Root Zone Evolution Review Committee (RZERC) Meeting Minutes
15 February 2022 | 19:00 - 20:00 UTC

Attendance

IETF	Tim April
ASO	Carlos Martinez
ccNSO	Peter Koch
ICANN Board	Kaveh Ranjbar
PTI	Kim Davies
GNSO RySG	Howard Eland
RSSAC	Daniel Migault
SSAC	Geoff Huston
Verisign (RZM)	Duane Wessels
Staff	Danielle Rutherford

Action Items from this Teleconference

- **ACTION ITEM: Staff to publish approved 18 January 2022 minutes on RZERC's website.**

Call to Order
Tim April called the teleconference to order at 19:03 UTC.

Roll Call
Danielle Rutherford conducted a roll call.

Agenda Review
There were no amendments to the agenda for this meeting.

Administration
Draft Minutes from 18 January
Tim April called for a vote on the draft minutes from the previous teleconference. There were no objections to the minutes and the minutes were approved.

- **ACTION ITEM: Staff to publish approved 18 January 2022 minutes on RZERC's website.**

Discussion Items
ZONEMD Deployment Plan
Duane Wessels presented a draft plan for deploying ZONEMD in the root zone that was jointly developed by Verisign, as the Root Zone Maintainer, and by ICANN as the IANA Functions

Operator. In the interest of proceeding with caution, the ZONEMD record in the root zone shall be introduced in two phases. Prior to adding any ZONEMD record to the root zone, Verisign must implement and deploy changes to its Root Zone Management System and all Root Server Operators must confirm their readiness for the ZONEMD record. The first phase shall use a private-use hash algorithm number. This makes the ZONEMD digest unverifiable and allows impacted parties to ensure that the mere presence of the ZONEMD record does not cause problems. In the second phase, the hash algorithm will be changed to SHA-384. At this point the ZONEMD record becomes verifiable.

Geoff Huston asked if Duane Wessels has checked the compliance of the draft deployment plan against RFC 8976 and where does it vary? And if it does vary, would the draft deployment change or would RFC 8976 change? Duane Wessels responded that RFC 8976 addresses this, “the hash algorithm field must be checked. If the verifier does not support the given hash algorithm, verification must not be considered successful with this ZONEMD RR.” So it can’t use that particular record to verify the zone. If that’s the only one, then the verifier has no way to verify the zone. If there are multiple records with different hash algorithms then it can proceed to using a different record or different hash algorithm to perform the verification. Duane Wessels agreed to add that in the first phase, it will cause an unsuccessful attempt to verify as per the RFC and implementations are expected to accept the zone in such a case.

Geoff Huston asked why the deployment plan referred to RFC 3597 in reference to the ZONEMD appearing in the unknown/generic format on internic.net servers when RC 8976 calls for a specific ZOMEMD presentation format. Duane Wessels clarified that if you’re a ZONEMD aware implementation, then you should use the ZONEMD presentation format. If you’re unaware, then you should use the generic format. Peter Koch shared a line from RFC 3597 that actually explicitly allows the use of this generic format from the implementation side. Peter Koch also voiced his support for the phased approach. Geoff Huston responded that if that context was added as a footnote his concern would be addressed. Daniel Migault voiced support for a footnote.

Daniel Migault asked if there was criteria for a rollback from either phase one or phase two of if there’s significant impact noticed. Duane Wessels stated at this time the potential impacts are unknown and that we’re going to have to sort of just watch it closely around these dates and see what happens. Duane Wessels stated he would add a defined communication mechanism and points of contact for problem reports to the draft deployment plan.

Geoff Huston asked what will happen if RSOs do not enable ZONEMD verification, as it is not required according to the draft deployment plan. Duane Wessels confirmed it is not a requirement and added in his discussions with the RSOs none of them are planning to turn on the verification in the near future. They’re all taking a cautious approach to wait and see how this goes. Geoff Huston responded the draft deployment plan doesn’t address the scenario of what if RSOs implement verification and it fails, and recommended that the draft deployment plan should confirm that the outcome of verification should not affect the publication of the root zone. Peter Koch added that the draft deployment plan is ambiguous as to why the RSOs are

not required to implement verification and suggested adding a source to make it clear that position is not originating in the deployment plan.

Tim April asked if there was a defined escalation path in case that someone notices an error with ZONEMD. Duane Wessels confirmed he will add points of contact for problem reports in the next draft of the deployment plan. Kim Davies noted that he and Duane will discuss if there should be a standing mechanism for reporting errors in the root zone contents.

Kim Davies asked in chat if the RSOs currently validate the root zone RRSIGs to pre-empt publication. Kim Davies added on the call in a broader context if any kind of validation done with DNSSEC already might gate publication of the root zone and stated it's an area to get a better understanding to inform anything specific to ZONEMD.

Daniel Migault observed that the introduction of ZONEMD is the least problematic thing compared to the architecture that local root enables, which is coming from a completely managed root zone system to a completely unmanaged way to handle the root zone. Daniel Migault asked if that should be considered for the draft deployment plan. Duane Wessels stated it was out of scope for the deployment plan but could be a general topic of conversation for the RZERC to consider. Peter Koch agreed it was out of scope for the deployment plan and stated a more in-depth understanding of the consequences of this paradigm shift should probably be something that the RZERC engages in.

AOB

RZERC Charter Review Kick Off

Tim April stated that members should expect a doodle poll soon for the first meeting of the RZERC Charter REview. Tim April requested RZERC members review the topics from the scoping exercise RZERC has been discussing to try and close out the list of topics.

Adjournment

The RZERC concluded the teleconference without objections at 19:57 UTC.