RIPE DNS Working Group

DNSSEC Key Repository Task Force Recommendations in Response to Proposed Trust Anchor Repository (TAR)

Authors: The RIPE DNS Working Group
Document ID: ripe-601
Date: January 2014

Note: this RIPE Document was created in 2014 for archival purposes and reflects work from 2008 that was later overtaken by events.

The following letter was produced by the DNSSEC Key Repository Task Force and sent to Barbara Roseman at ICANN in 2008. The letter was in response to IANA's proposed Trust Anchor Repository (TAR).

Dear Barbara,

Thank you for your note about the proposed DNSSEC key repository for TLDs. The RIPE DNS working group (DNS WG) welcomes this development. We would like to see IANA establish this DNSSEC Trust Anchor Repository (TAR) as soon as possible. We have developed a set of requirements for such a repository. As these may be useful for you when implementing the service, we offer them here:

[1] The TAR should be technology neutral. It should not exclude or prevent different flavours of trust anchors from being published, provided those trust anchors conform to the relevant standards.

[2] The TAR should be OS/DNS implementation neutral. Tools and documentation should be provided for use of the repository with common DNS resolver and name server platforms.

Comment: IANA should publish such documentation and tools, or pointers to them. Once we know details of repository, we can help putting together this documentation.

[3] The TAR should verify that the keying material it receives comes from an authorised source, verify it is correctly formatted and verify it is consistent with what is published in the TLD zone before publishing it. There should also be a secure channel for authenticating the repository and any data it is publishing.

Comment: Using the same channels IANA uses to process update requests to the root zone from TLDs should be fine. We do not mean special new channels. https delivery and possibly checksums are sufficient for publication.

[4] A process is needed to revoke a trust anchor and notify those who may be using the now withdrawn or invalid trust anchor.

Comment: An opt-in mailing list for operational news should be sufficient to satisfy this.

[5] The TAR should be clear what support, if any, is available.

[6] The TAR must have a published exit strategy.

Comment: The proposal includes that.

[7] The TAR should only publish keying material with the consent of the respective key manager.

Please let us know any the details of the repository as well as the time-line for implementation as soon as they become available. Please feel free to make our support for this repository known publicly or within ICANN.

Kind Regards

RIPE DNS WG
Jim Reid
Chair