



80 | POLICY
FORUM



ICANN Technical Engagement efforts toward more DNSSEC deployment in Middle East and Africa

ICANN 80 - DNSSEC and Security Workshop

Yazid Akanho

Technical Engagement
Office of the CTO

June 10, 2024



Technical Engagement: who we are ?

- A team within OCTO, mainly in charge of DNS secured operations outreach, training, capacity building and capacity development programs:
 - Develop and deliver technical content on DNS, DNSSEC, DNS security.
 - A more digestive approach: presentations, webinars, hands-on.
 - Language diversity: English, Spanish and French.
- Regionalized team to better align regional specificities and ICANN Strategic Goals.
 - Audience: ccTLDs, registrars, DNS hosting providers, ISPs, MNOs, Governments, LEAs, NOGs, Universities, ...
 - Similarities and differences in needs and expectations from regions.



TE Course catalogue ... being revisited

Technical Engagement Training Course Catalogue

If you are interested in having the Technical Engagement team present any of the courses listed in the catalogue, or would like more information, please do not hesitate to [contact us](#).

[ICANN's Technical Mission](#)

[DNS 101](#)

[DNSSEC 101](#)

[Advanced DNS](#)

[Advanced DNSSEC](#)

[Registry Operations for ccTLDs](#)

[OSINT: Fighting DNS Abuse \(DNS Abuse for LEAs\)](#)

[DNS Abuse: Threats and Mitigation](#)

[Introduction to RDAP for Domain Names Registrations](#)

[DNS Ecosystem Security](#)

[DNS for Internet Service Providers](#)

[Network Operation Security](#)

[UA: Email Address Internationalization \(EAI\)](#)

[UA: Universal Acceptance for Java Developers](#)

<https://www.icann.org/resources/pages/tech-engagement-training-course-catalogue-2021-04-22-en>

Request training and hands-on : email us at OCTO@icann.org

The online lab platform: important for our hands-on

- A set of LXC containers running on AWS LightSail/EC2.
- Connect from anywhere: browser + Internet.
- Efficient:
 - Fast deployment compared to physical infrastructure.

Simultaneous multiple deployment.

- Scalable:

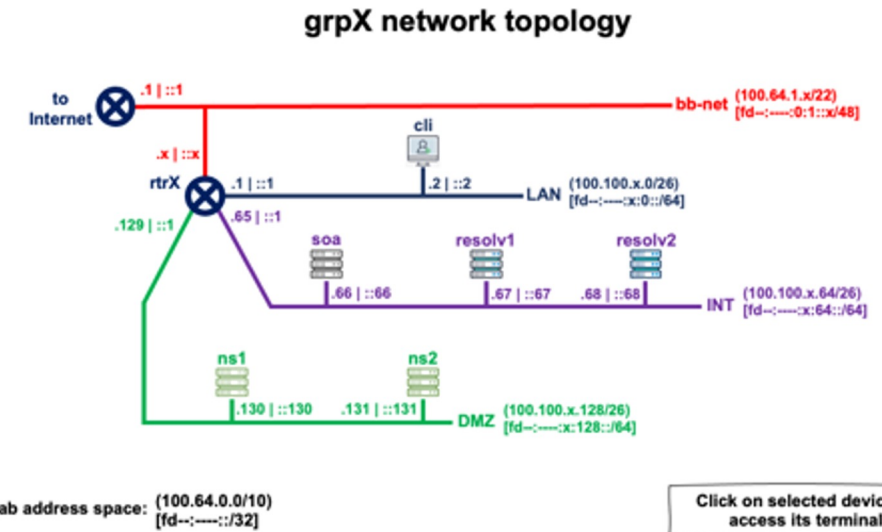
Parallel trainings (different audiences, configuration, and locations).

integration to ICANN learn (under analysis).

- 'Hardwareless':

hardware fault risk limitation: loss, physical damage, cabling, power issues, etc.

Helpful in locations with hardware restrictions or infosec cyber risk.

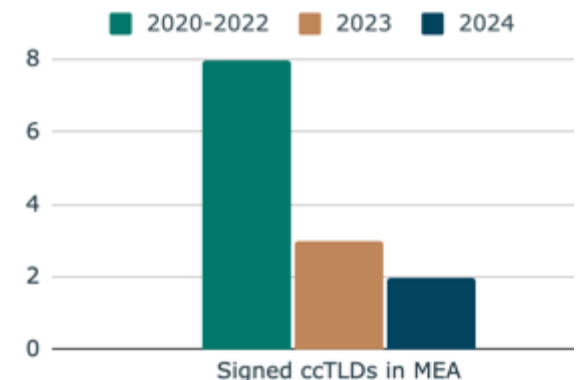


OCTO029: a guidebook for DNSSEC deployment

- Aims to assist ccTLD registry operators in understanding DNSSEC deployment at a TLD.
- Target audience:
 - TLD registry managers, staff, registrars, registrants
 - Operators who administer zones
 - Anyone willing to have an overview of how to deploy DNSSEC on a ccTLD.
 - Either you are already DNSSEC signed or not, you can glean insights on
- DNSSEC deployment checklist: simplify your DNSSEC journey with a list of adjustable action items.
- Download the guidebook : <https://www.icann.org/en/system/files/files/octo-029-12nov21-en.pdf>

Our DNSSEC (signing) related activities in MEA region

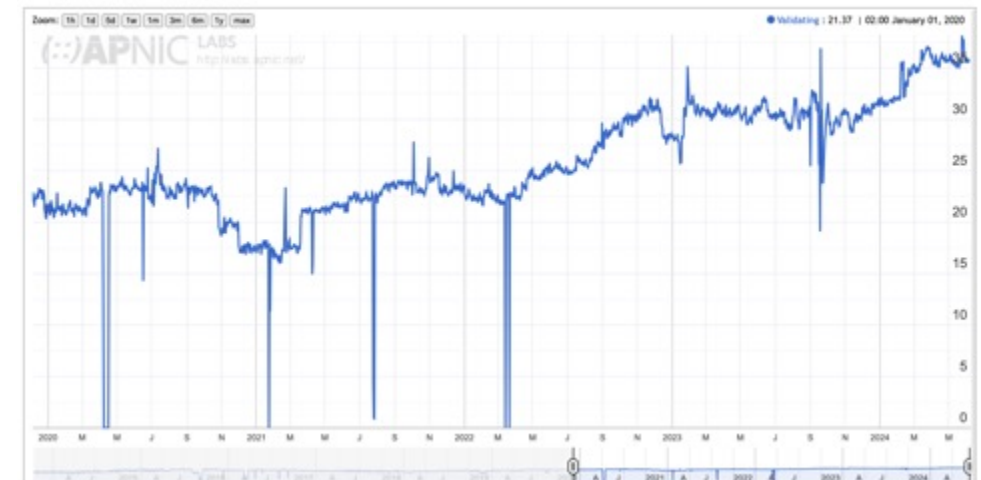
- Awareness and hands-on activities to hundreds of people (technical and non technical): explain – share best practices – build new technical skills – practice – guide.
- Technical support and collaboration with + 20 ccTLD to help
 - prepare for a DNSSEC journey: guidance to improve operational processes, fix zone configuration issues, elaborate strategy and steps to deployment (DNSSEC guidebook).
 - enhance their DNSSEC operations and level of adoption (signing down the DNS hierarchy).
- A “special” initiative: DNSSEC Roadshow of Coalition for Digital Africa (CDA) project
 - Provide the needed technical assistance to make the ccTLD signed
 - .bw is the first, work in progress with other ccTLDs.



Our DNSSEC (validation) related activities in MEA region

- Direct assistance to a large number of various size ISPs and MNOs in +25 countries :
 - help turn on DNSSEC validation in their infrastructure: prepare, activate, test, monitor.
 - +50 operators assisted: large MNOs (MTN, Orange, Vodafone), other operators, RENs, government entities, ... sometimes beyond DNSSEC.
 - +12% increase in DNSSEC validation rate in Africa (APNIC Labs).
 - Work in progress in Tanzania, Nigeria and other countries.

Use of DNSSEC Validation for Africa (XB)



Few observations

- Better understanding of the critical role of the DNS in the region and the need of securing the DNS in general.
- Greater interest in improving cybersecurity posture and resiliency within institutions and organizations in the region.
- More confidence in their capabilities to run a service beyond the “default” DNS.
- However, some operators tend to prefer running the DNS as “default”, mainly due to:
 - lack of confidence in themselves and absence of a rigorous operations management
 - low level of documentation combined to high staff turn over rate,
 - lower level of commitment, more outsourcing with less “control” over the infrastructure.The fact that DNS has for long not been seen as a “critical infrastructure”.
- leading to more technical assistance expectations from some stakeholders.
- There is still much to do and we should continue putting efforts together for more impact.

Way forward

- Systemic collaboration approach: documentation is key.
- Advocate and support for more collaboration in the region.
- Improve the messaging within the decision makers to help the technical teams in their challenge of getting effective support from their management.
- Continue providing a direct assistance to the stakeholders.
- Continue promoting the best current operational practices and help increase their adoption (KINDNS).

Engage with ICANN – Thank You and Questions



One World, One Internet

Visit us at icann.org



@icann



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



slideshare/icannpresentations



soundcloud/icann