ARIN

American Registry for Internet Numbers

RPKI Relying Party Agreement (RPA) Change

John Curran, President and CEO
Thru Steve Ryan, Counsel

January 2016

RPKI RPA Change

Situation

- Resource certification/RPKI is a system allowing resource holders to publish and maintain specific information about their IP address blocks in a secure manner

- ARIN's customers use ARIN's RPKI services to publish (to other ISPs globally) the allowed routing for their ARIN-issued IP address blocks

- This RPKI information is publicly available, similar in concept to other information ARIN publishes, such as Whois and DNS information from ARIN's customers (which is used and relied upon by third parties who often have no direct contractual relationship with ARIN and thus no specific limitation on ARIN's liability)

- ISPs may use the RKPI data (when available) to confirm that routes they receive are from the appropriate/authorized party

RPKI RPA Change

Situation (cont.)

- Presently, third-parties must go to the ARIN web site and *click-to-accept* on ARIN's Relying Party Agreement (RPA) in order to obtain access to the encryption key (i.e. the "trust anchor") for ARIN's published RPKI data

- ARIN has consistently heard from the community that requiring third-parties to do this RPA acceptance step should not be necessary, and is inhibiting the deployment of RPKI in the ARIN region. The principle complaint is that technical staff must do an extra step compared to other regions in order to use ARIN data (specifically, having to send the RPA to their lawyers for review as a result of explicit legal acceptance) before being able to obtain access to ARIN RPKI data.

In 2015, ARIN undertook a multi-disciplinary review of the liability associated with its RPKI services and the RPKI agreement structures - the changes made as a result of this review are summarized in this presentation.

RPKI RPA Change

Typical RPKI Usage & Potential Liability Claims

Scenario 1

[Redacted Scenario Explanation]

Scenario 2

[Redacted Scenario Explanation]

RPKI RPA Change

Typical RPKI Usage & Potential Liability Claims (cont.)

- In either Scenario 1 or Scenario 2, if the inability to reach **ISP A**'s customers is believed to be connection to **ISP A**'s use of ARIN's RPKI services, then **ISP A** has indemnification duties to ARIN from any related claims

- This applies is all circumstances – there cannot be a relying party whose connectivity to a destination is allegedly impacted (as a consequence of ARIN's RPKI services) without the ISP or organization providing connectivity to that destination being an ARIN customer under RSA or LRSA.

However, indemnification is only as useful as the resources of the indemnifying party. *A case of particular concern would be if a small ISP served a large bank or financial firm and the financial firm was seriously impacted (e.g. $[Redacted Value]) by the small ISP's RPKI usage – the small ISP may not be have sufficient resources to provide meaningful indemnification of ARIN against such claims.*

RPKI RPA Change

Challenges with RPKI liability

- *All of the information in ARIN's RPKI system comes from an ARIN customer <u>who has signed an RSA/LRSA</u> which requires indemnification of ARIN from any allegation of damage or loss incurred in connection with any third-party claim, demand or action arising from their use of Services*

   (while this is applicable to any service we provide to customers, we have also made "RPKI services" explicit in the "Services" definition in the RSA 12/LRSA 4 agreement

- [Redacted Challenge]

- [Redacted Introduction], it is desirable to also set clear expectations upon parties accessing ARIN's RPKI data, hence the Relying Party Agreement.   In particular, it is important to make clear that RPKI data may and should be used to strengthen routing when available, but a relying party should readily handle the unexpected lack of RPKI information.

RPKI RPA Change

Relying Party Agreement

- Contains similar indemnification language for any party <u>using or accessing</u> ARIN's RPKI services

- This limitation is prominently displayed on the ARIN web site and in our RPKI tutorial and announcement materials

  (Note also that each of ARIN's digital RPKI certificates include a "policy qualifier" pointing to our Certificate Practices Statement (CPS) which contains the same indemnification language as the RPA)

- We proposed that ARIN amend our RPA practices and rely solely upon access of RPKI services as acceptance of the agreement

- [Redacted Introduction], it would bring ARIN into alignment with the practices in the other four regions and will remove a significant barrier for those deploying RPKI

- Upon careful review, there is a reasonable basis to argue that parties receiving the ongoing benefit of ARIN's RPKI services are bound to the Relying Party Agreement by such usage.

RPKI RPA Change

ARIN Insurance Coverage

- As a result of the RPKI liability question, ARIN undertook in 2015 its first comprehensive insurance coverage review

- [Redacted insurance background]

- [Redacted insurance background]

- For 2016 and beyond, we have established a new professional liability policy with $[Redacted value] coverage and improved language regarding scope of coverage.

In light of ARIN's existing indemnification against third-party claims by customers using our RPKI services, and the improved professional services insurance coverage, we propose that ARIN change its approach to the Relying Party Agreement in order to facilitate further RPKI deployment, and consider the overall risk profile to be acceptable.

RPKI RPA Change

Discussion?