

**SIDROPS Agenda For IETF-109 (version 1)

**

Session: November 16th 2020, 16:00 - 18:00 UTC+7 (09:00 - 11:00 UTC)

1. Agenda bashing and Chair's slides - [5 minutes]
 - Administrivia. Nathalie/Warren/Keyur divvy up notes and jabber.
 - Can discuss other stuff in AOB at the end, there isn't a lot of time-pressure
2. Alexander Azimov - [15 minutes] ASPA drafts
 - [Slides](#)
 - Discussion
 - Questions about multiple ASPA, and the ability of the system to encompass more than one TA validating prefixes and ASN.
 - The Union of all states is used (Asimov)
-Overclaims, the overlap of the union of all the TA roots will mean in future state we have to deal with multiple competing ASPA (Asimov in the context of ROA, more specifics to be processed before less specific, perhaps analogous methods here) (ben: RP should be confident they have completed a full fetch before proceeding -type language)
 - Randy: as you come "down" from a TA, use the "lowest" instance of a customer-AS to be unique. talking about uniqueness, its the customer-AS. the RP knows the chain. If in multiple TA, chain, ASPA, don't think you have a choice other than the union of the states.
 - Rudiger: RP fetching from several different TA, think you have to understand the time is not uniform between all the different TA. a "complete fetch" for a certain state of a total system is just not possible.
3. George Michaelson - [10 min] Signed TAL
 - [Slides](#)
 - Discussion

- Randy: worth documenting, but with Rob K on security issues
 - Tim: 2 keys should be enough
 - GGM: lets carry work forward on list to WGLC in future state
4. George Michaelson - [10 min] Resource Tagged Attestations
- Slides
 - Discussion
 - Some TA may still consider they incur liability. Can't be ignored.
 - Specifically asked for this for GeoFeed use signing. stronger attestation, useful to have this. There are quibbles, but can take offline.
 - Tim: can work outside RPKi repo, the CMS is signed under existing RPKI CA certificates, wouldn't see the objects in the RPKI itself, may be use cases, its not necessary for the validation
 - Ben: think this is useful. can see problems this will solve straight off the bat (using routing registry hacks). Visible in repo or not: there are use cases either way. When its a signal of intended business? no But, use cases where people dealing with each other at arms-length need to be able to communicate their intention, requiring out of band is not helpful (lost audio at this point). Like to volunteer to bang on AfriNIC to make this be supported.
 - RobK: value being able to show and hide end-objects in the chain, the certificate that is used, should be in the REPO. have mechanisms, all the oid, to be in there, validate, so, could see way forward the certificate end user is in the repo, in mnf, but object isn't. GGM: not envisioned but ASN1 won't exclude this. RobK can then only validate the EE and doc, everything else is pre-validated.

- Randy: scaling issues and garbage collection. GGM: need to note. Not intending publishing the signed objects just the detached sigs.

5. AOB

- Chris: anyone has any topic?
- Tim: Earlier in draft of agenda, speak to RSYNC-FALLBACK discussion. Still planning?
 - Chris: had planned to, but it closed itself out.
 - Tim: what RFCs say must be done vs what is the best thing which should be done? willing to do the RFC, but do Rsync deprecation as a separate effort
 - GGM: keen to continue the work, progress things. (co-author)
 - Nathalie: looked at implementation burdens, fallback, can't implement in time. we're not going to implement fallback, focus on RRDP being rock solid.
 - Tim: no more to add.