

19 May 2022

RE: Statement on DNSSEC Signing and Validation

Tijani Ben-Jemaa
Vice Chair, African Regional At-Large Organization (AFRALO)
The Middle East Space Community

Dear Tijani,

Thank you for sharing your Statement regarding DNSSEC signing and validation in the Middle East region. The statement addresses an issue that is at heart of ICANN technical engagement. We note with great satisfaction that you recognize how important secured operation of the DNS is to the overall stability and resilience of the Internet, which is core to ICANN's mission.

Your statement makes a series of recommendations for ICANN org to consider. We have no doubt that these recommendations will be taken into consideration, as they are aligned with the [ICANN Strategic Plan for Fiscal Years 2021-2025](#) and the [Middle East and Adjoint Countries Regional Plan for Fiscal Years 2021-2025](#). More specifically, the recommendations relate to the regional goals to:

- Support the development of technical capacities and the building of regional networks of technical experts in partnership with relevant stakeholders.
- Identify and mitigate security threats to the DNS through engagement with relevant stakeholders.

The Board appreciates the thoughtful input from the Middle East Community and looks forward to continuing to work with you on all needed improvements.

Please find attached highlights of actions already in motion and related to the recommendations raised in your letter.

Best regards,



Maarten Botterman
Chair, ICANN Board of Directors

1. Highlights of ICANN Org Work to Support DNSSEC Signing and Validation

Throughout its existence, ICANN has worked with the community and other partners to promote and support DNSSEC deployment (<https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en>). Here are highlights of the activities that support our engagement on DNSSEC deployment:

- 1. Root zone signing and key management:** ICANN has ensured a secure signing and maintenance of the DNS root zone, providing a single Trust Anchor (TA) to the whole DNS tree. Signing the root zone is a critical component of effective DNSSEC deployment globally. Root Key Signing Key Ceremonies are performed several times a year using a model that is highly transparent, serves as a role model for others in the industry, and actively engages trusted community representatives in the process deployment globally (<https://www.iana.org/dnssec>).
- 2. Operational knowledge sharing.** The policies and procedures, as well as software IANA has developed for root zone key management are published and we encourage other operators to learn or adapt them to suit their needs. Our core policy, the DNSSEC Practice Statement, is published along with the associated framework as RFC 6841. (<https://www.iana.org/dnssec/procedures> and <https://datatracker.ietf.org/doc/html/rfc6841>)
- 3. TLD signing requirements in Registry contracts:** ICANN has a clear requirement for generic TLD operators to DNSSEC sign their zone. Today we are proud that in compliance with these requirements, 100% of generic TLDs are DNSSEC-signed, and many offer automated processes through their registrars to also allow registrants to sign their second level domains (https://stats.research.icann.org/dns/tld_report/).
- 4. DNSSEC awareness engagement globally:** ICANN Organization has been engaged in DNSSEC deployment awareness for several years, working directly with operators or partnering with external organizations, such as NSRC, to do capacity development. This activity recently took a new positive turn with the creation of a regional Technical Engagement training team - part of the Office of the CTO (OCTO) - that actively conducts capacity-building events across the world on DNS ecosystem security and particularly on DNSSEC, including validation by resolver operators. (<https://www.icann.org/resources/pages/tech-engagement-training-course-catalogue-2021-04-22-en>)
- 5. DNSSEC hands-on capacity building in the Middle East:** Our regional Technical Engagement team has conducted more than 25 training sessions in the Middle East

region over the past two years despite the pandemic-related restrictions imposed globally. These were practical trainings using our virtual hands-on lab platform that helped operators to raise their confidence level in the DNSSEC deployment process. The team is increasing its capacity and tools in order to address the specific support needs expressed by operators in the region

(<https://www.icann.org/en/blogs/details/icann-strengthens-its-technical-engagement-in-africa-and-the-middle-east-13-10-2021-en>).

6. **DNSSEC deployment in the Middle East region:** Among ccTLDs in the region, since 2019, several ccTLD operators have deployed DNSSEC following hands-on DNSSEC training. Operators for the following ccTLDs have signed their zones or provided Delegation Signer records to IANA: .LY, .BH, .MR, .DZ, and .KW. In addition, the operators for .SA, .TN, .MA, and .SY have deployed DNSSEC for many years. This practice sets a good example for others to follow for DNSSEC deployment in the region.
7. **ICANN Org is working to launch KINDNS:** This is an initiative to further promote DNS operational best practices among operators. With support of the community, the platform will identify critical security best practices for DNS operation and guidebooks will be developed on how to implement them. We expect to actively promote the program in the ME region, providing the community with an additional tool to help them in their DNSSEC deployment journey (<https://community.icann.org/display/KINDNS>).
8. **Resolver operators forum:** ICANN hosted a new DNS resolver operator forum in order to engage more with the resolver community, hear about their evolving environment, and share with each other privacy and security challenges they face in their day-to-day operations. (<https://www.icann.org/en/announcements/details/a-global-icann-resolver-operator-forum-announced-2-12-2021-en>)
9. **ICANN DNS Symposium:** The ICANN DNS Symposium is a one-day event focused on all aspects of the Domain Name System (DNS). Geared to those who have a foundational understanding of the DNS and an interest in DNS operations, engineering, research and standards development or operational security, it helps strengthen ICANN engagement with DNS experts outside ICANN in order to explore with them challenge facing the ecosystem for maintaining a secure, stable and resilient global DNS including DNSSEC deployment. (<https://www.icann.org/ids>)