Request to Reconsider ARIN RPKI Trust Anchor Approach

Background

- In January 2016, the ARIN Board of Trustees considered at length the requirements regarding the RPKI Relying Party Agreement (RPA) and access to ARIN's RPKI Trust Anchor - https://www.arin.net/vault/about_us/bot/bot2016_0111.html

- The review resulted in significantly easier access to the ARIN' RPKI trust anchor (changing the Trust Anchor Locator to available via direct download from ARIN's web page rather than only via email after explicit RPKI RPA acceptance)

- The requirement for specific and conscious action to access ARIN's RPKI TAL supports agreement between ARIN and the relying parties regarding expectations

- We've been asked if it is possible to further simplify access to ARIN's RPKI Trust Anchor, so as to help speed RPKI deployment

Request Regarding ARIN's RPKI Trust Anchor Locator (Job Snijders)

A goal should be to make it easy as possible for Asian, Russian, African and European ISPs to use the ARIN TAL to mitigate attacks on resources assigned to ARIN members.

1. Unlike the other four TALs, the ARIN TAL is not included in common RPKI software, that in itself is a considerable difference and additional work compared to working with the other TALs. Firstly someone has to notice the ARIN TAL is not included, and subsequently work out why the ARIN TAL is not included.

2. A majority of internet stakeholders are based outside the ARIN region, in order for RPKI to be successful (e.g. to generate the most security benefits for ARIN members), broad and global adoption is paramount. Understanding and agreeing to the RPA might require the hiring of (legal translation) expertise in "foreign" (American) law.

3. One has to set up a business process to monitor for changes to the ARIN RPA.

Should the five RIRs fail to form a united front, and fail to provide a consistent experience, I theorize that failure will promote the concept and lead to acceptance of third party non-RIR TALs. In choosing to not be part of "the bundle", and acting like a random third party, ARIN is showing the world the exact path how third parties can be part of the RPKI ecosystem. I believe this is reminiscent to the TLS world, which goes counter to what the IAB and NRO have stated is the optimal RPKI configuration.

I ask that that you consider how ARIN can best drive adoption of the ARIN TAL outside the ARIN region, as that is where a considerable amount of benefit can be generated for the ARIN members. BGP hijacks don't respect RIR region borders, so RPKI validating deployments outside the ARIN region are a key component to improving the routing security posture for ARIN members.

Questions?