IETF 123 - PQC DNSSEC Implementation

Andrea Jiménez-Berenguel	Universidad Carlos III de Madrid
Joe Harvey	Verisign
Javier Blanco-Romero	Universidad Carlos III de Madrid
Swapneel Sheth	Verisign
Ondřej Surý	ISC
Willem Toorop	NLNet Labs

IETF PQC DNSSEC Hackathon Efforts

- IETF-118
  - Introduced MTL mode open-source library
- IETF-120
  - Demonstrated SLH-DSA-MTL signatures on zone file
- IETF-121
  - Implemented draft-fregly-dnsop-slh-dsa-mtl-dnssec in NSD and Unbound
- IETF-122
  - PQC DNSSEC Metrics with MTL mode
    - Signed zones and ran authoritative service (mtlauthoritative.versignlabs.com)
    - Measured response size and query time across difference networks
    - Compare and contrast NIST PQC signature algorithms and MTL mode DNSSEC signatures
  - PQC for DNSSEC – New Kids on the Block
- IETF-123
  - PQC DNSSEC implementations
  - POC Service at pqc.verisignlabs.com

Name server implementations

Open-Source implementations:

Reference Open-Source	Link	Algorithms
MTL reference library	https://github.com/verisign/MTL	MTL mode with SLH-DSA
MTL LDNS library	https://github.com/verisign/mtl-mode-ldns	RSA, ECDSA, ML-DSA[1], FL-DSA[1], SLH-DSA[1], Mayo I/II[1], SQI Sign[1], Hawk[1], SNOVA[1] , SLH-DSA w/MTL mode[1]
NSD [authoritative name server]	https://github.com/NLnetLabs/nsd/pull/397	RSA[2], ECDSA[2], ML-DSA[2], FL-DSA[2], SLH-DSA[2], Mayo I/II[2], SQI Sign[2], Hawk[2], SNOVA[2] , SLH-DSA w/MTL mode[2][3]
Unbound [recursive resolver]	https://github.com/verisign/mtl-mode-unbound	RSA, ECDSA, SLH-DSA w/MTL mode[3]
BIND [authoritative and recursive resolver]	TBD	RSA, ECDSA, FL-DSA[1], Mayo [1], SQI Sign[1], Hawk[1], ANTRAG-512, SLH-DSA w/MTL mode[1]
Core DNS [authoritative]	https://github.com/fjblanco/mtl_coredns_plugin	RSA, ECDSA, ML-DSA[1], FL-DSA[1], SLH-DSA[1], Mayo I/II[1], SNOVA[1] , SLH-DSA w/MTL mode[1]

1 - Enabled at compile time, depends on additional cryptographic libraries
2 - When signed with LDNS.
3 - Includes POC for MTL mode EDNS option.

Next Steps

Will be discussing this and more at the PQ DNSSEC side meeting Thursday, July 24th – 8:30 am.