IETF 124 - PQC DNSSEC MTL Mode Update

Joe Harvey Verisign
Swapneel Sheth Verisign

PQC DNSSEC Strategy Draft

- New draft document (draft-sheth-pqc-dnssec-strategy) to capture the direction and momentum from the PQC DNSSEC side meeting at IETF 123.

- Aligns with the presentations at NIST and DNS OARC on PQC DNSSEC strategy
  - NIST 6th PQC Standardization Conference
  - DNS OARC 45

Updates to MTL Mode

- Updated the MTL Mode specification to allow for more underlying signature schemes.
  - No longer reliant on properties of SLH-DSA keys
  - Streamlined the process for adding support for new signature schemes
  - Added support for ML-DSA
  - Planning on supporting other PQC schemes as they get standardized

- Update MTLLIB (version 1.2.0) to allow for signatures using the SLH-DSA and ML-DSA signature schemes

Name server implementations

Reference Open-Source	Link	Algorithms
MTL reference library	https://github.com/verisign/MTL	MTL mode with SLH-DSA and ML-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), ML-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) , ML-DSA w/MTL mode(2)(3)
Unbound [recursive resolver]	https://github.com/verisign/mtl-mode-unbound	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)), ML-DSA w/MTL mode(2)(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)

Reference Source	Link	Algorithms
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 presenting at DNSOP to help determine where the building blocks for PQC DNSSEC should be standardized.