ARIN
American Registry for Internet Numbers

Securing Core Internet Functions – Resource Certification, RPKI

Mark Kosters
Chief Technology Officer

Core Internet Functions: Routing & DNS

- The Internet relies on two critical resources
  - DNS: Translates domain names to IP addresses and IP addresses to domain names
  - Routing: Tells us how to get to an IP address
- These critical resources <u>are not secure</u>
- DNSSEC and RPKI secure these critical resources

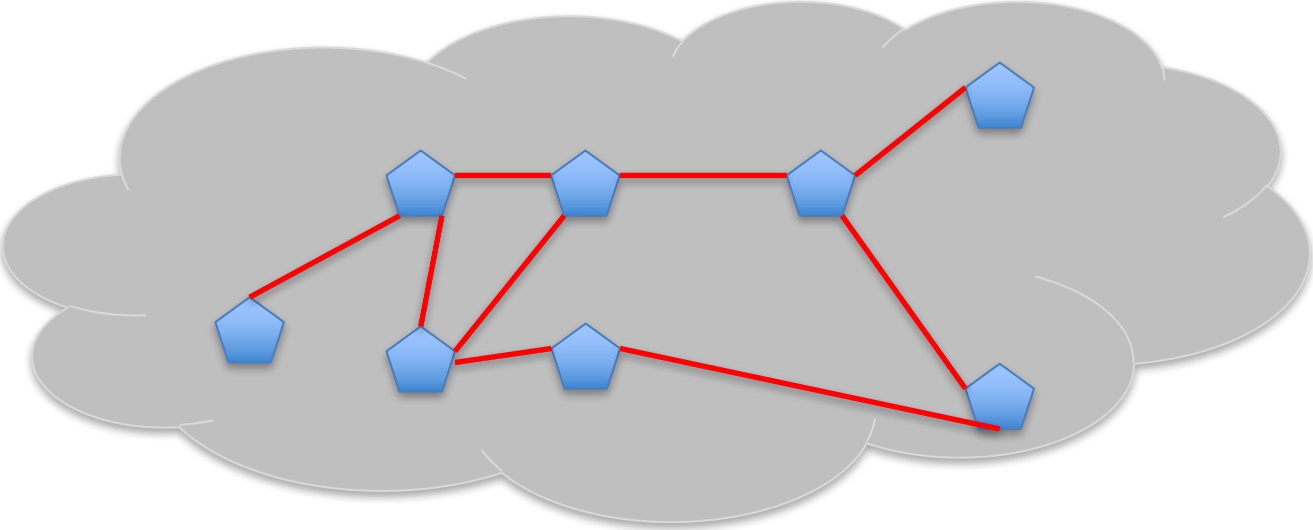
Routing – A Primer

Routing Architecture

- The Internet uses a *two level* routing hierarchy:
  - – Interior Gateway (Routing) Protocol - IGP
  - – Exterior Gateway (Routing) Protocol - EGP

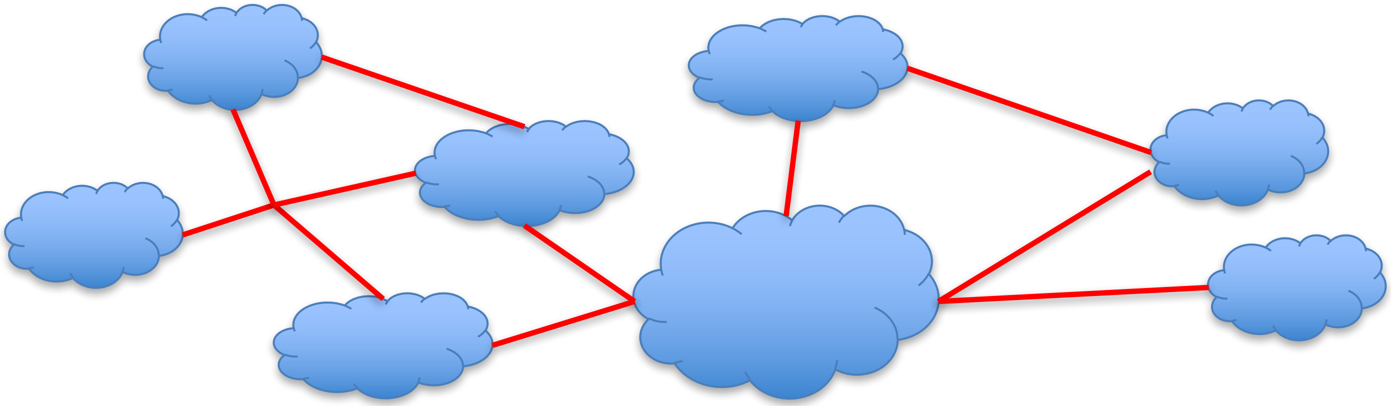
Routing Architecture

- IGP:
  - **Interior** Routing Protocols, used by each network to determine how to reach all destinations that lie within the network
  - **Interior** Routing protocols maintain the current topology of the network



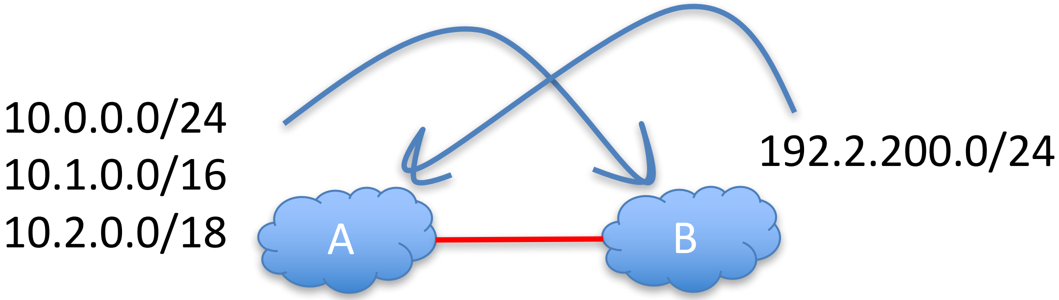
Routing Architecture

- EGP:
  - **Exterior** Routing Protocol, used to link each component network together into a single whole
  - **Exterior** protocols assume that each network is fully interconnected internally



Exterior Routing: BGP

- BGP is a large set of bilateral (1:1) routing sessions
  - A tells B all the destinations (prefixes) that A is capable of reaching
  - B tells A all the destinations that B is capable of reaching



10.0.0.0/24
10.1.0.0/16
10.2.0.0/18

192.2.200.0/24

Securing Routing With RPKI

What is RPKI?

- **R**esource **P**ublic **K**ey **I**nfrastructure
- Cryptographically certifies network resources
  - AS Numbers
  - IP Addresses
- Also certifies route announcements
  - Route Origin Authorizations (ROAs) allow you to authorize your block to be routed

Why is RPKI Important?

- Allows routers (or other processes) to validate routes
- Provides stronger validation than existing technologies, such as:
  - IRR registries
  - LOAs
  - or just "Seems legit"

Case Study: YouTube

- Pakistan Telecom was ordered to block YouTube
    - – Naturally, they originated their own route for YouTube’s IP address block
- YouTube’s traffic was temporarily diverted to Pakistan
- This incident could have been prevented with widespread adoption of RPKI

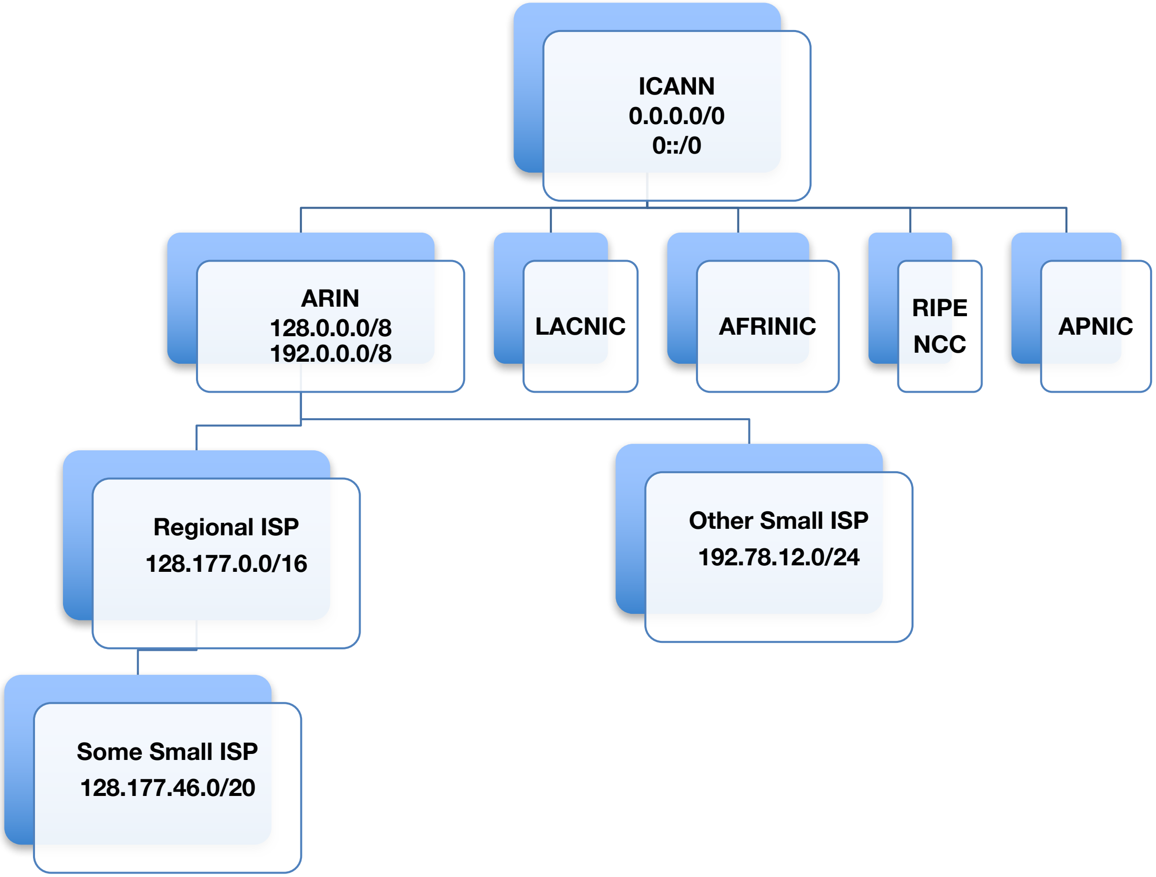
Case Study: Turk Telekom

- Turkish President ordered censorship of Twitter
- Turk Telekom's DNS servers were configured to return false IP addresses
  - So people started using Google's DNS (8.8.8.8)
- Turk Telekom hijacked Google's IP addresses in BGP
  - Could have been prevented with RPKI

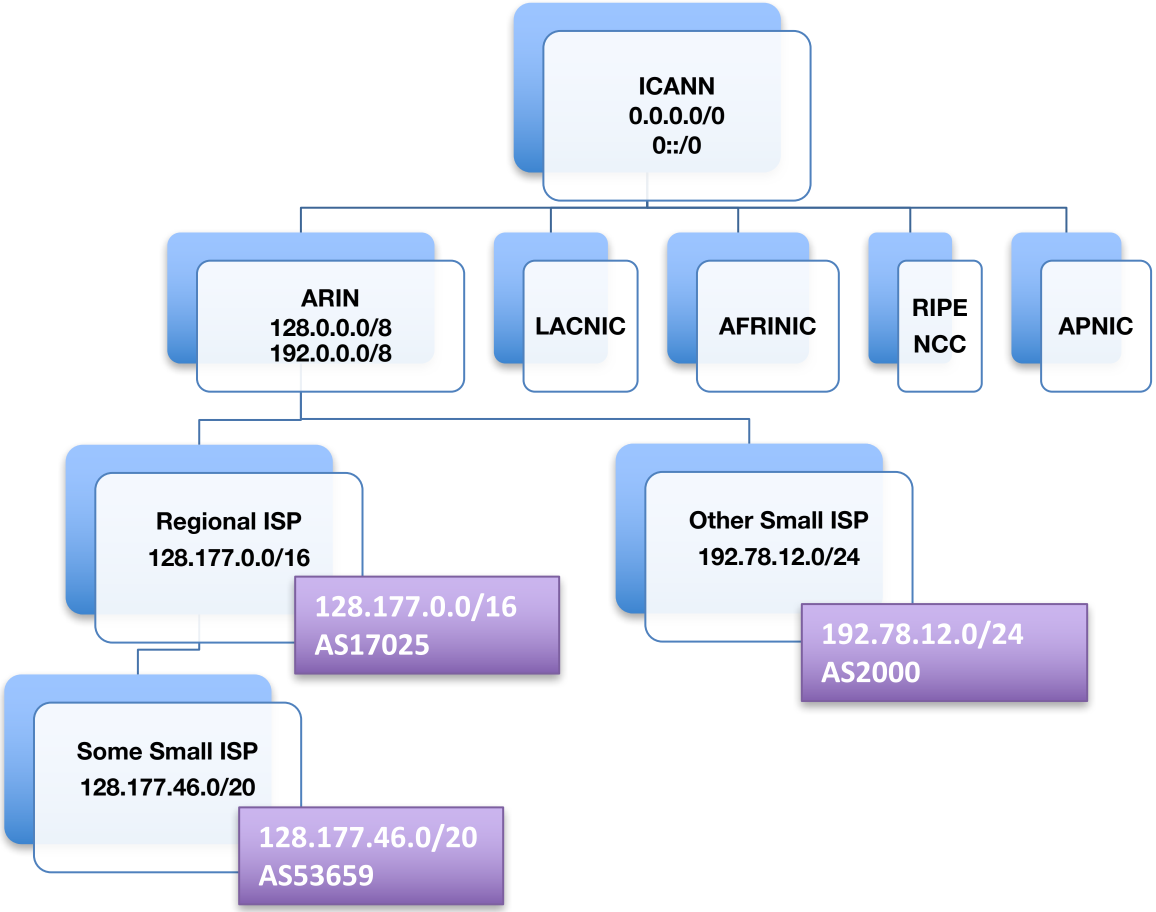
RPKI Basics

- All of ARIN's RPKI data is publicly available in a repository
- RFC 3779 certificates show who has each resource
- ROAs show which AS numbers are authorized to announce blocks
- CRLs show revoked records
- Manifests list all data from each organization

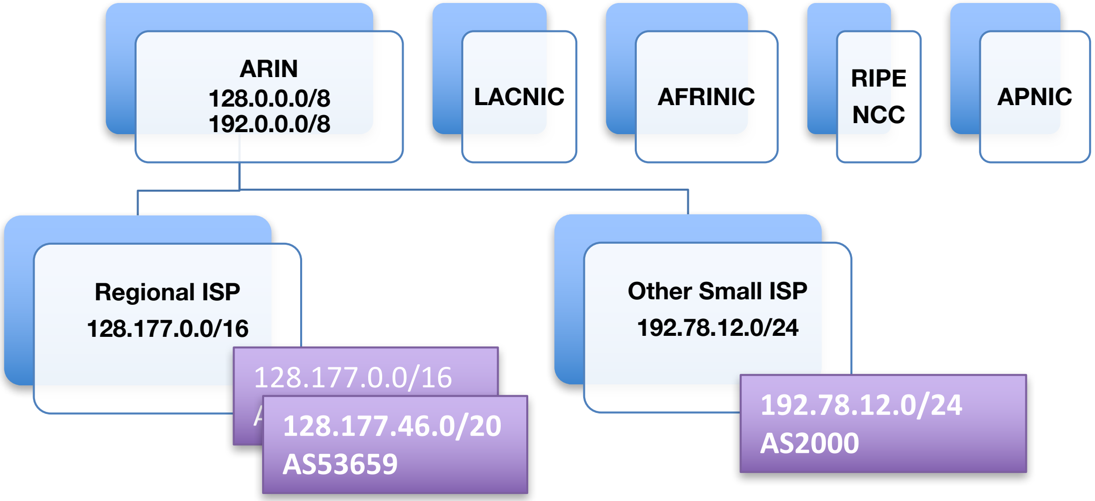
Hierarchy of Resource Certificates



Route Origin Authorizations



Current Practices



ARIN
128.0.0.0/8
192.0.0.0/8

LACNIC

AFRINIC

RIPE NCC

APNIC

Regional ISP
128.177.0.0/16

128.177.0.0/16
A

128.177.46.0/20
AS53659

Other Small ISP
192.78.12.0/24

192.78.12.0/24
AS2000

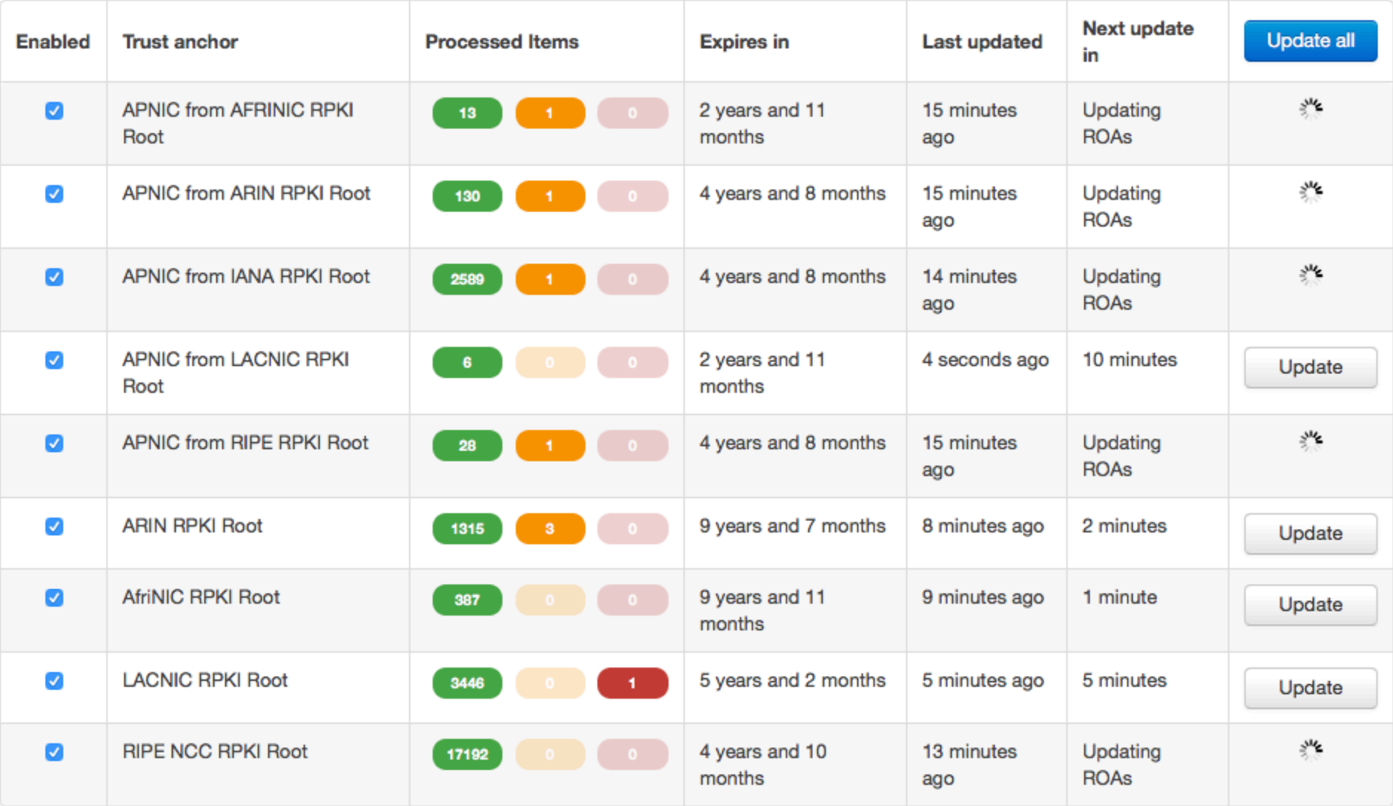
Using ARIN's RPKI Repository (Theory)

1. Pull down these files using a manifest-validating mechanism
2. Validate the ROAs contained in the repository
3. Communicate with the router to mark routes:
   - Valid
   - Invalid
   - unknown

Ultimately, the ISP uses local policy on how to route to use this information.

Using ARIN's RPKI Repository (Practice)

1. Get the RIPE NCC RPKI Validator



Enabled	Trust anchor	Processed Items	Expires in	Last updated	Next update in	Update all
☑	APNIC from AFRINIC RPKI Root	13 1 0	2 years and 11 months	15 minutes ago	Updating ROAs	
☑	APNIC from ARIN RPKI Root	130 1 0	4 years and 8 months	15 minutes ago	Updating ROAs	
☑	APNIC from IANA RPKI Root	2589 1 0	4 years and 8 months	14 minutes ago	Updating ROAs	
☑	APNIC from LACNIC RPKI Root	6 0 0	2 years and 11 months	4 seconds ago	10 minutes	Update
☑	APNIC from RIPE RPKI Root	28 1 0	4 years and 8 months	15 minutes ago	Updating ROAs	
☑	ARIN RPKI Root	1315 3 0	9 years and 7 months	8 minutes ago	2 minutes	Update
☑	AfriNIC RPKI Root	387 0 0	9 years and 11 months	9 minutes ago	1 minute	Update
☑	LACNIC RPKI Root	3446 0 1	5 years and 2 months	5 minutes ago	5 minutes	Update
☑	RIPE NCC RPKI Root	17192 0 0	4 years and 10 months	13 minutes ago	Updating ROAs	

Using ARIN's RPKI Repository (Practice, continued)

2. Get the ARIN TAL
   - https://www.arin.net/resources/rpki/tal.html
3. Plug it in to your routing policy engine:
   - Directly to the router via RTR protocol
   - Using custom scripts and the REST API
   - As RPSL route objects

Putting Your Routes in the RPKI

1. Determine if you want to allow ARIN to host your Certificate Authority (CA), or if you want ARIN to delegate to your Certificate Authority.
2. Sign up with ARIN Online.
3. Create Resource Certificates and ROAs.

Hosted vs. Delegated RPKI

- Hosted
  - – ARIN has done all of the heavy lifting for you
  - – Think “point click ship”
  - – Available via web site or RESTful interface
- Delegated using Up/Down Protocol
  - – A whole lot more work
  - – Might make sense for very large networks

Hosted RPKI - ARIN Online

- **Pros**
  - Easy-to-use web interface
  - ARIN-managed (buying/deploying HSMs, etc. is expensive and time consuming)
- **Cons**
  - Downstream customers can't use RPKI
  - Large networks would probably need to use the RESTful interface to avoid tedious management
  - We hold your private key

Delegated RPKI with Up/Down

- Pros
  - Allows you to keep your private key
  - Follows the IETF up/down protocol
  - Allows downstream customers to use RPKI
- Cons
  - Extremely hard to set up
  - Requires operating your own RPKI environment
  - High cost of time and effort

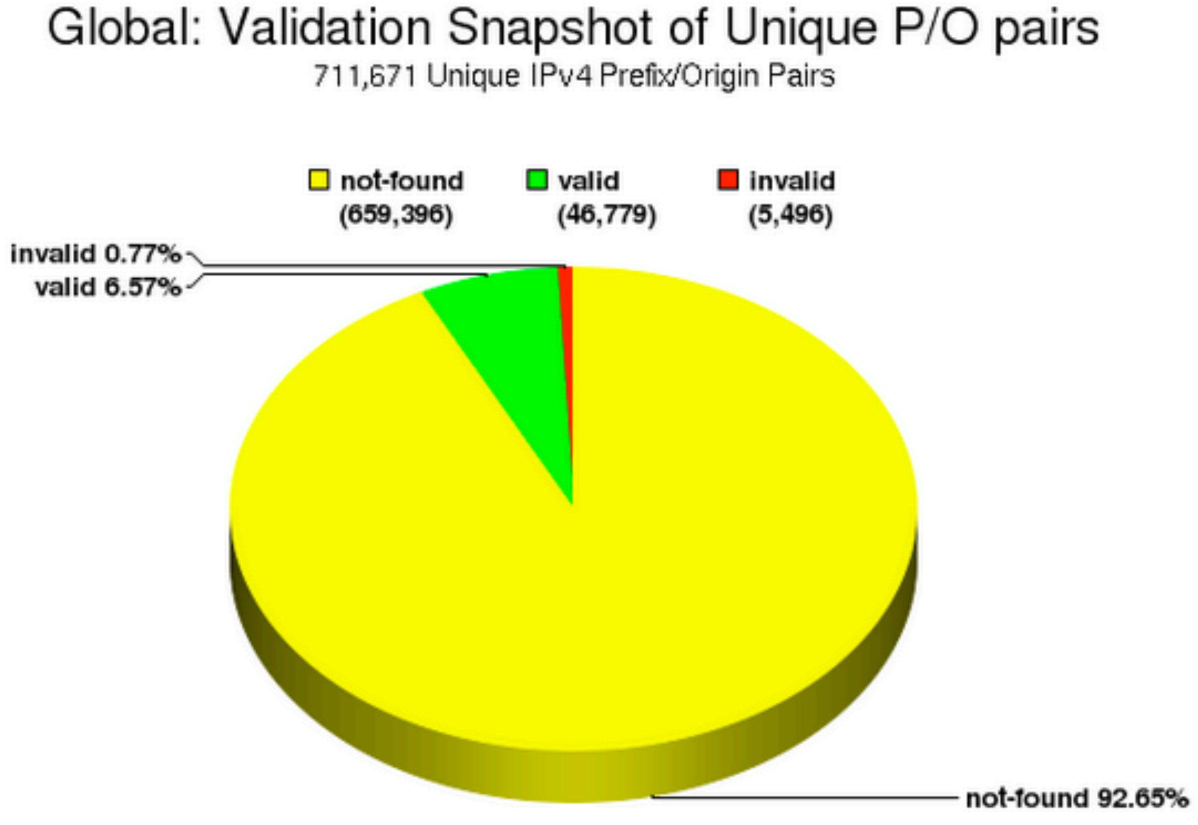
Delegated with Up/Down

- You have to do all the ROA creation
- Need to set up a Certificate Authority
- Have a highly available repository
- Create a CPS

RPKI Usage

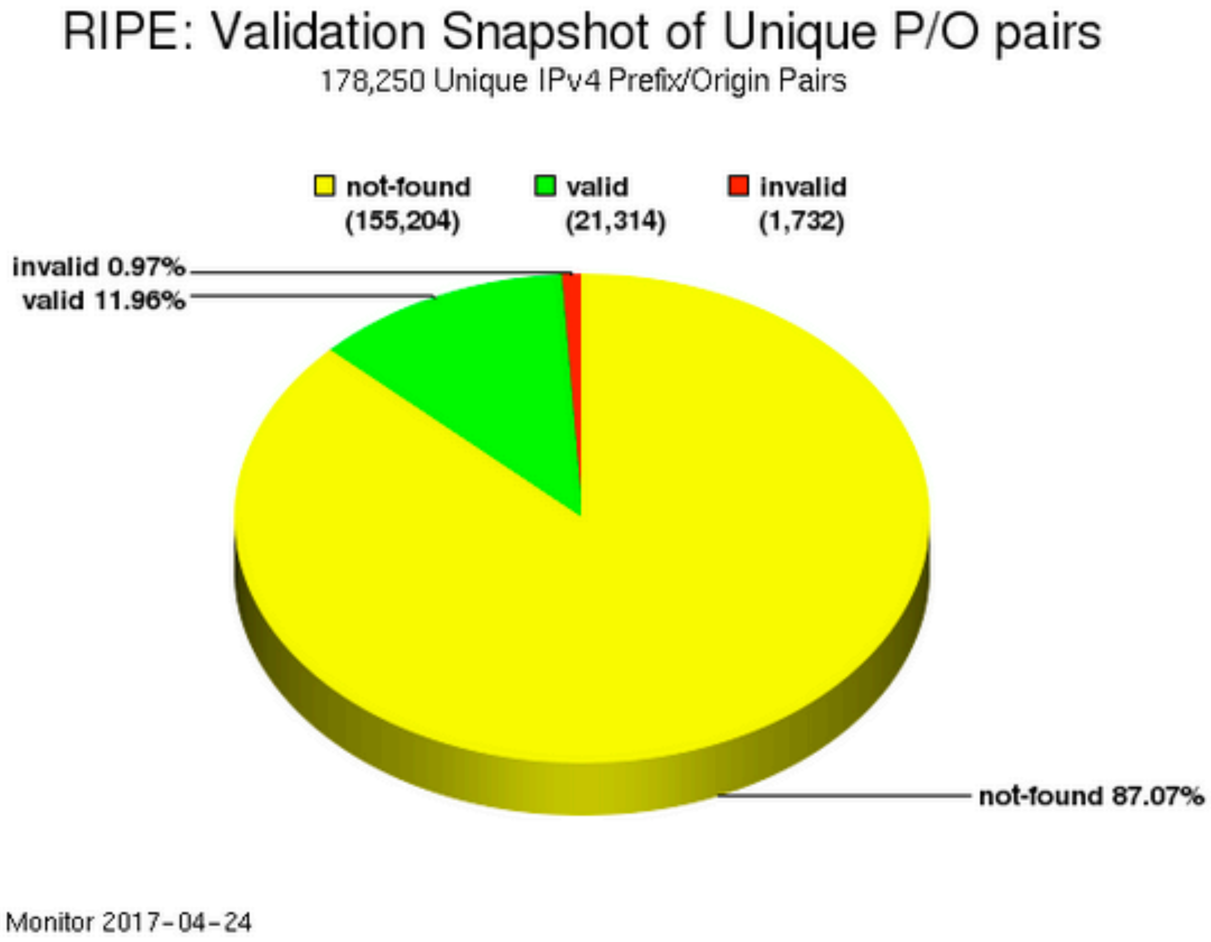
	Oct 2012	Apr 2013	Oct 2013	Apr 2014	Oct 2014	Apr 2015	Oct 2015	Apr 2016	Oct 2016	Apr 2017
Certified Orgs		47	68	108	153	187	220	250	268	292
ROAs	19	60	106	162	239	308	338	370	414	470
Covered Resources	30	82	147	258	332	430	482	528	577	640
Up/Down Delegated			0	0	0	1	2	1	2	2

RPKI vs The Routing Table: Globally

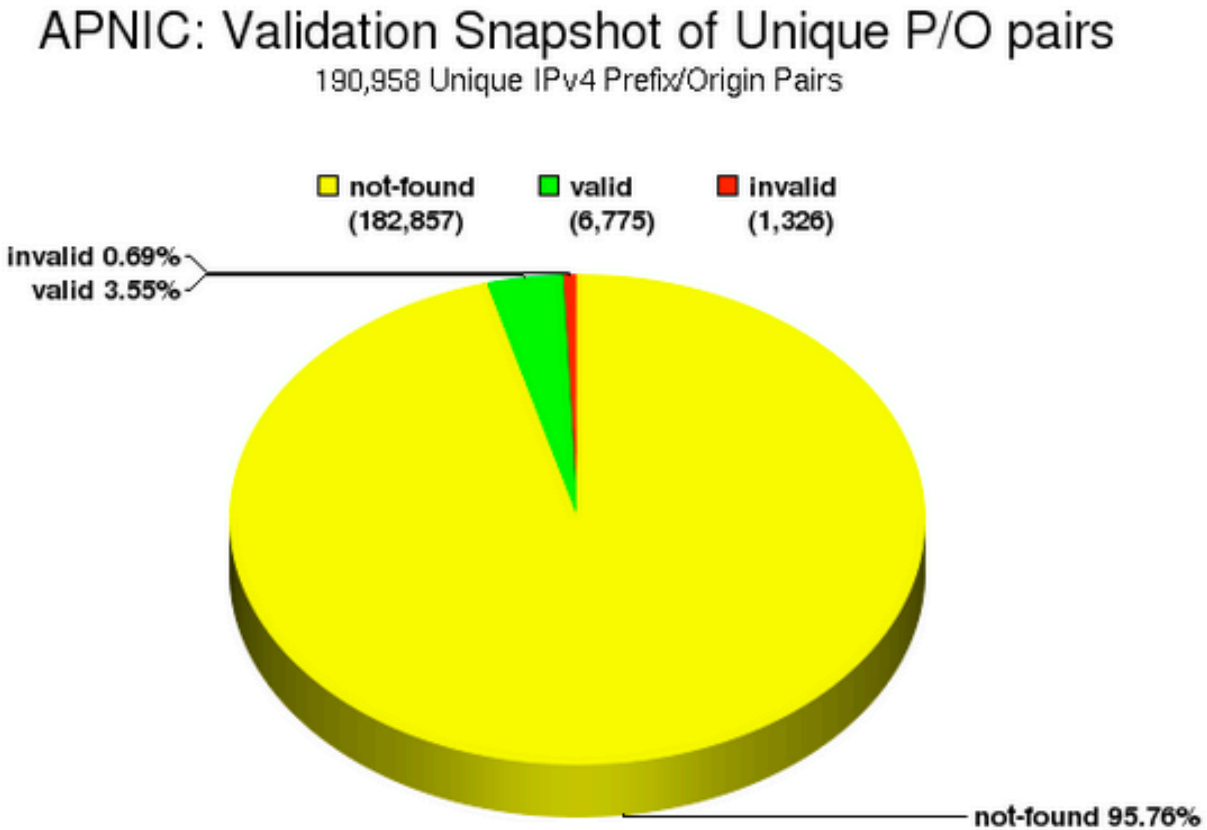


NIST RPKI Monitor 2017-04-24

RPKI vs The Routing Table: RIPE

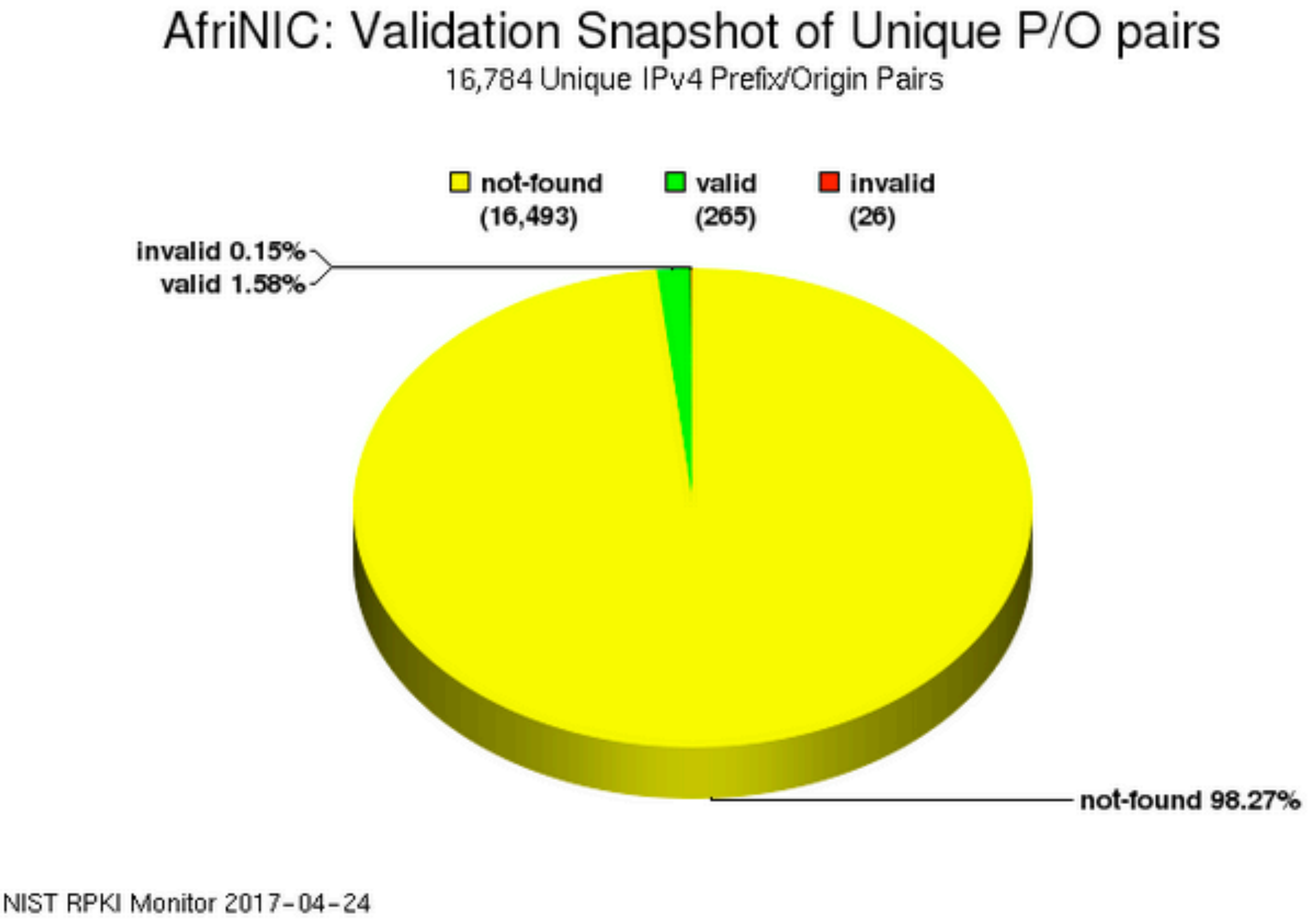


RPKI vs The Routing Table: APNIC



NIST RPKI Monitor 2017-04-24

RPKI vs The Routing Table: AFRINIC

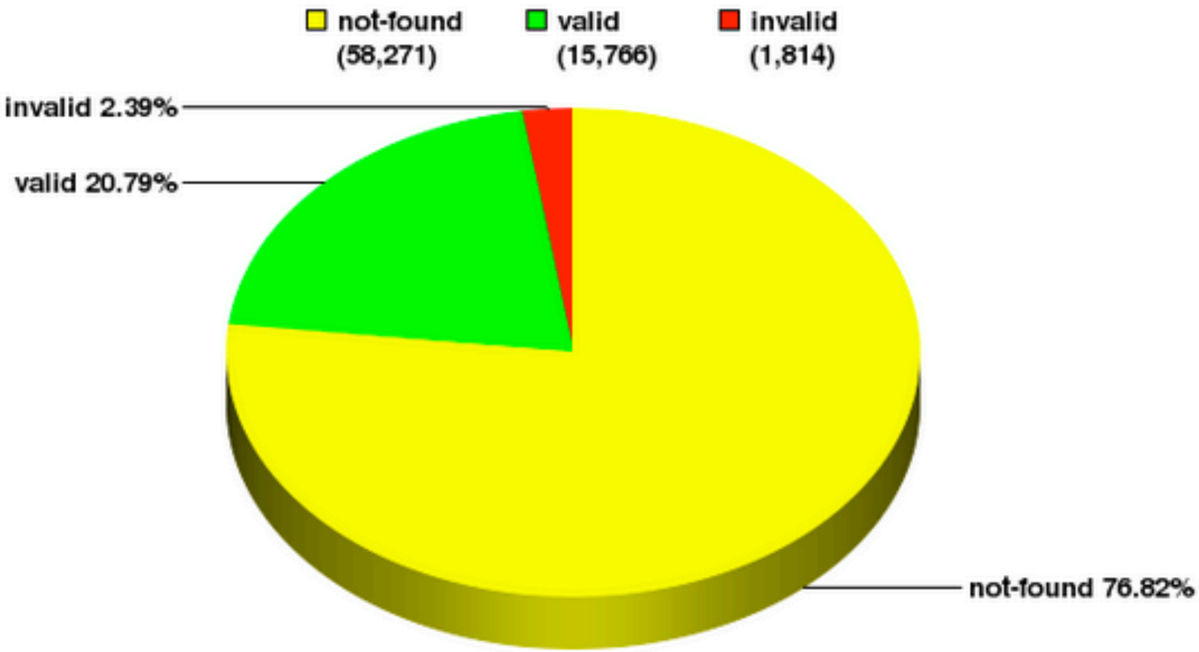


NIST RPKI Monitor 2017-04-24

RPKI vs The Routing Table: LACNIC

LACNIC: Validation Snapshot of Unique P/O pairs

75,851 Unique IPv4 Prefix/Origin Pairs

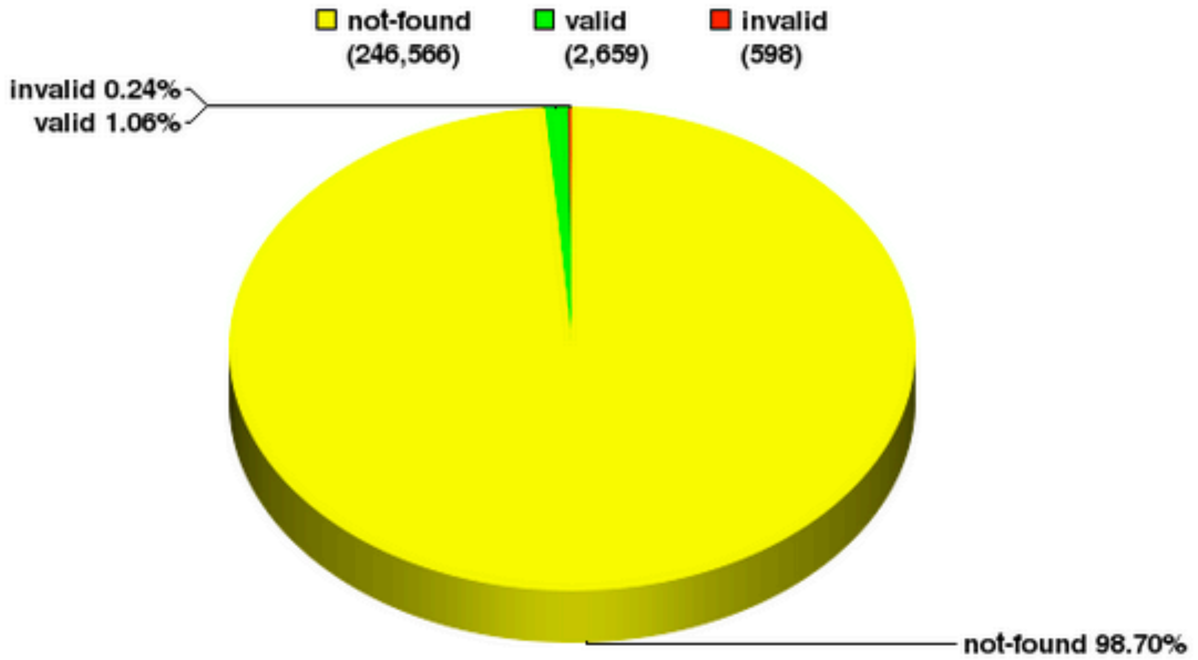


NIST RPKI Monitor 2017-04-24

RPKI vs The Routing Table: ARIN

ARIN: Validation Snapshot of Unique P/O pairs

249,823 Unique IPv4 Prefix/Origin Pairs



NIST RPKI Monitor 2017-04-24

Takeaways

- If you’re not using RPKI, you’re vulnerable to route hijacking
- Plenty of readily available documentation

  regarding implementation details
- If we can help, contact us

Q&A