



DNSSEC Technical Workshop

Implementation and Deployment Syllabus

- * DNS Fundamentals 101
- * a quick recap of DNS fundamentals * DNS Namespace
- * Delegation
- * Nameserver
- * DNS Message Format
- * Name Resolution
- * Caching
- * DNS Practice
- * Resource Records
- * DNSSEC Theory and History

- * DNS Threats
- * what is wrong with the good old DNS? * Spoofing
- * Man in the Middle Attacks
- * Betrayal of a trusted name server
- * Attack on authoritative data
- * the danger of Denial of Service Attacks

- * DNSSEC Introduction
- * DNS and DNSSEC History
- * TSIG and DNSSEC
- * Basics of Public Key Cryptography * DNSSEC Technical Overview
- * DNSSEC Record Types

- * DNSKEY (DNS Key Material)
- * RRSIG (Resource Record Signature) * NSEC (Next Secure)
- * DS (Delegation Signer)

- * Zone Signing Key (ZSK) and Key Signing Key (KSK) * the DNSSEC chain of trust

- * DNSSEC Infrastructure Requirements * signing tools
- * authoritative DNS Servers
- * Caching/Resolving DNS Servers

- * Middleboxes (Firewalls, Load-Balancer, NAT ...) * Application Requirements

- * DNSSEC Deployment
- * DNSSEC signing with BIND 9.6-ESV * creating keys
- * adding keys to a zone
- * signing a zone
- * test the setup
- * getting DS record in the parent zone * resigning a zone
- * Maintenance: Signature Expiration
- * Lab: DNSSEC zone signing

- * DNSSEC with BIND 9.7+
- * managing key timing values
- * DNSSEC automation
- * dynamic zones and DNSSEC
- * managing zone content with nsupdate * Lab: DNSSEC with BIND 9.7+

Course Syllabus

- * DNSSEC Validation
- * DNSSEC in DNS Messages
- * the AD and CD flags
- * DNSSEC Name resolution
- * DNSSEC Lookaside Validation (DLV)
- * Validating DNSSEC in the Internet
- * DNSSEC validation in Web-Browsers (Firefox, IE, Chrome)

- * A validating caching only configuration for BIND 9 * BIND as a caching server
- * named.conf setup (ACL, rndc, statistics channel) * getting the root-anchor

- * Verifying the root zones key
- * DNSSEC validation setup (BIND 9.6-ESV) * DNSSEC validation setup (BIND 9.7.0+)
- * Lab: DNSSEC validation with BIND

- * signing zones with NSEC3 * the NSEC3 Record
- * NSEC3 zone signing
- * Salt and Iterations

- * NSEC3 opt-out

- * DNSSEC Key rollover
- * the need of key rollover
- * Key rollover with pre-publication * Key rollover with double-signing * Emergency key rollovers
- * Algorithm Rollover
- * Switching DNS Operators

- * operator rollover (cooperative)

- * operator rollover (non-cooperative) * Lab: ZSK and KSK rollover

- * DNSSEC tools and troubleshooting
- * DNSSEC troubleshooting with "DIG"
- * Lab: find the cause of DNSSEC lookup failures
- * other DNSSEC tools (drill, unbound-host, dnssec-tools, zonecheck, OpenDNSSEC) * DNSSEC monitoring tools

- * DNSSEC in BIND 9.9

- * Hardware Security Modules (HSM) * the role of a HSM
- * selection criteria for HSM
- * SoftHSM - an HSM Emulator

- * using BIND with SoftHSM