

DNSSEC and Security Workshop Program
ICANN70 Virtual Meeting
Wednesday, 24 March 2021

Key to Level of Difficulty:

NOVICE = New to DNSSEC and want to learn more

INTERMEDIATE = Familiar with DNSSEC and how it works, but not of all concepts

EXPERT = Expert understanding of DNSSEC and extensive experience in deployment/implementation

DNSSEC and Security Workshop – Part I 09:00 -10:00 Local Cancun (14:00 – 15:00 UTC)
1. 09:00 – 09:015(14:00 – 14:15UTC) – Presentation: Dan York, <i>DNSSEC Workshop Introduction, Program, Deployment Around the World – Counts, Counts, Counts</i>
09:00 – 10:00 (14:15 – 15:00 UTC)
Moderator: Russ Mundy
2. 09:15 – 09:30 (14:15 – 14:30 UTC) – Moritz Muller, SIDN; Jins de John, TNOS: Retrofitting Post-Quantum Cryptography in Internet Protocols – A Case Study of DNSSEC
3. 09:30 – 09:45 (14:30 – 14:45 UTC) – Scott Hollenbeck, A Balanced DNS Information Strategy: Minimize at Root and TLD, Encrypt when Needed Elsewhere
09:45 – 10:00 (14:45 – 15:00 UTC) – Q&A
DNSSEC and Security Workshop – Part II 10:30 – 12:00 Local Cancun (15:30 – 17:00 UTC)
4. 10:30 – 11:40 (15:30 – 16:40 UTC) Panel Discussion: DNSSEC Provisioning Automation
Moderator: Steve Crocker
4.1. Steve Crocker, Shinkuro, Inc: DNSSEC Provisioning Automation Overview
4.2. Brian Dickson, GoDaddy: Status of GoDaddy support for CDS/CDNSKEY scanning
4.3. Steve Crocker & Shumon Huque, Salesforce: Introduction to the Multisigner Project
4.4. Ulrich Wisser, Swedish Internet Foundation, & Shumon Huque: Multi-Signer Protocols
4.5. Peter Thomassen, SSE - Secure Systems Engineering: Multisigner support at deSEC
4.6. Ulrich Wisser: Multisigner testbed
4.7. Priya Ravichander & Eric Osterweil, George Mason University: DNSKEY Transition Observatory
4.8. Eric Osterweil, Pouyan Fotouhi Tehrani, Matthias Waehlich & Thomas C. Schmidt: Anatomy of DNSSEC Transition
Moderator: Steve Crocker
5. 11:40 – 12:00 (16:40 – 17:00 UTC) – Mark Elkins, Posix: Registrar DS management for DNS providers
DNSSEC and Security Workshop – Part III 12:30 – 14:00 Local Cancun (17:30 – 19:00) UTC
12:30 – 13:30 (17:30 – 18:30 UTC)
Moderator: Fred Baker
6. 12:30 – 12:50 (17:30 – 17:50 UTC) – Edward Lewis, ICANN: Measuring ROA deployment in the DNS Core
7. 12:50 – 13:10 (17:50 – 18:10 UTC) – Edward Lewis, ICANN: Visualizations of DNSSEC deployment in the DNS Core
8. 13:10 – 13:25 (18: 10 – 18:25 UTC) – Viktor Dukhovni, NSEC3 iterations etc. High counts and opt-out considered harmful, avoid fixed salt
9. 13:25 – 13:40 (18:25 – 18:40 UTC) – Wes Hardaker, Intentionally Temporarily Insecure: the cheater’s guide to algorithm rolls
13:40 – 14:00 (18:40 – 19:00 UTC) – Q&A