IETF 122 - PQC DNSSEC Metrics with MTL Mode

Joe Harvey (jsharvey@verisign.com)
Swapneel Sheth (ssheth@verisign.com)

MTL Mode DNSSEC

Draft Specifications

Document	Purpose
draft-fregly-dnsop-slh-dsa-mtl-dnssec	Describes the application of MTL mode to DNSSEC.

Open-Source implements MTL mode:

Reference Open-Source Implementation	Link
MTL LDNS library	https://github.com/verisign/mtl-mode-ldns
MTL reference library	https://github.com/verisign/MTL
NSD [authoritative resolver]	https://github.com/NLnetLabs/nsd/pull/397
Unbound [recursive resolver]	https://github.com/verisign/mtl-mode-unbound

IETF 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
    - NSD providing full and condensed signatures based on EDNS option flag
    - Unbound providing verification of SLH-DSA-MTL signatures
      - Verifies condensed signatures from cached ladders
      - Requests full signatures for records that do not have a cached ladder
- IETF-122
  - 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

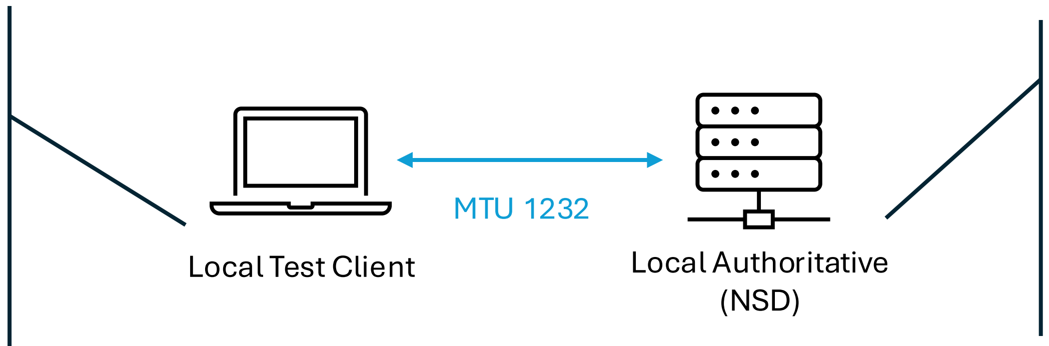
Test Environment Setup

Test Signing Scripts

- Generate a key for each algorithm
- Sign the test zone
- Verify the test zone
- Collect metrics on time, size, and validity

Test Query Scripts

- Warmup query
- One set of tests per algorithm
- Collect metrics on response time, size, and messages


MTU 1232

Local Test Client

Local Authoritative
(NSD)

Signed Zone Files

(one per algorithm)

- RSA
- ECDSA
- FL-DSA-512
- ML-DSA-44
- SLH-DSA-SHA2-128
- SLH-DSA-SHAKE-128
- SLH-DSA-MTL-SHA2-128
- SLH-DSA-MTL-SHAKE-128

IETF-122 Metrics

Response Size

Algorithm	Condensed Signature (bytes)	Full Signature (bytes)
ecdsa		277.5
fl-dsa		979.3
ml-dsa		1932
rsa		558.5
slh-dsa-sha		6020
slh-dsa-shake		6025
slh-dsa-mtl-sha	350	6144

Query/Response Time

Algorithm	TCP (seconds)	UDP (seconds)
ecdsa	0.597641766	0.304942071
fl-dsa	0.587359607	0.298148235
ml-dsa	0.572127938	Truncated
rsa	0.559029245	0.294401248
slh-dsa-sha	1.011730075	Truncated
slh-dsa-shake	0.660917719	Truncated
slh-dsa-mtl-sha		
Condensed	0.623684605	0.283434391
Full	0.669570049	Truncated

Thanks

Caspar Schutijser – SIDN Labs
Wataru Ohgai - JPNIC

Next Steps

- Will be discussing this and more at the PQ DNSSEC side meeting

  Tuesday March 18th, 2025

  9:30-10:30 (local Bangkok time)

  Meeting Room 2