PQ DNSSEC with MTL Mode Metrics and Observations

IETF-122 PQ DNSSEC Research Side Meeting

March 18th, 2025

Joe Harvey (jsharvey@verisign.com)

Swapneel Sheth (ssheth@verisign.com)

MTL Mode Specifications

Document	Version	URL
draft-harvey-cfrg-mtl-mode	04	https://datatracker.ietf.org/doc/draft-harvey-cfrg-mtl-mode/
draft-harvey-cfrg-mtl-mode-considerations	00	https://datatracker.ietf.org/doc/draft-harvey-cfrg-mtl-mode-considerations/
draft-fregly-dnsop-slh-dsa-mtl-dnssec	03	https://datatracker.ietf.org/doc/draft-fregly-dnsop-slh-dsa-mtl-dnssec/

MTL Mode Open Source

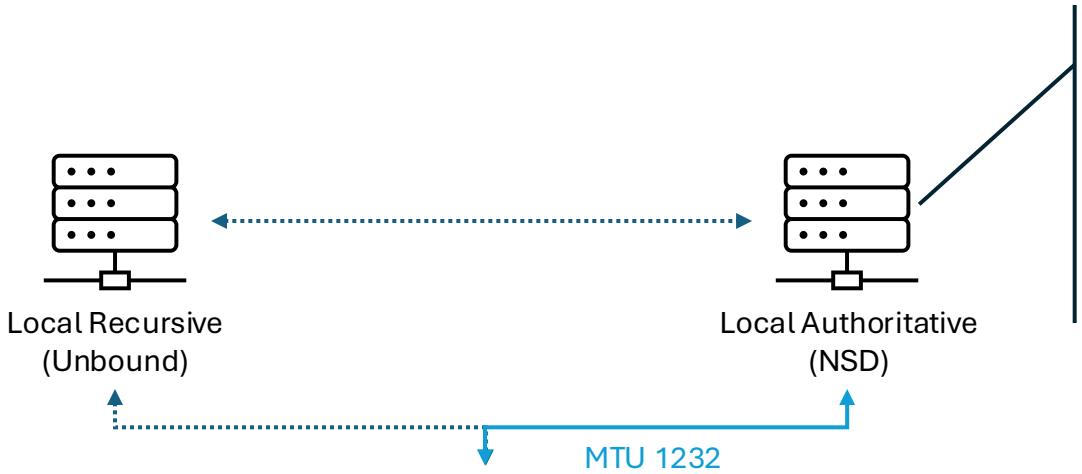
Application	Repository
Keygen/Zone Signing/Zone Verifying with MTL mode	https://github.com/verisign/mtl-mode-ldns
NSD Authoritative with MTL Mode Support	https://github.com/NLnetLabs/nsd/pull/397
Unbound with PQC MTL Validation	https://github.com/Verisign/mtl-mode-unbound
MTL Reference Library	https://github.com/verisign/mtl

Intellectual Property

- Verisign announced a public, royalty-free license to certain intellectual property related to the Internet-Drafts
- IPR declarations 6174-6176, 6240-6242, and 6501 give the official language

https://datatracker.ietf.org/ipr/search/?submit=draft&id=draft-harvey-cfrg-mtl-mode
https://datatracker.ietf.org/ipr/search/?submit=draft&id=draft-harvey-cfrg-mtl-mode-considerations
https://datatracker.ietf.org/ipr/search/?submit=draft&id=draft-fregly-dnsop-slh-dsa-mtl-dnssec

Test Environment Setup



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

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

Signer and NSD Host Configuration
CPU: 4 core Intel Xeon – 2.30 GHz
Ram: 32 GB
OS: RedHat 8.10
Compiler: Gcc version 13.3.1
with optimizations –O2 enabled

Zone File Signing And Verifying

Zone File Signing And Verifying

Sample zone with 1500 Delegated Sub-Domains

Algorithm	Time to Sign (seconds)	Time to Verify (seconds)	Signed Zone Size (MB)	Public Key Size (bytes)
RSA	2.4	0.4	2.72	260
ECDSA	0.4	0.7	2.06	64
FL-DSA-512	1.5	0.6	4.36	897
ML-DSA-44	0.7	0.9	11.13	1312
SLH-DSA-SHA2-128	534.5	2.7	32.15	32
SLH-DSA-SHAKE-128	1058.4	3.1	32.22	32
SLH-DSA-MTL-SHA2-128	0.8	0.4*	2.96*	32
SLH-DSA-MTL-SHAKE-128	1.2	0.4*	3.04*	32

* - Two full signatures, one for DNSKEY (with KSK) and one for the SOA record (with ZSK). All other signatures are condensed.

Zone File Signing And Verifying

Sample zone with1500 Delegated Sub-Domains

Observations

1. ECDSA is the most efficient algorithm for signing, although the MTL based signatures are not far behind.

2. MTL based signatures largely mitigate the larger elements of the SLH-DSA algorithms while keeping the beneficial small public key sizes.

3. ML-DSA is popular right now for WebPKI, although the public key size means that the ZSK or KSK will not fit in a UDP DNS response (based on MTU).

4. DS records support SHA256 hashes but do not support SHAKE.

Query/Response With PQC DNSSEC

Query/Response With PQC DNSSEC

			Message Size				Query Time (10 samples)			RR Count in response				
Protocol	Algorithm	Record	Query (bytes)	Response (bytes)	Truncated	EDNS(0) MTL Full Signature	Average (ms)	Median (ms)	Stdev (ms)	RRSIG	NS	A	DS	AAAA
UDP	RSA	NS	54	715			1.53	1.50	0.10	1	1	5	1	5
TCP	RSA	NS	54	715			2.21	2.18	0.25	1	1	5	1	5
UDP	ECDSA	NS	56	527			1.59	1.58	0.08	1	1	5	1	5
TCP	ECDSA	NS	56	527			2.24	2.31	0.17	1	1	5	1	5
UDP	FL-DSA-512	NS	57	1120			1.54	1.52	0.06	1	1	5	1	5
TCP	FL-DSA-512	NS	57	1120			2.30	2.40	0.22	1	1	5	1	5
UDP	ML-DSA-44	NS	60	150	TRUE		0.82	0.84	0.07	0	1	0	0	0
TCP	ML-DSA-44	NS	60	2891			1.77	1.71	0.15	1	1	5	1	5
UDP	SLH-DSA-SHA2-128	NS	62	152	TRUE		0.82	0.81	0.05	0	1	0	0	0
TCP	SLH-DSA-SHA2-128	NS	62	8331			1.80	1.75	0.13	1	1	5	1	5
UDP	SLH-DSA-SHAKE-128	NS	64	154	TRUE		0.92	0.81	0.25	0	1	0	0	0
TCP	SLH-DSA-SHAKE-128	NS	64	8335			1.86	1.85	0.06	1	1	5	1	5
UDP	SLH-DSA-MTL-SHA2-128	NS	58	684			1.68	1.69	0.10	1	1	5	1	5
UDP	SLH-DSA-MTL-SHA2-128	NS	62	148	TRUE	TRUE	0.85	0.86	0.06	0	1	0	0	0
TCP	SLH-DSA-MTL-SHA2-128	NS	58	684			1.70	1.59	0.28	1	1	5	1	5
TCP	SLH-DSA-MTL-SHA2-128	NS	62	8700		TRUE	1.73	1.73	0.09	1	1	5	1	5

Queries are for a NS record using the network default MTU of 1232 bytes.

Query/Response With PQC DNSSEC

Observations

1. Assuming the default MTU of 1232 the following algorithms work over UDP and TCP: Classical (RSA, ECDSA) and PQC (FL-DSA-512, SLH-DSA-MTL-SHAXX-128)

   Note: NSEC3 requires multiple signatures in the response which may result in truncated responses, even if normal responses fit.

2. MTL does have a retry cost when a condensed signature does not have a cached ladder. The query for the full signature over UDP will always be truncated and need to be requested over TCP.

3. UDP truncated full signatures take less processing time and are smaller than condensed signatures over both UDP and TCP responses, which reduces potential attacks. (e.g. less memory lookups and less to transfer over wire)

Open Questions

- How can we best optimize MTL for small response sizes and minimal retries?
- How do other resolvers perform with these zones?
- What impact do forwarding proxies have on this model?
- What are the impacts on resource consumption and DoS resilience?