

5th of May getting in y/our way

DNSSEC Incident at DE

2026-05-17

Peter Koch, DENIC eG

DNS-OARC 46, Edinburgh



Components

- ~17.9 million domains, ~420,000 signed delegations
- Near realtime zone *Updates* (sans zone file)
- Validation, consistency/integrity checks against live zone
- Two datacenters, one *Signer* with 3 HSMs per loc
 - Third signer design
 - Scheduled ZSK roll (pre-publish)

Incident & Mitigation

- 21:33 (UTC+2) DE signed with new ZSK 33834
- 21:57 incident declared
- Symptoms: `SERVFAIL` (Validating resolvers)
- HSMs using three different keys (1/3 `RRSIGs` correct)
- 01:15 zone signed with previous ZSK, fully distributed

Lessons Learned (preliminary)

- Improve QA, tests, alarms, rollback
- Review Dependencies
- Prepare Communication (status, NTA, ...)