A post-quantum cryptography strategy for DNSSEC

IETF-123 PQ DNSSEC Research Side Meeting
July 24th, 2025

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

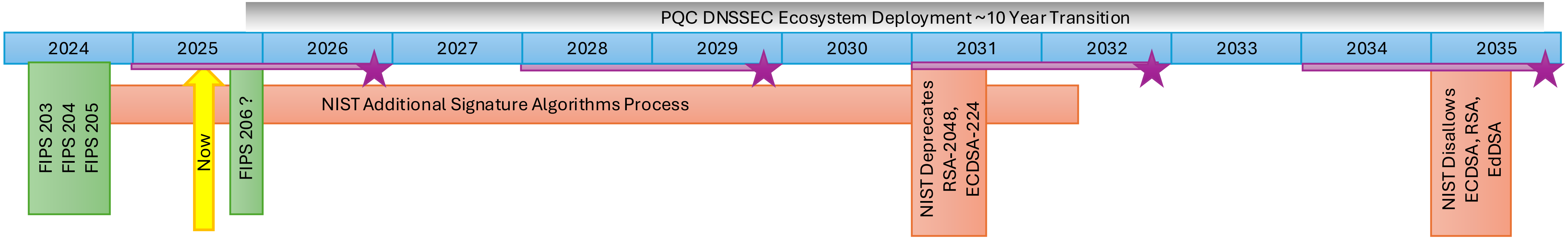
PQ DNSSEC Context

- DNSSEC currently uses digital signature algorithms that are at risk of compromise by quantum computers.

- The PQC signature algorithms that are currently standardized (e.g., ML-DSA in FIPS 204 and SLH-DSA in FIPS 205) have large signature sizes relative to DNSSEC's constraints.

- NIST's "onramp" call for additional PQC signature algorithms intends to standardize algorithms with smaller signature sizes – but they likely will be based on newer cryptographic assumptions.

Challenge 1 – Deployment Lifecycles



PQC DNSSEC Ecosystem Deployment ~10 Year Transition

2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035

FIPS 203
FIPS 204
FIPS 205

Now

FIPS 206 ?

NIST Additional Signature Algorithms Process

NIST Deprecates
RSA-2048,
ECDSA-224

NIST Disallows
ECDSA, RSA,
EdDSA

▭ DNS Root Key Publication Period

★ Planned DNS Root Key Rollover

Current Community Efforts

IETF

PQ DNSSEC Research Side Meetings (https://wiki.ietf.org/en/group/pq-dnssec)

- Randomized simulation of SLH-DSA-MTL's impact on reducing PQ-DNSSEC signature sizes
- PQ DNSSEC with MTL Mode (Verisign) - Metrics and Observations
- Feasibility of the new Post Quantum Cryptography for DNSSEC
- Field study on mitigating the costs of Post-Quantum DNSSEC with Merkle Trees
- PQ DNSSEC with MTL Mode
- A testbed to evaluate post-quantum cryptography in DNSSEC

Hackathons

- 122 – PQC for DNSSEC
- 122 – PQC DNSSEC Metrics with MTL Mode
- 121 - Experiments with MTL Mode in DNS Resolvers
- 120 - Stateless Hash-Based Signatures in Merkle Tree Ladder Mode (SLH-DSA-MTL) for DNSSEC
- 118 - MTL Mode Experiments

Documents

- Stateful Hash-based Signatures for DNSSEC
- Merkle Tree Ladder (MTL) Mode Signatures
- Stateless Hash-Based Signatures in Merkle Tree Ladder Mode (SLH-DSA-MTL) for DNSSEC

Other Venues

ICANN 70 Workshop

- The Impact of Post-Quantum Cryptography on DNSSEC

PQ Net Workshop

- The Challenges in Using PQC for DNSSEC

ACM SIGCOMM

- Retrofitting post-quantum cryptography in internet protocols: a case study of DNSSEC

SPACE

- Post-quantum DNSSEC over UDP via QNAME-Based Fragmentation

IEEE

- Securing Post-Quantum DNSSEC Against Fragmentation Mis-Association Threat

Real World Crypto Conference

- Field Experiments on Post-Quantum DNSSEC

Network Traffic Measurement and Analysis Conference

- Evaluating Post-Quantum Cryptography in DNSSEC Signing for Top-Level Domain Operators

Masters Thesis

- Beernink, G.J. - Taking the Quantum Leap: Preparing DNSSEC for Post Quantum Cryptography
- Gortzen, J. - Enabling Post-Quantum Signatures in DNSSEC: One ARRF at a time
- Surý, O. - Feasibility of the new Post Quantum Cryptography for DNSSEC

Challenge 2 – Operational Constraints

- The User Datagram Protocol (UDP) can support packets of up to 65,535 bytes in principle, a typical practical limit in DNS implementations is 1232 bytes.
- Signature size range (typical) by standardized algorithm.

Classical		Post-Quantum Algorithm	
RSASHA256	ECDSAP256SHA256	ML-DSA	SLH-DSA
128-256 bytes	64 bytes	2420-4627 bytes	7856-49,856 bytes

- The comparison of packet size to signature size understates the challenge.
- DNS responses can in some cases include up to three signatures (an NSEC3 "non-existence" response).
- During key rollovers, a DNS response may include signatures under both a previous and a new key.

Proposed diversity strategy

✗ DO NOT wait for NIST’s onramp effort to conclude before starting to prepare, anticipating the availability of one or more additional signature algorithms more suitable for DNSSEC in terms of signature size.

✓ Find a way to deploy the currently standardized PQC algorithms.

✓ A post-quantum diversity strategy for DNSSEC that involves at least one algorithm from two sets with complementary properties.

- At least one conservatively designed algorithm
- At least one low-impact drop-in algorithm

✓ DNS operators choose which supported algorithm to use to sign a particular zone.

Finding a Way

Select a high-performance signature algorithm to ensure **routine performance** with a conservative signature algorithm for **resilient fallback**. Enables the potential for newer low-impact, algorithms while minimizing overall risk of adopting something newer and less proven.

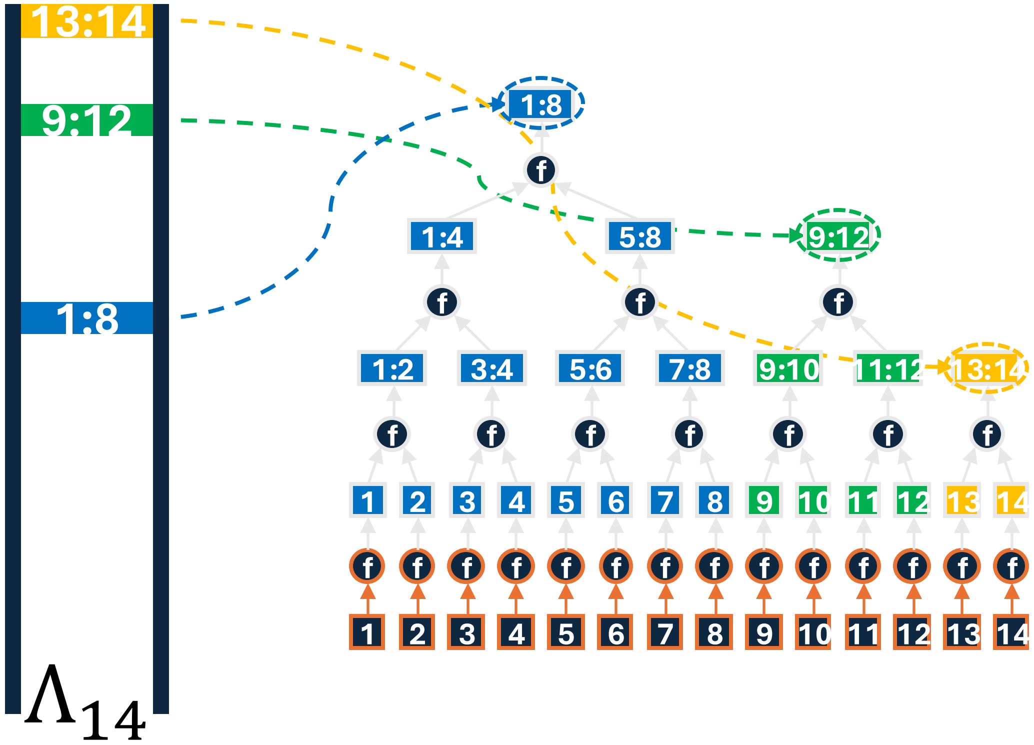
Routine Performance - Low-impact, drop-in algorithm used same way as traditional signature algorithms.

- No recommendation yet for low-impact, “drop-in” algorithm

Resilient Fallback - Conservatively designed algorithm unlikely ever to need to be replaced.

- Propose SLH-DSA as the choice for conservatively designed algorithm
- Open to considering ML-DSA as well as Falcon
- Open to HSS-LMS and XMSS^MT, while noting that state management introduces an operational risk

MTL Mode : Reducing the Operational Impact



- Rather than signing individual messages, MTL mode signs Merkle Tree Ladders
- Messages are authenticated with Merkle proofs relative to ladders
- Ladders provide backward compatibility since they can verify Merkle proofs constructed relative to future ladders too
- Useful for signature series that sign multiple things at one time. (DNSSEC, OCSP, etc.)

IPR

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

Next Steps

- Continued community participation in PQC DNSSEC discussion around low-impact drop-in algorithms.
- Analyze DNS resource consumption attacks (along the lines of KeyTrap) and impacts on PQC algorithms.

Given a better understanding of the operational impact of a broad range of PQC signature algorithms on DNSSEC, including attacks and countermeasures, the DNS community can then proceed to selecting specific algorithms for future use.

Conclusions

- We should aim for a goal where any standardized PQC signature algorithm can be integrated into DNSSEC in principle.
  - *Perhaps combined with a mode of operation that mitigates its operational impact such as MTL Mode*

- PQC DNSSEC should support a conservatively designed algorithm and a low-impact, drop-in algorithm.

- With NIST deadlines looming for current DNSSEC algorithms, action is needed to ensure the DNS community has time to migrate to PQC.