ARIN Relying Party Agreement Impact? Workarounds? My Ever So Humble Opinion

Sandra Murphy
sandra.murphy@sparta.com

sponsored by DHS under an Interagency Agreement with AFRL

ARIN Relying Party Agreement

- See https://www.arin.net/resources/rpki/rpa.pdf for full text

IETF Role

- The IETF can not dictate legal matters to ARIN
  - That is a matter for ARIN members or their Board
- The IETF can evaluate the impact on envisioned architecture and use and attempt to develop mechanisms that could relieve impact

Cautionary Note to All

- The ARIN RPA was announced 17 Sep
- So this is quite early days yet
- Don’t panic
- This expresses concerns about impact; I do not presume to be making definitive statements about impact

Definitions

- ONLINE RESOURCE CERTIFICATION PKI (“ORCP”)
- “ORCP Services” means the validation of a Certificate, accessing or using an ARIN or ARIN-affiliate database of Certificate revocations, relying on any Certificate-related information, or otherwise accessing, using or relying on a Certificate, the ORCP (or any part thereof), and/or related services provided pursuant to any ORCP Service Terms. In connection with the ORCP Services, ARIN may provide you with a Trust Anchor Locator (“TAL”).
- “Relying Party” means an individual, entity or other organization that relies on a Certificate or the information contained in a Certificate, or otherwise accesses or uses any ORCP Services.

Caution on Uses

- <not> intended for…
- use in connection with equipment in hazardous circumstances or for uses requiring fail-safe performance,uses requiring fail-safe performance, including uses in connection with the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead to death, personal injury, or severe environmental damage.

INDEMNIFICATION

- You shall indemnify, defend, and hold harmless ARIN and CAs and each of its respective parent and subsidiaries, <etc>

PROHIBITED CONDUCT

- You shall not, directly or indirectly, use or attempt to use the ORCP Services (or any part thereof) or any of its related content to engage in any activity: that is not permitted by the ORCP Service Terms or otherwise is a violation of any law; that violates the rights of any third party; that transfers or in any way gives any other party Your access to or use of any ORCP Services; that would compromise the security or operation of any ORCP Services; or that would create any modifications or derivative works of any ORCP Services or any of its related content. Further, You shall not use, copy, link to, rebroadcast or disclose the ORCP Services (or any part thereof) or any of its related content, except as permitted by the ORCP Service Terms. You shall not, directly or indirectly, disclose, share, divulge, link to, rebroadcast, provide access to or in any other way make available the TAL to any third party, except as permitted by the ORCP Service Terms.

Derivative Works

- You shall not .. engage in any activity: that would create any modifications or derivative works of any ORCP Services or any of its related content.

Potential Impact

- Operators have said to me “I don’t want to run anything. I just want to click on a website somewhere”
- There are already tools/sites that display stats and summaries
- There are already tools/sites that display the certification status of prefixes, that display the validity of BGP routes, etc.
- Public services like Looking glass sites – extensions to report validity
- Are these modes of use permitted under the ARIN RPA?

Sharing RPKI data

- You shall not .. engage in any activity: that
- transfers or in any way gives any other party Your access to or use of any ORCP Services;
- Further, You shall not use, copy, link to, rebroadcast or disclose the ORCP Services (or any part thereof) or any of its related content,
- You shall not, directly or indirectly, disclose, share, divulge, link to, rebroadcast, provide access to or in any other way make available the TAL to any third party

Potential Impact

- The RPKI is object security
  - Objects carry their security with them
  - Verifying security requires only access to a trust anchor
  - Which means you can get the objects from anyone – neighbor, billboard, etc
- Contrast that with transport security
  - There is one trusted source
  - Verifying security means getting the objects from the trusted source over a secure transport

Object Security Architecture&Use

- Single authoritative source
  - Transport security: source is single point of access
  - Object security: Objects created by source can be mirrored by anyone anywhere – global caches, regional, metro, …
- Would the ARIN RPA prevent this object security architecture and use

Object Security Architecture&Use

- RPKI-rtr cache hierarchies
- Would the ARIN RPA forbid hierarchies across organizational boundaries

Object Security Architecture&Use

- Bootstrapping new network, restarting after failure - how to get info for securing routing before routing is functioning?
  - Transport security: retrieve from outside network somehow
  - Object security: bringing up connection to neighbor anyway, get feed from neighbor
- Would the ARIN RPKI forbid neighbor sharing

Object Security Architecture&Use

- Exchange point
  - Transport security: redundant retrieval by each
  - Object security: shared repository
- Would the ARIN RPA forbid the shared repository

Object Security Architecture&Use

- If all sharing sorts of architectural possibilities are prohibited by the ARIN RPA
- .. then ARIN would become the single point of access to ARIN RPKI data
- Is there anything we can do to/with the RPKI to make that not create a problem?
  - New communication mechanisms? Anything to reduce object churn? etc

JIT Response on list from John Curran

- I would also like it made clear during the presentation that the ARIN RPA does _not_ prevent the object security architecture, but does require that the participants in the model confirm _once_ that they follow the basic requirement of the PKIX architecture (per RFC 5280) of being aware of the applicable policy for ARIN's CA. Parties are free to replicate objects far and wide by any and all methods; it is simply validation that requires that they have accepted the RPA in the process of obtaining the TAL (which presumably occurs once during their initial setup.)

  (underlining is my own)

Crazy Ideas to Reduce Impact

- Suppose the intended recipient could prove it had signed the RPA.
  - *I*F* that would satisfy ARIN
  - What could that proof be
    - Some sort of signed object seems right
    - But does not seem related to RPKI authority
    - Something signed by ARIN?

Crazy Ideas to Reduce Impact

- Suppose the data was encrypted from ARIN
  - *I*F* that would satisfy ARIN
  - ARIN would transmit data encrypted
  - Data could be shared in encrypted form
  - Recipient would have to contact ARIN to get decrypt key

Crazy Ideas to Reduce Impact

- Are there changes to the CP that could help?
  - Should the no-nuclear-reactors type language be in the CP?
  - Is there anything else we can put in the CP that would help? (hesitantly – anything on liability?)