ARIN 52
POWERED BY PARTICIPATION

Routing Security Update

Brad Gorman | *Senior Product Owner, Routing Security*

Agenda

- Resource Public Key Infrastructure (RPKI) overview
- ARIN's RPKI services
- RPKI adoption at ARIN
- New features and upcoming development

RPKI Overview

What is RPKI?

RPKI provides a cryptographically signed method for an Internet number resource holder to make an authoritative statement about the origin of a prefix(s) announced to the Internet.

Benefits of RPKI

- Provides operators another data set to make more informed routing decisions
- Protects resource holders from impact resulting from human error or nefarious activity
- Reduces the overall attack surface for attempted hijacks on the greater Internet

RPKI Services

Key Terms

Trust Anchor

An established point of trust from which an entity begins the validation of cryptographic objects in the RPKI repository.

Route Origin Authorization (ROA)

A signed statement made by the authorized resource holder that contains an origin Autonomous System Number, a prefix, and an optional maxLength value.

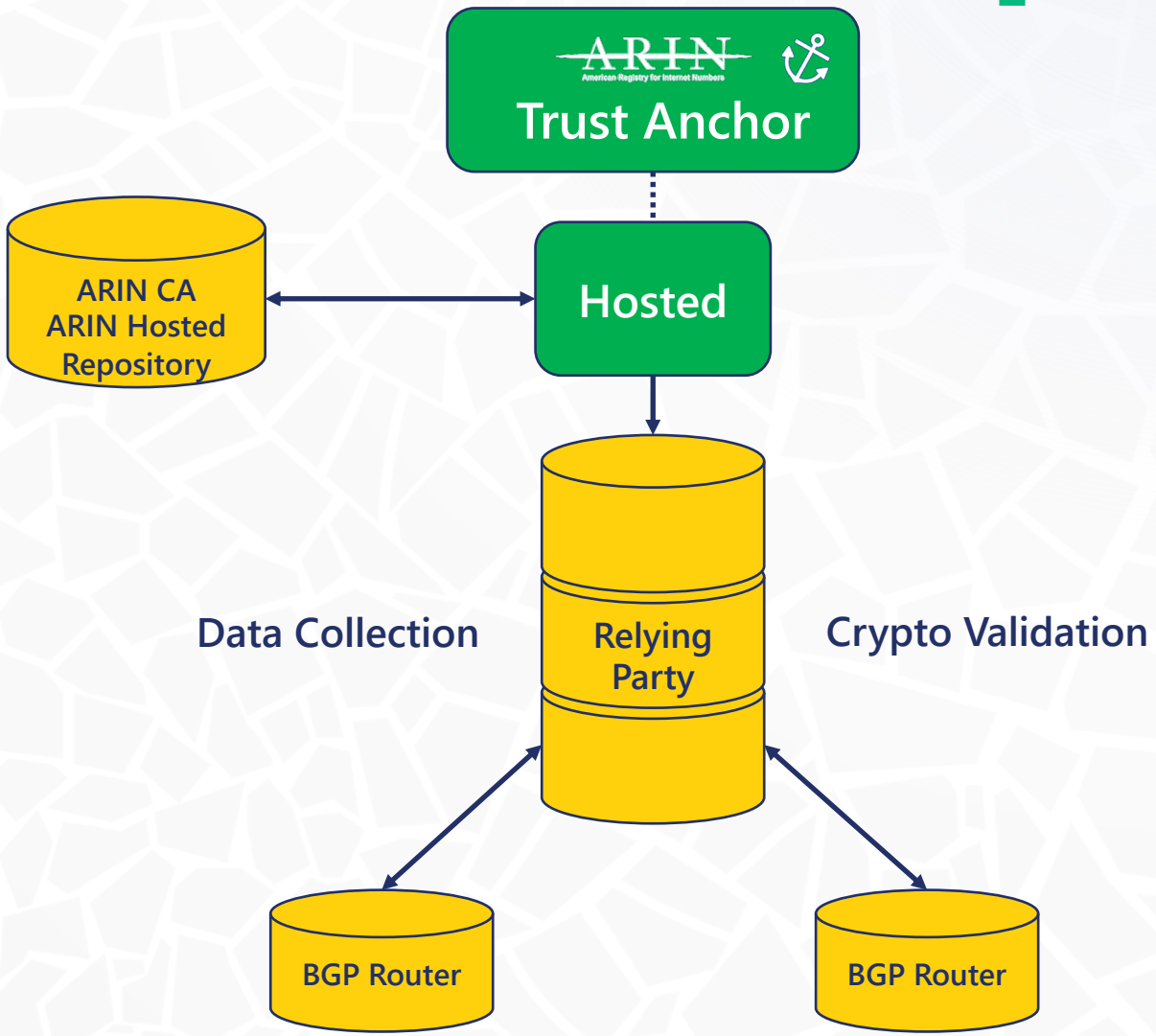
Relying Party Software

Open source software, otherwise known as a validator, confirms the chain of trust for all published objects in a RPKI repository, then stores the validated data into its cache.

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

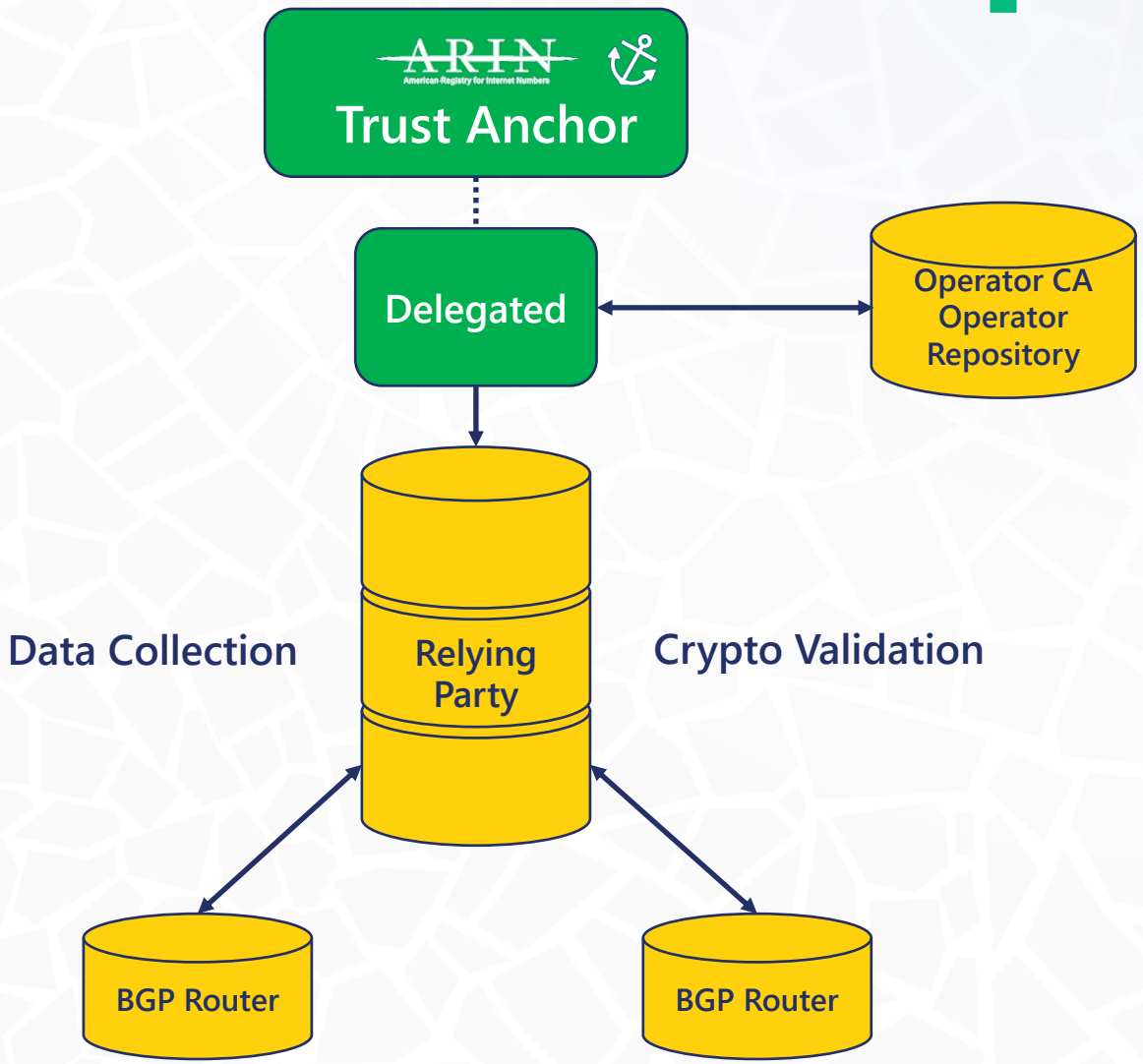
Easiest to use! Recommended for most organizations just getting started with RPKI. Nearly 98% of ARIN participants use Hosted RPKI.



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

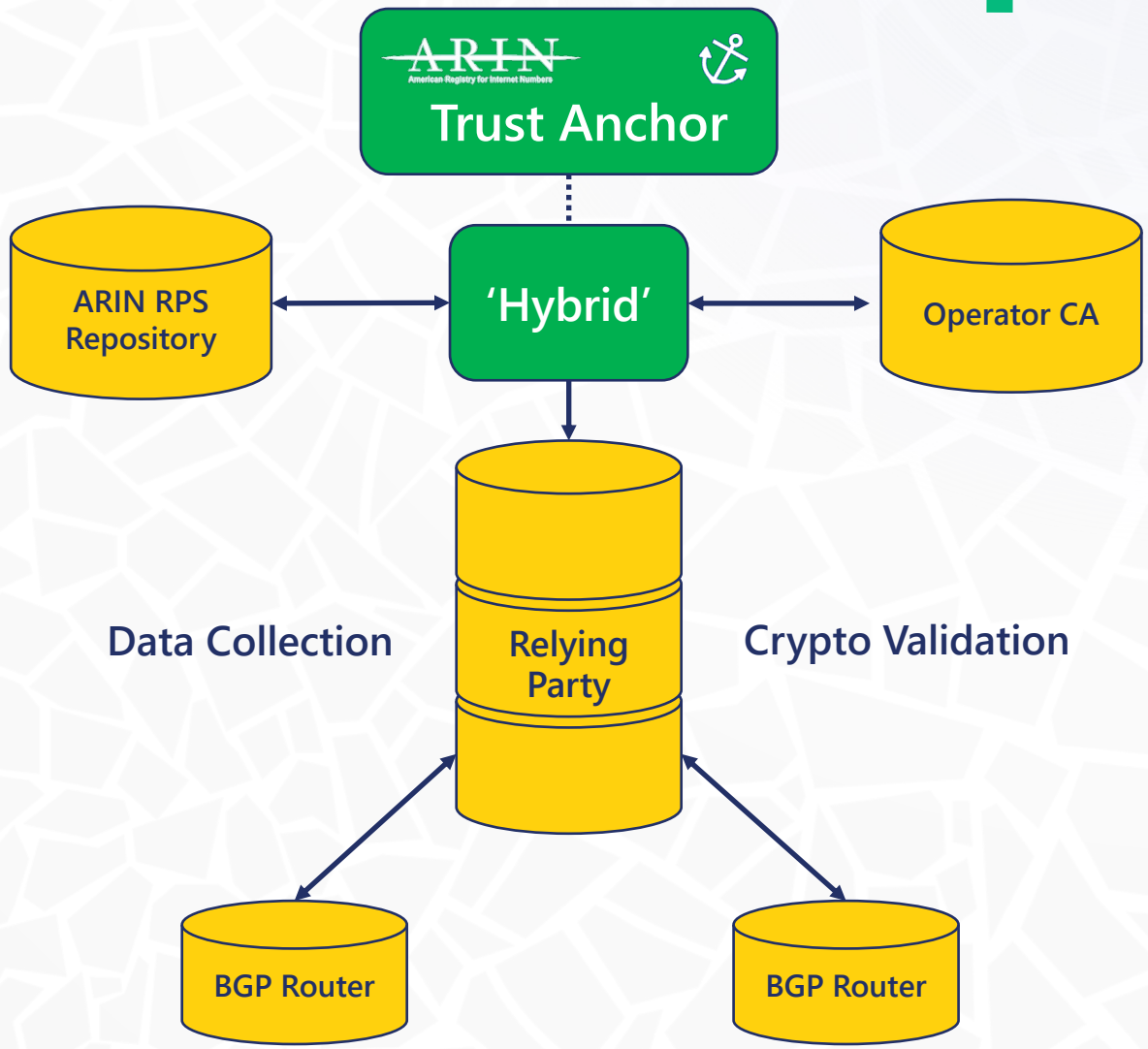
Highest responsibility and uptime requirement: Only organizations with in-depth knowledge of RPKI and resources to run a CA and a publication server should select Delegated RPKI.



Repository Publication Service (RPS)

- 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 but do not want to maintain the high availability repository and publication functions

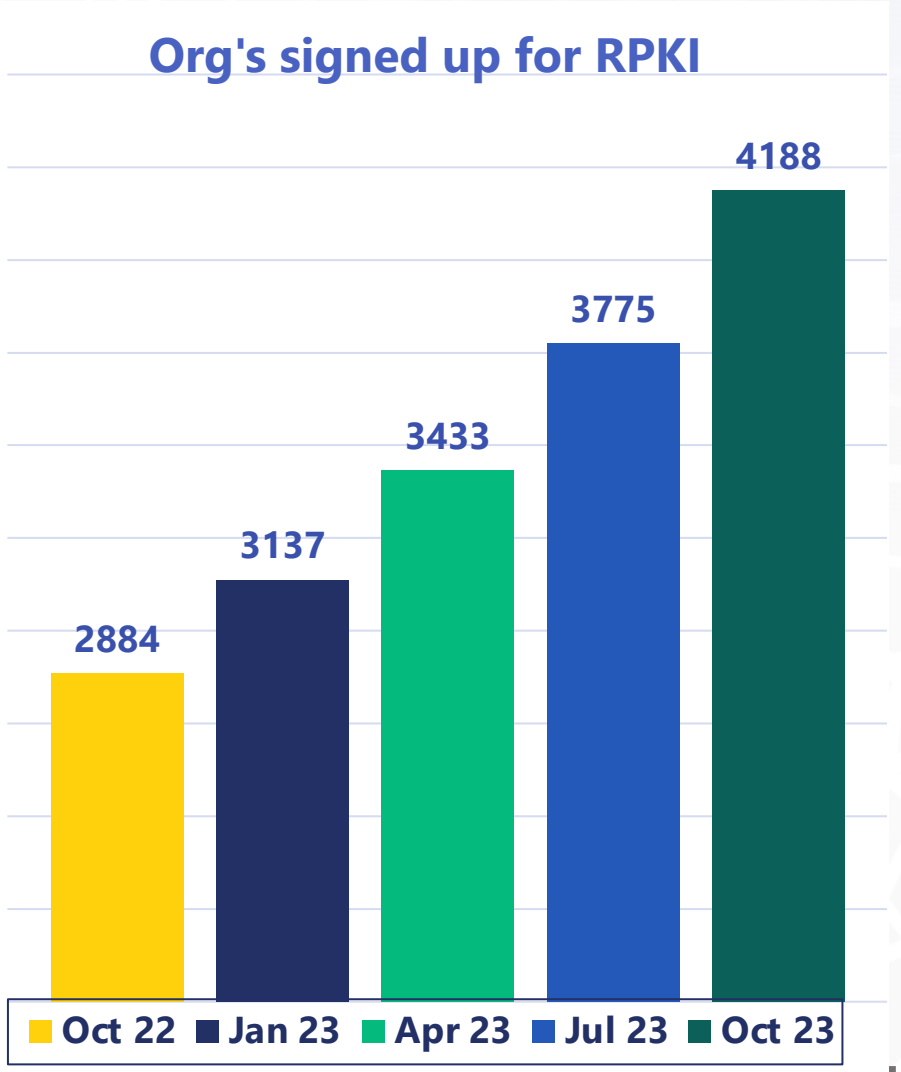


RPKI Adoption

RPKI Adoption – Org Participation

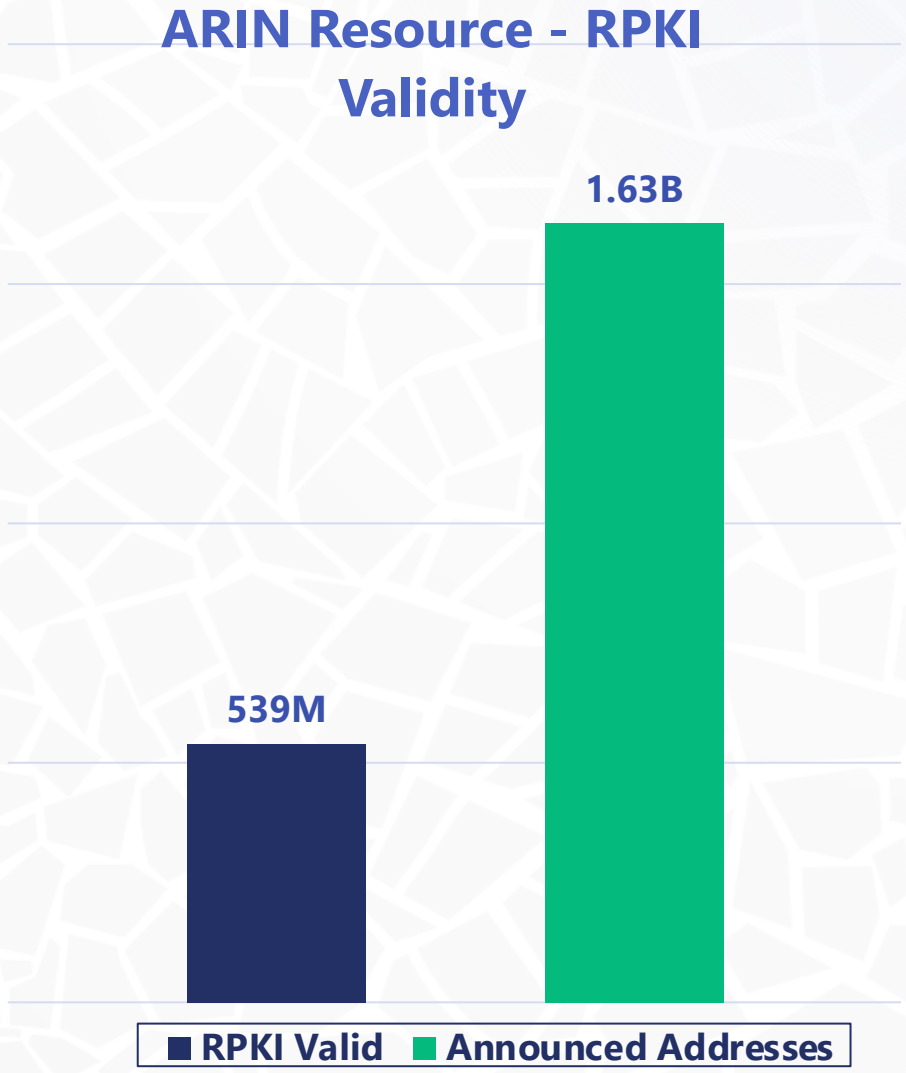
23.9% of Orgs registered to use ARIN's RPKI services

- Hosted – **4078**
- Delegated – **110**
- Repository Service (Hybrid) – **17**



RPKI Adoption – Address Coverage

33.1% of ARIN-allocated IPv4 space announced to the Internet is marked RPKI valid



New Features and Upcoming Development

Features Delivered Since ARIN 51

New RESTful API

- Atomic updates, multiple actions in single call

ROA auto-renewal

- 90-day lifespan, renew at 80 days
- ROAs created with 2014 API **DO NOT** auto-renew, must be regenerated

Resource Cert reroll automated

- New allocation or transfer
- Transfer out can impact RPKI deployment

Eligibility Matrix

- Visual confirmation of privileges based on Point of Contact role

RPKI/IRR Integration Consultation Outcome

Organizations in ARIN Online will have the ability to set an Organizational default for automatic creation of managed Route Objects for RPKI ROAs.

- The default setting of this feature will be “On” (i.e., to create auto-managed Route Objects when creating ROAs).
- Users will be able to opt in or opt out of the creation of a managed Route Object at individual ROA creation time without changing the Organization level setting.
- This default setting will not apply to existing ROAs at autorenewal.

All auto-managed Route Objects will be identified as such in a remark field on the object.

At ROA creation, there will be a check to see if there is an existing, matching, and unmanaged Route Object. If so, the user will have the option to replace it with an auto-managed Route Object or continue and leave the unmanaged Route Object in place.

RPKI/IRR Integration Consultation Outcome

Auto-managed Route Objects resulting from ROA creation will not consider the maxLength value and use the prefix entry only (least specific match) as recommended in RFC 9319/BCP 185. ROAs with multiple prefixes will create an auto-managed Route Object for each prefix. Users may manually create longer match IRR objects, and these manually created objects will not be auto-managed.

Deleting a ROA will remove an auto-managed Route Object(s). A user can opt out of deleting a Route Object at individual ROA deletion without changing the Organization level setting. If a Route Object is separated from the associated ROA in this manner, it will no longer be auto-managed, and the corresponding notation about auto-management in the Route Object's remark field will be removed.

The API will be updated for Reg-RWS to reflect these new capabilities.

Development Pipeline

RPKI/ROA Intelligence

(ACSP 2022.30)

- Provide early warning of potential impact from ROA creation
- Show ROA validity state based on current Internet routing announcements

RPKI advanced features via ARIN Online interface

- Download full list of ROAs to a file for offline processing
- Accept ROA changes via file upload
- Add Functionality to Assist Customers Transitioning From Hosted to Delegated RPKI (ACSP 2022.26)

Thank You

Questions or Comments?