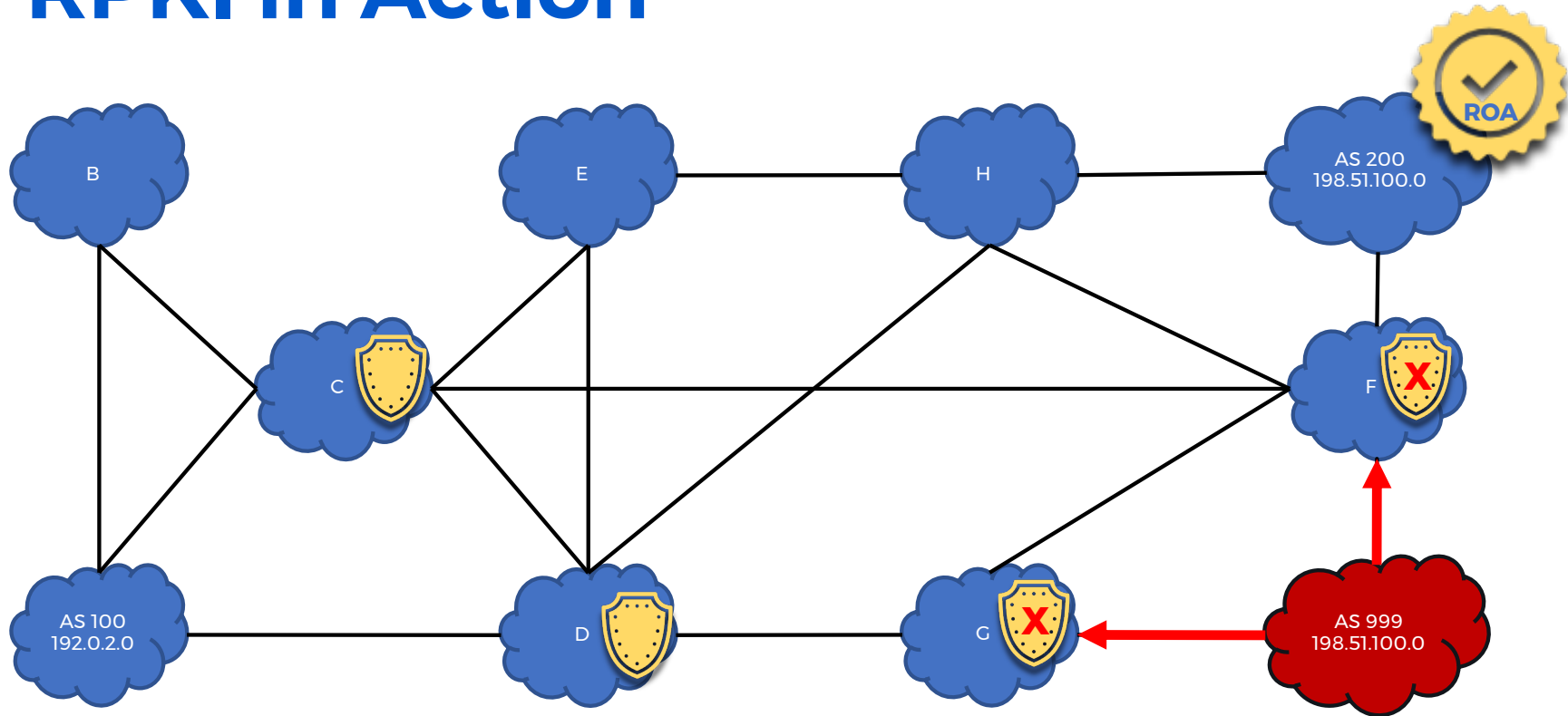
Bad Actors Will Find a Way



RPKI in Action



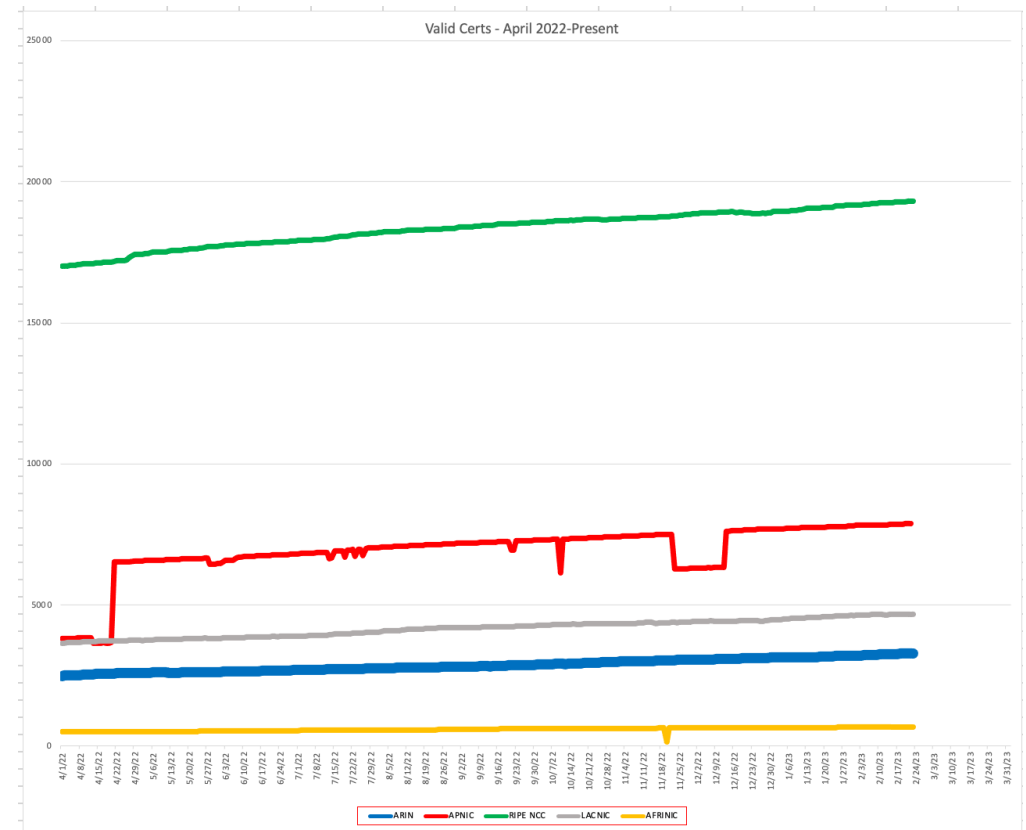
RPKI in Action



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**



RPKI ROAs – Covered Prefixes

- Hosted Repository
 - Route Origin Authorizations (ROAs)
53,912
 - Validated ROA Payloads (VRPs*)
65,581
- RPS (Hybrid) Repository
 - ROAs - **1,073**
 - VRPs - **2,892**

* VRPs identify an IP prefix, a maximum length, and an origin AS number derived from a validated ROA, (verified by ARIN to contain authoritative data).



RPKI Valid Route Announcements

- **28.91%** of Internet routes with ARIN IPv4 resources marked as RPKI Valid*
 - **Up 6.5%** year over year
- **47.88%** of Internet routes with ARIN IPv6 resources marked as RPKI Valid*
 - **Up 4.2%** year over year

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

RPKI Valid IP Resources

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

- 508M / 1.12B (eligible)
- **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!



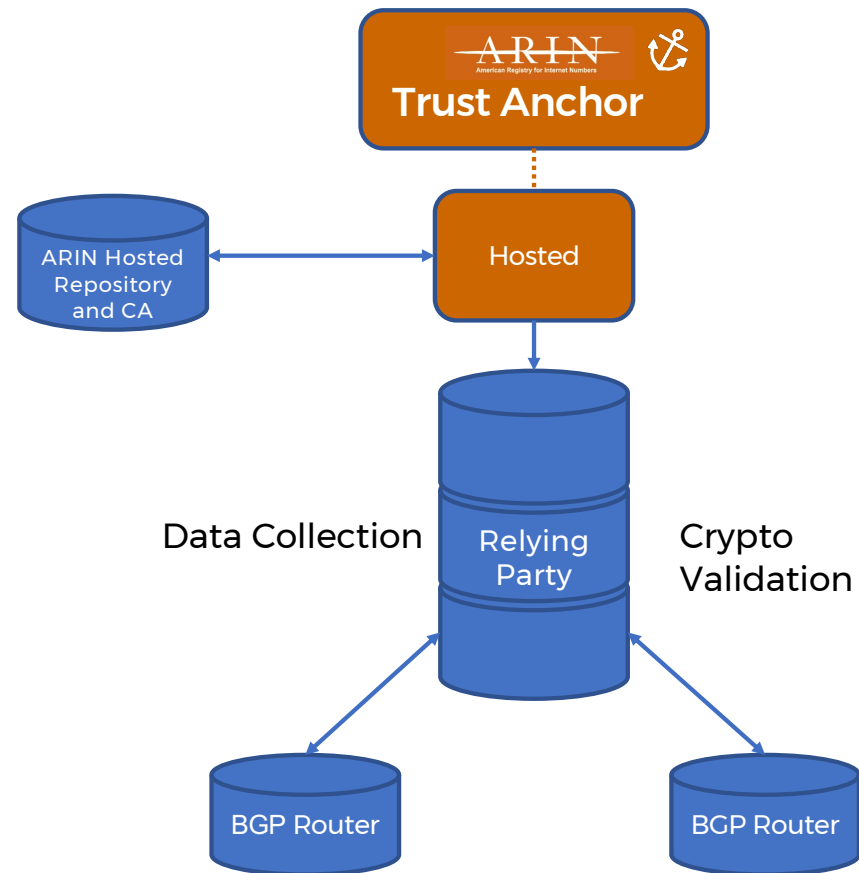
RPKI Services and Development



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

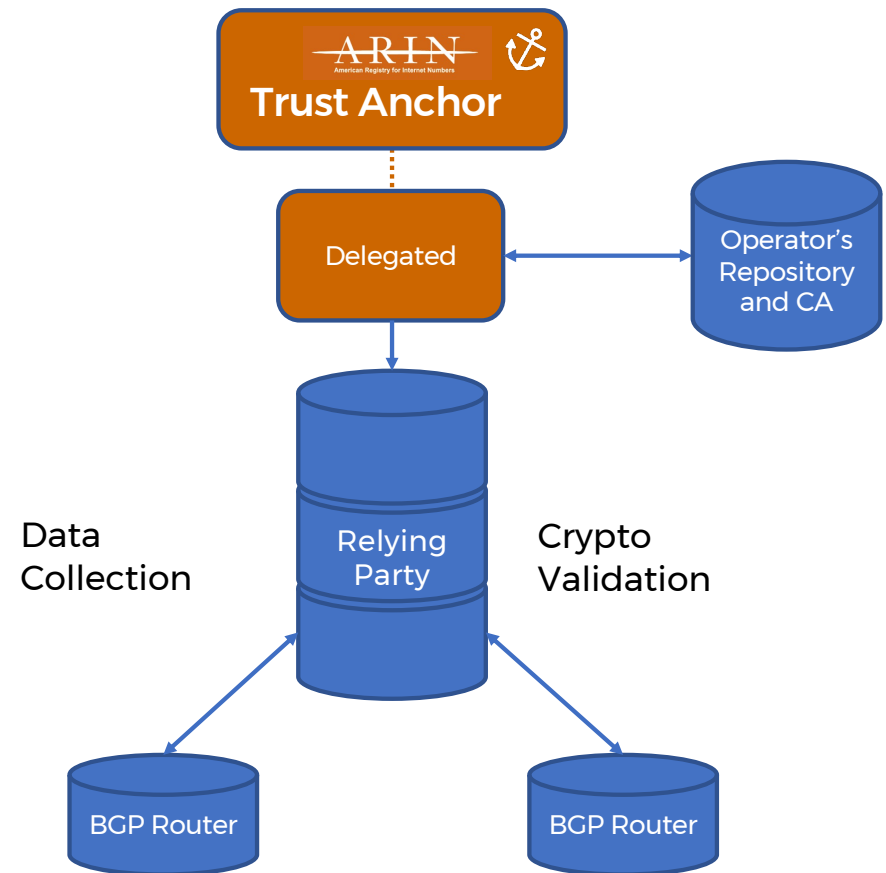
* Easiest to use; Recommended for most organizations just getting started with RPKI. Nearly 98% of ARIN participants use Hosted RPKI.



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

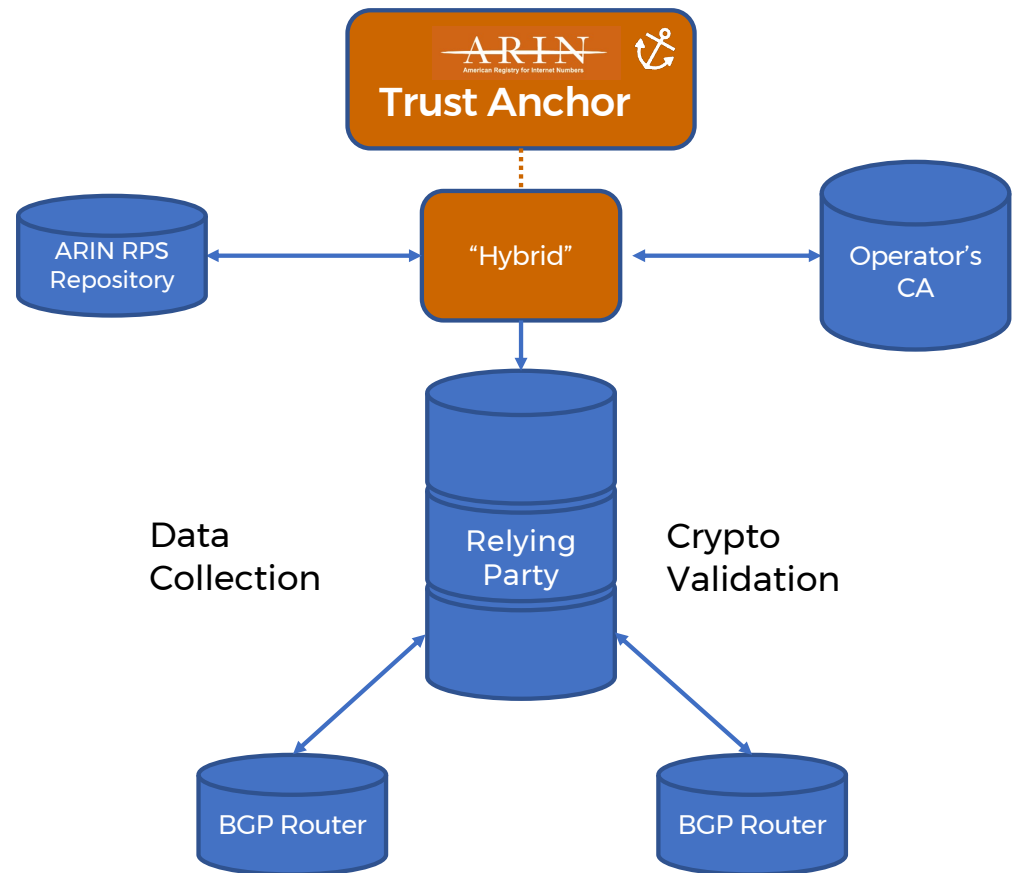
* Highest responsibility and uptime requirement; only organizations with in-depth knowledge of RPKI and resources to run a Certificate Authority (CA) and a publication server, should select Delegated RPKI.



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 ToS if needed)



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

Keys no longer required to sign ROAs!

Simplified Navigation

ARIN Feedback 3 Welcome, SPO

ACCOUNT MANAGER


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](#)

RPKI
Get Resource Certificate or Manage ROAs

IRR
Manage Your Objects

Transfer Resources

Payments & Billing

Downloads & Services

Ask ARIN
Create a help desk ticket

- 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

The screenshot shows the ARIN Account Manager interface. At the top, there is a navigation bar with the ARIN logo, a home icon, a 'Feedback' button, a notification bell with '3' alerts, and a user profile for 'Welcome, SPO'. The main content area is titled 'Manage RPKI'. On the left is a sidebar menu under 'ACCOUNT MANAGER' with items: Dashboard, Tickets, Your Records, IP Addresses, ASNs, Routing Security, RPKI (highlighted), IRR, Transfer Resources, Payments & Billing, Downloads & Services, and Ask ARIN. The RPKI section is active, displaying a green success message: 'Success! Your organization is now enrolled in RPKI.' Below this, there is a dropdown for 'Org ID' set to 'ARINL', and 'Hosted RPKI' tabs for 'Overview', 'ROAs', and 'Certified Resources'. A text prompt asks to 'Choose the item you want to access, or create a new Route Origin Authorization (ROA)'. A link for 'Resource Certification' is provided. The 'Status Overview' section shows 'Last Updated: 04-25-2023' with a link to 'Current Certificate', 'Certified Resources: 2 ASNs, 3 Nets', and 'ROAs: 0'. A 'Create ROA' button is located at the bottom right of the status overview.

- 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"/>




ROA Name:

Optional: Provide a helpful nickname, such as DDOS_Mitigation



- 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

Back to Create More ROAs

ARIN Feedback 3 Welcome, SPO

ACCOUNT MANAGER **RPKI: ROAs**

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

Org ID: ARINL 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

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
- There are documented cases where RPKI has been proven to interrupt hijack attempts before they become impactful
- More service providers are requiring you 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



Thank you

