Lessons learned running an RPKI service

Alex Band – Product Manager
@alexander_band

NANOG 63, San Antonio, Texas

RPKI: Ultra Quick Intro

- RIR becomes a Certificate Authority
  - Puts IPs and ASNs on a digital certificate; issues to LIRs
  - LIRs use certificate to make statements about their IPs
  - Statement is called a Route Origin Authorization (ROA):
    - “This AS may originate these of my prefixes in BGP”
    - “This is how much the AS may deaggagate the prefix”
- BGP Origin Validation
  - Operators validate and compare ROAs to real-world BGP
    - Authorised announcements make them happy 😊
    - Unauthorised announcements make them sad 😡

The Case For BGP Origin Validation

"Would you like a reliable way of telling whether a BGP Route Announcement is authorised by the legitimate holder of the address space?"

RIPE NCC


HELL YEAH BROTHER
memecrunch.com

Phased Approach: Start Small

- RIPE NCC worked on a prototype since 2006

- Launched an open beta mid-2010
  - Get operational experience and feedback before launch

- A limited production service on 1 January 2011
  - Not every type of address space was eligible
  - Only hosted system available with a web interface
  - No production grade support for Delegated RPKI

Keeping It Simple

- Conscious decision to keep it simple
  - Offer a stable and robust service
  - Gain operational experience
  - Gather user feedback
  - Automate all crypto complexity

- Mantra: Simplicity will spur on adoption
  - RPKI is a new technology
  - Small to no gains for early adopters
  - Avoid making users jump through burning hoops

Less Functionality, More Usability

- Automate signing and key roll overs
  - One click setup of resource certificate
  - User has a valid and published certificate for as long as they are the holder of the resources
  - Changes in resource holdership are handled automatically
- Hide all the crypto complexity from the UI
  - Hashes, SIA and AIA pointers, etc.
- Just focus on creating and publishing ROAs
  - Match you intended BGP configuration

That Should Be Easy, Right?!

- A ROA is nothing more than a statement that:
  - specifies which AS can originate your prefix, and
  - what the maximum length of that prefix is…

Route Origin Authorization

AS Number	Prefix	Maximum Length	
			Submit

Our first stab…

LIR Portal
RIPE NCC

Resource Certification - ROA Specification

You are logged in as [nl.bluelight.alexb]

- Logout
- General
- Billing
- Certification
- LIR Contacts
- IPv4
- IPv6
- ASN
- Request Forms
- Object Editors
- Tickets
- Training
- Tools
- Change Password
- X.509 PKI
- Events
- Glossary
- Contact

News | My Certified Resources | My ROA Specifications | History | RIPE NCC ROA Repository

ROA Specification

ROA specifications are used by the system to automatically publish the required ROA objects. See below for an explanation of the fields used to specify your ROA objects:

AS number *

My unique name for this customer/ROA *

Drag your resources here

Not valid before

and/or after

Add ROA

My certified resources

Search

85.118.184/21
93.175.146/23
2001:7fb:fd02::/47

Name: A unique name for use within your organisation. The name is not visible to anyone else.

ASN: The number of the Autonomous System that you authorise to route the listed resources.

Prefix: The IPv4 or IPv6 prefix to authorise.

Maximum Length: When not present, the Autonomous System is only authorised to advertise exactly the prefix specified here. When present, this specifies the length of the most specific IP prefix that the Autonomous System is authorised to advertise. For example, if the IP address prefix is 10.0/16 and the maximum length is 24, the Autonomous System is authorised to advertise any prefix under 10.0/16, as long as it is no more specific than /24. So in this example, the Autonomous System would be authorised to advertise 10.0/16, 10.0.128/20, or 10.0.255/24, but not 10.0.255.0/25.

Initial Results

- The Good:
  - Great adoption: 226 certificates in the first month
  - Lots of requests for other types of address space
- The Bad:
  - Almost nobody created ROAs
  - Awful data quality: more invalid announcements than valid
- The Ugly:
  - Maximum prefix length is the cause of much pain
  - Also, guys, please stick to just BGP Origin…

Lessons Learned

- Nobody knows what they actually originate in BGP
- Created ROAs don’t match BGP announcements
- Much misunderstanding of Maximum Length
- Side effects of poorly created ROAs were unclear
  - More and less specific overlaps, and their validity state
- Nobody cares about running their own CA

Results For The Roadmap

- Production support Delegated CA on back burner
- Show users which announcements they do
- Educate users about Maximum Prefix Length
- Add an alerting system when data gets stale
  - Also alerts when a hijack occurs
- Make the UI more intuitive

Our second stab…

BGP Route Validity

All | Valid | Invalid | Unknown | Suppressed

Items per page: 10 | Search by AS or IP...

Origin AS	Prefix	Route Validity
AS3333	2001:67c:2e8::/48	Valid
AS12654	2001:7fb:ff03::/48	Valid
AS12654	84.205.80.0/24	Valid
AS12654	2001:7fb:fd02::/48	Valid
AS12654	2001:7fb:ff01::/48	Valid
AS12654	2001:7fb:ff07::/48	Valid
AS12654	84.205.71.0/24	Valid
AS12654	84.205.93.0/24	Valid
AS12654	2001:7fb:fe01::/48	Valid
AS12654	2001:7fb:ff0a::/48	Valid

Suggest ROAs | Suppress Alerts | Re-enable Alerts

Go to page: < 1 of 5 >

Step 1/6

This overview shows all **eligible** address space on your resource certificate. If new resources are allocated to you, your certificate is automatically updated.

Learn more...

Next » End tour

Alerts

You currently have **0** invalid and **0** unknown BGP announcements (0 are suppressed).

All alerts are sent to **han.solo@example.net** once every 24 hours.

Configure

Certified Resources

- 84.205.64.0/19
- 93.175.144.0/20
- 193.30.30.0/23
- 2001:67c:e0::/48
- 2001:67c:2e8::/48
- 2001:67c:2888::/47
- 2001:67c:2900::/43
- 2001:7fb::/32
- 2001:7fd::/32

ROA Configuration

Items per page: 10 | Search by AS or IP...

AS number	Prefix	Maximum length

RIPE NCC RPKI Validator

Download the **RPKI Validator toolset** to use RPKI data in your BGP decision making workflow. **Learn more...**

The Key Differences

- Focus on BGP Announcements with certified address space instead of ROAs!
  - Show which BGP announcements are being done according to RIPE NCC Route Collectors
- Guided product tour with detailed documentation
- Suggest ROAs based on best practices
- Show the effects of a ROA ***before*** publication
- Email alerts if there is a hijack or problematic ROA

What We Saw

- The Good:
  - Dramatic increase in uptake, especially ROA creation
  - Vast improvement in data quality (>90% accuracy)
- The Bad:
  - After initial creation of ROAs, cruft starts creeping in
  - Operators create invalids but don’t know how to fix them
- The Ugly:
  - Deleting 10 ROAs = 10 clicks and 10 page refreshes…

Results For The Roadmap

- Add Event Tracking: analyse where user gets stuck
- More simplicity, better usability
- Combine everything on a single page
- Give better indication of problematic ROAs
- Suggestions for fixing invalids using best practices
- Offer RESTful API for the hosted system
- Add two-step verification (applies to all services)
- Future proofing…
  - Foundation for expanding feature set

Our third stab…

RPKI Dashboard

9 CERTIFIED RESOURCES | NO ALERT EMAIL CONFIGURED

41 BGP Announcements

4 Valid | **1** Invalid | **36** Unknown

4 ROAs

3 OK | **1** Causing problems

BGP Announcements | Route Origin Authorisations (ROAs) | History

Search...

Create ROAs for selected BGP Announcements

Valid | Invalid | Unknown

Origin AS	Prefix	Current Status
AS12654	2001:7fb:fe01::/48	UNKNOWN
AS12654	2001:7fb:fe0c::/48	UNKNOWN
AS12654	2001:7fb:fe0f::/48	UNKNOWN
AS12654	2001:7fb:ff00::/48	UNKNOWN
AS12654	2001:7fb:ff01::/48	UNKNOWN
AS12654	2001:7fb:ff02::/48	UNKNOWN
AS12654	2001:7fb:ff03::/48	UNKNOWN

Building a Community

- Having a good product is not enough: first people need to know about it and then engage with it.

- The #RPKI hashtag on Twitter
- Feedback button and live chat in the mgmt UI
- Monthly webinars dedicated to RPKI
- Integral part of RIPE NCC Routing Security course
- Discuss at operator and regional meetings

Community Activity

- Open source RPKI Tools
  - rpki.net
- SURFnet RPKI Dashboard
  - rpki.surfnet.nl
- BGPMon Route Monitoring
  - bgpmon.net/services/route-monitoring/
- RIPE NCC Github
  - github.com/RIPE-NCC

What Operators Tell Us…

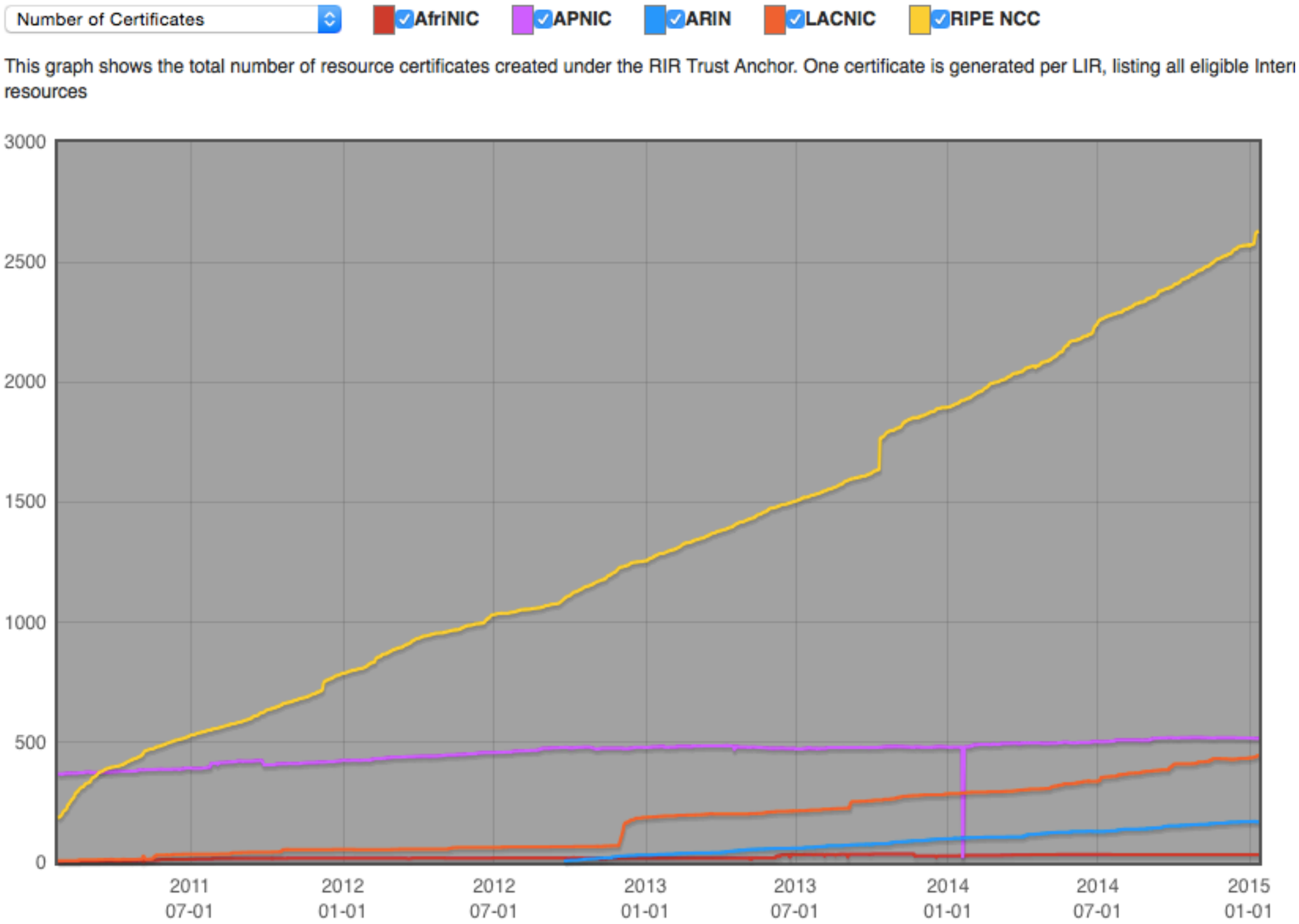
- Give me new data faster!
- Running the delegated model is not interesting
  - They prefer an API into the hosted system for now
- Used to have stale route objects, now stale ROAs
- The various relying party tools are not that mature
- There are different flavours of invalid announcement but I can’t filter on them in my router
  - “Unauthorized AS” and “Too specific prefix”

Our Future Plans

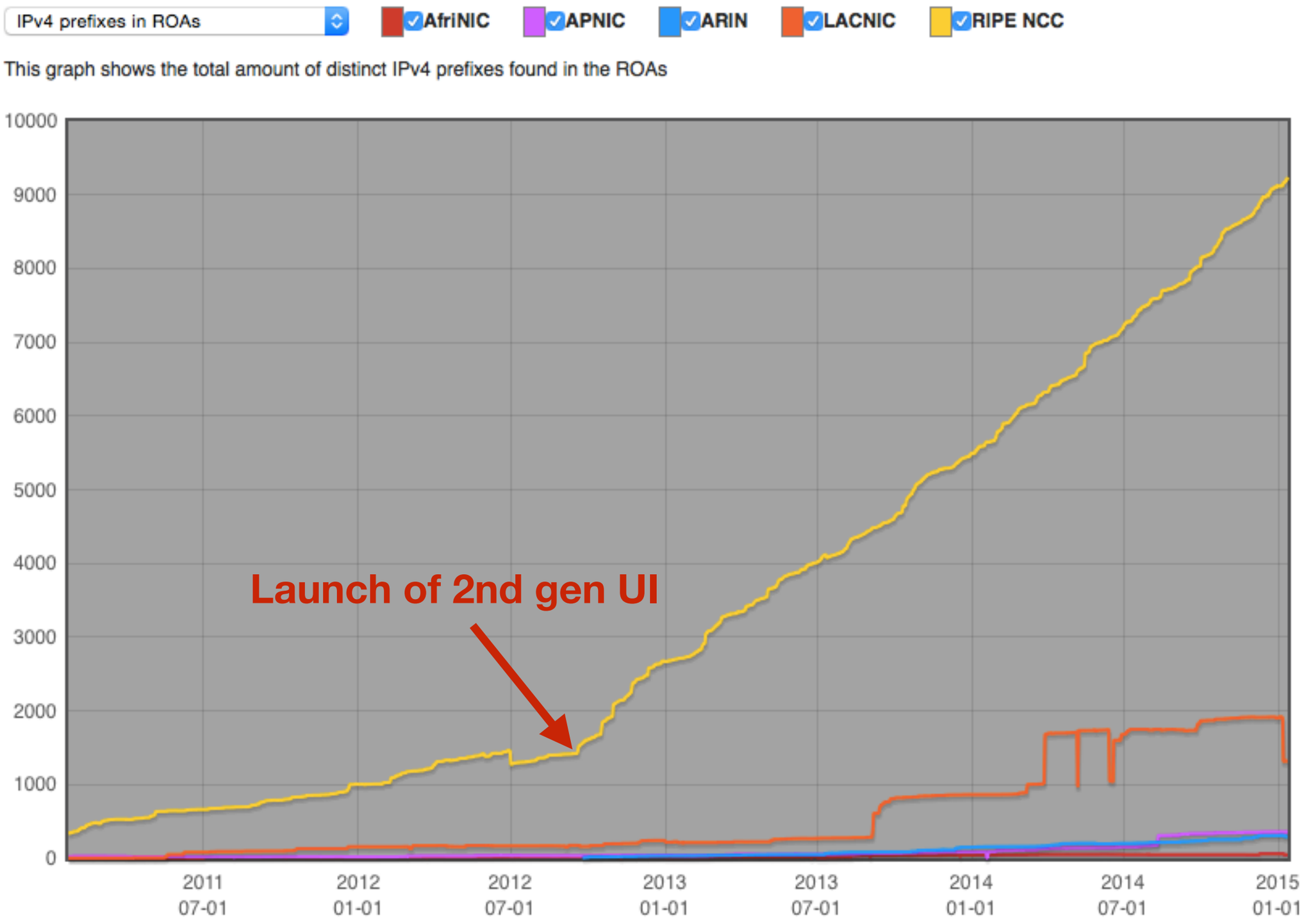
- Merge IRR ‘route’ object management in RPKI UI
- Replace rsync as protocol for fetching data
  - something faster and more scalable (HTTP)
- Support Inter-RIR transfers
- Production support for the delegated model
  - Yes, really… 😉
- Path Validation

The current global reality…

People Requesting a Certificate



People Actually Creating ROAs



RIPE NCC

The Take Away…

- Technology and functionality alone isn't enough
- Cherish your early adopters, listen to them
- Usability, education and community building works

Questions?

alexb@ripe.net

@alexander_band