Post-Quantum DNSSEC

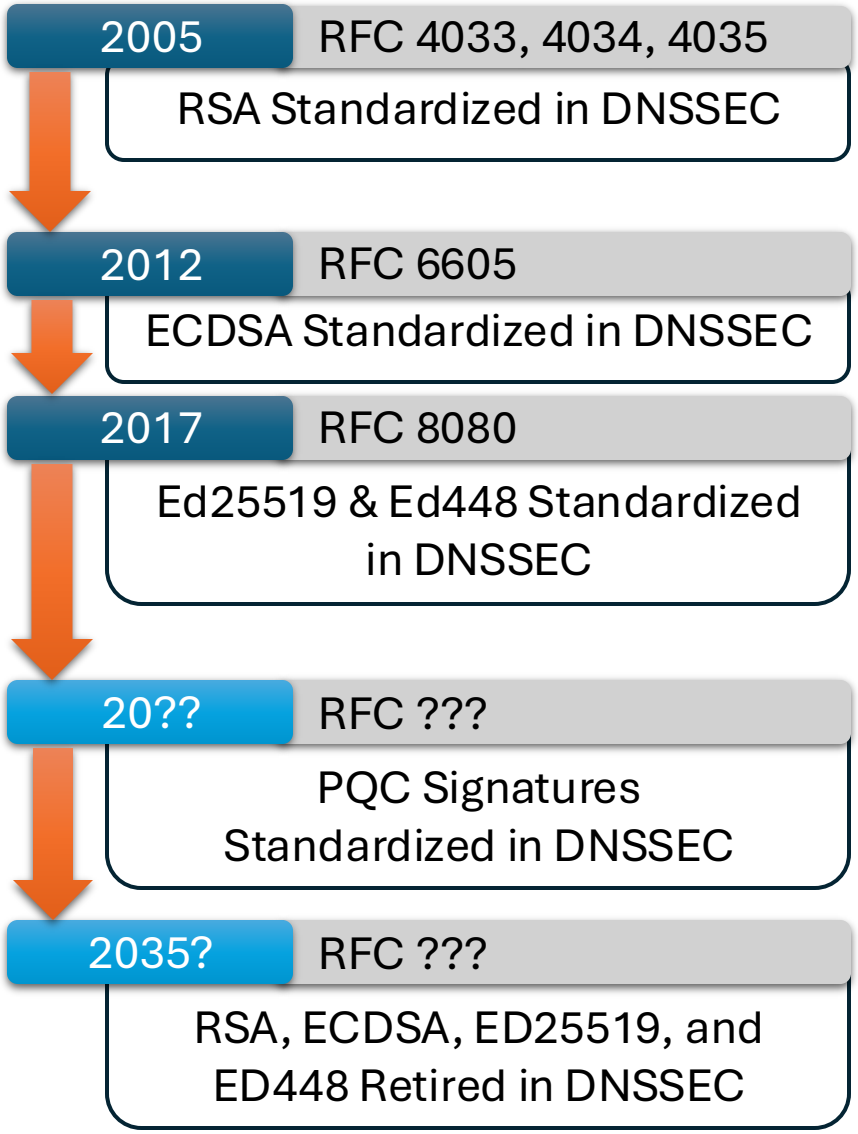
IETF-124
November 7, 2025

Taejoong (tijay) Chung[1] Joe Harvey[2]
Benno Overeinder[3] Swapneel Sheth[2]

[1]Virginia Tech
[2]Verisign Labs
[3]NLnetLabs

The Motivation

- The Domain Name System Security Extensions (DNSSEC) help protect the integrity of DNS data.
- Large-scale quantum computing threats mean the current algorithms may one day no longer suffice.
- As has been done over the last 20 years, new standards are needed to introduce PQC secure algorithms.



The Challenge

Transitioning DNSSEC to PQC is shaped by two realities.

1. New DNSSEC algorithm/s require wide adoption and global coordination.

2. PQC algorithms such as the National Institute of Standards and Technology's (NIST's) SLH-DSA produce much larger signatures than today's DNS was designed to handle.
   - Large signatures risk fragmentation, performance bottlenecks, and operational complexity.

The transition is therefore not just a cryptography problem—it is equally an engineering and operations challenge.

PQC Community

- PQC DNSSEC Side Meeting
  - A year of PQC DNSSEC research presentations
- Interoperability Studies
  - Hackathons – IETF-123, IETF-122 (New Algorithms) (MTL Mode)
  - Open-source code
    - MTL Reference Library*
    - LDNS Library with PQC Algorithms
    - NSD Authoritative Name Server
    - Unbound Recursive Resolver
    - BIND Authoritative and Recursive Resolver
  - Other Public Repositories
    - Core DNS Authoritative Resolver
- Operational Measurements
  - DNS OARC 45

*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

A Strategy

- Introduce two classes of PQC algorithms in DNSSEC
  - **Routine Performance** - One algorithm that delivers efficient performance in everyday use which may be based on less proven new cryptographic algorithms.
  - **Resilient Fallback** – A conservative PQC algorithm that has different and more trusted properties than the routine performance algorithms. A promising candidate for the fallback is SLH-DSA, a hash-based algorithm with strong security assurances.

- Reducing the impact:
  - Apply techniques like Merkle Tree Ladder (MTL) mode, which uses a Merkle tree structure to amortize the cost of large signatures across the message set.

- We have published draft-sheth-pqc-dnssec_strategy, per consensus at the PQC DNSSEC side meeting in Madrid, to capture the strategy for resilience and cryptographic agility in PQC DNSSEC.

Recent Engagements

- NIST 6th PQC Conference
  - Post-Quantum Diversity for DNSSEC: Routine Performance, Resilient Fallback
- DNS OARC
  - Measurement of PQC DNSSEC for Routine Performance, Resilient Fallback

Where does this work belong?

- Previously DNSEXT worked on DNSSEC mechanisms like NSEC3.
  - Handled not only the DNSSEC components but also the hashing constructs for NSEC3.
  - Do we need a new group like this to take on PQC DNSSEC and MTL Mode?
  - CFRG was not interested in taking on this work.

- DNSOP has since handled most of the DNSSEC work
  - E.g. draft-ietf-dnsop-must-not-sha1
  - May be home for DNSSEC components but may not be best place for Merkle Tree constructions?

- PLANTS is being formed for work which includes a Merkle tree construct.
  - Should this be more generic to handle more than Merkle trees for certificates?
  - Is this the right place for Merkle trees for DNSSEC?