ARIN

American Registry for Internet Numbers

RPKI Service Terms and Conditions Update

John Curran, President and CEO

January 2015

RPKI Terms/Conditions

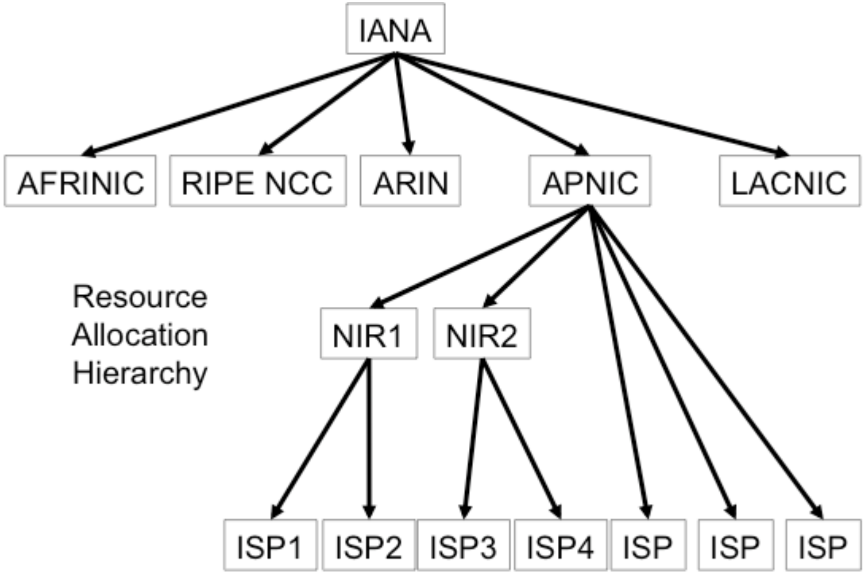
Situation

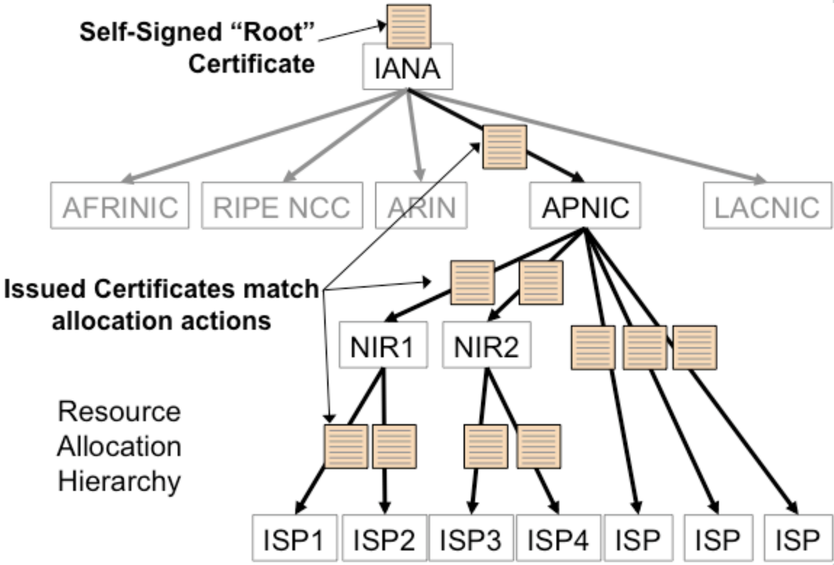
- ARIN provides resource certification services (i.e. RPKI services) to parties with an RSA/LRSA and address / ASN resources in the ARIN database directly assigned by ARIN or predecessor
- Resource certification is a system which publicly associates parties with specific addresses and autonomous system numbers. This is the same function performed to some extent by ARIN's Whois database, only RPKI does it using digital signatures. Both RPKI and Whois are methods of publication for ARIN's Internet number resource registry.
- Resource certification also allows address holders to associate specific AS numbers with their address blocks for purposes of allowing those network to announce routes for those blocks. This is quite similar to the information that parties presently put in routing registries, including ARIN's routing registry.

RPKI Terms/Conditions

Situation (cont.)

- RPKI information is published in an hierarchy which follows the IP address allocation hierarchy; each registry issues certificates corresponding to the resources it has issued.
- ARIN's RPKI participants publish their information by agreeing to ARIN's terms and conditions for RPKI services, and then using ARIN's "hosted" RPKI services or running their own "delegated" RPKI servers that link to ARIN's RPKI certificate authority servers.




Self-Signed "Root" Certificate
IANA
AFRINIC
RIPE NCC
ARIN
APNIC
LACNIC
Issued Certificates match allocation actions
NIR1
NIR2
Resource Allocation Hierarchy
ISP1
ISP2
ISP3
ISP4
ISP
ISP
ISP

Diagrams – G. Huston, 2008

RPKI Terms/Conditions

Situation (cont.)

- ARIN's customers use ARIN's RPKI services to publish associations that describe the routing which is valid for the networks which ARIN issued to that customer
- This RPKI information is publicly available, just ARIN publishes Whois and DNS information from ARIN's customers which s used numerous parties with not direct relationship with ARIN
- In the case of RPKI, the data is encrypted and there is a RPKI "Trust Anchor" that allows decoding & verification of the data.
- Parties who query and make use of the RPKI data are called "Relying Parties", and RPKI best practices encourage relying parties to "*manage the uncertainty associated with a system in early deployment; local policy can be applied to eliminate the threat of unreachability of prefixes due to ill-advised certification policies and/or incorrect certification data.*"

  RFC 7115 / BCP 185, "Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)"

RPKI Terms/Conditions

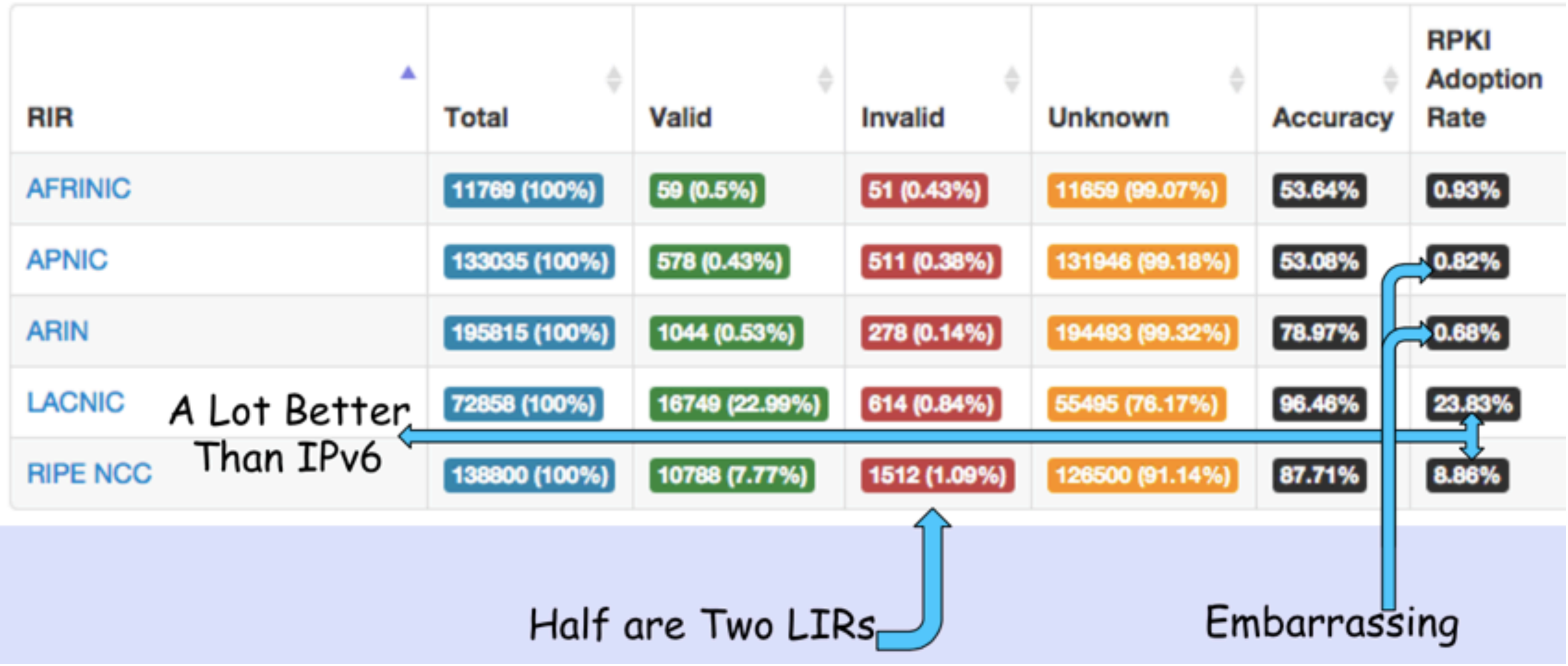
Situation (cont.)

- While the other 4 RIRs allow open access to their trust anchor, access to ARIN's Trust Anchor is presently only provided via a 'gold-standard' click-acceptance of the Relying Party Agreement (which outlines terms and conditions for use of data in the ARIN certificate authority, including disclaimer of warranty and indemnification of ARIN.)
- While other RIRs include disclaimers of warranty and indemnification in their RPKI terms of use, the application of these terms (via click-accept) to their actual members making use of the RPKI services for publication of associations, not the global community of services providers who may at some point be relying parties.
- The Relying-Party-Agreement click-accept is the logical equivalent

RPKI Terms/Conditions

Situation (cont.)

- Adoption of RPKI varies by region, with RIPE seeing the most activity overall (RIPE has invested heavily RPKI ease to use, has no overt legal barriers, and has done extensive community outreach & training.)
- Adoption in LACNIC is also quite strong within their user community



RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
AFRINIC	11769 (100%)	59 (0.5%)	51 (0.43%)	11659 (99.07%)	53.64%	0.93%
APNIC	133035 (100%)	578 (0.43%)	511 (0.38%)	131946 (99.18%)	53.08%	0.82%
ARIN	195815 (100%)	1044 (0.53%)	278 (0.14%)	194493 (99.32%)	78.97%	0.68%
LACNIC	72858 (100%)	16749 (22.99%)	614 (0.84%)	55495 (76.17%)	96.46%	23.83%
RIPE NCC	138800 (100%)	10788 (7.77%)	1512 (1.09%)	126500 (91.14%)	87.71%	8.86%

A Lot Better Than IPv6

Half are Two LIRs

Embarrassing

Diagram credit – Randy Bush, SURFNET

RPKI Terms/Conditions

Situation (cont.)

Some potential issues impacting RPKI deployment in ARIN region – service related

- Difficulty of use / user interface issues
  - Some credence to this, as ARIN's hosting RPKI user interface requires parties to encrypt their requests with a key known only to them (this provides non-repudiation and significantly reduces the possibility of an incorrect association being created.)
- Lack of user outreach and training
  - Also a possibility, as our levels of outreach
- Lack of actual of user demand for resource certification
  - Possible (but we would then need to understand why RPKI services are of interest and deployed in other regions)

RPKI Terms/Conditions

Situation (cont.)

Some potential issues impacting RPKI deployment in ARIN region – legal/packaging related

- ARIN RPKI service customer acceptance of T & C's
  - Recent service provider presentation at NANOG 52 specifically notes ARIN's indemnification as 'deal-breaker' (despite other RIRs having same obligations in the RPKI service terms.)
  - While indemnification already exists in ARIN RSA/LRSA, calling it out for RPKI via separate agreement creates an opportunity to review for what is perceived as an optional service (vis-à-vis requesting IP space)
- Global Relying Party Agreement (RPA) click-accept
  - Deployment of RPKI involves significant commitment of resources, and it is unclear if those services providers who are listening to RPKI associations will seek and/or be able to click-accept the ARIN's RPA (thus reducing the value of ARIN's RPKI services to the community.)

RPKI Terms/Conditions

Situation (cont.)

Some potential issues impacting RPKI deployment in ARIN region – legal/packaging related

- ARIN RPKI service customer acceptance of T & C's
  - Recent service provider presentation at NANOG 52 specifically notes ARIN's indemnification as 'deal-breaker' (despite other RIRs having same obligations in the RPKI service terms.)
  - While indemnification already exists in ARIN RSA/LRSA, calling it out for RPKI via separate agreement creates an opportunity to review for what is perceived as an optional service (constrast with requesting IP space)

- Global Relying Party Agreement (RPA) click-accept
  - Deployment of RPKI involves significant commitment of resources, and it is unclear if those services providers who are listening to RPKI associations will seek and/or be able to click-accept the ARIN's RPA (thus reducing the value of ARIN's RPKI services to the community.)

RPKI Terms/Conditions

Situation (cont.)

Legal related issues:

- *Information contained in RPKI is designed for real-time use to affect routing, and parties publishing such data and relying upon it have real potential for related-communication failures unless carefully following best practices in their deployment*
- *These communications failures can impact parties otherwise unrelated to ARIN, i.e. the customers of those using ARIN's RPKI services and the customers of the relying parties*
- *Complexity of the end-to-end RPKI system (ARIN's RPKI customer, ARIN's systems, relying party systems, customers of both, and the route processing) means that any operational failure will require complex analysis of cause-in-fact, proximate causation, etc.; resulting in a challenging situation in litigation*
- *Reliance upon RPKI customer indemnification does not fully address risks, as not all RPKI customers have necessary resourses*

RPKI Terms/Conditions

Next Steps

- *Service related issues:*
  - *Explore usability and training improvements to address*
- *Legal/packaging related issues:*
  - *Further research into RPKI customer indemnification requirements, various methods of agreement, and relation to existing RSA/LRSA indemnification language*
  - *Review Relying Party Agreement mechanisms and determine of indemnification by the RPKI data publisher (ARIN's RPKI customer) is sufficient to allow public Trust Anchor access*

RPKI Terms/Conditions

Discussion?