Research Agenda for a Post-Quantum DNSSEC

Andrew Fregly

OARC 40 –February 16-17, 2023

VERISIGN

Drivers for DNSSEC-Related Ecosystem Research

DNSSEC needs long-term cryptographic resiliency that addresses the long lead time to roll out new algorithms

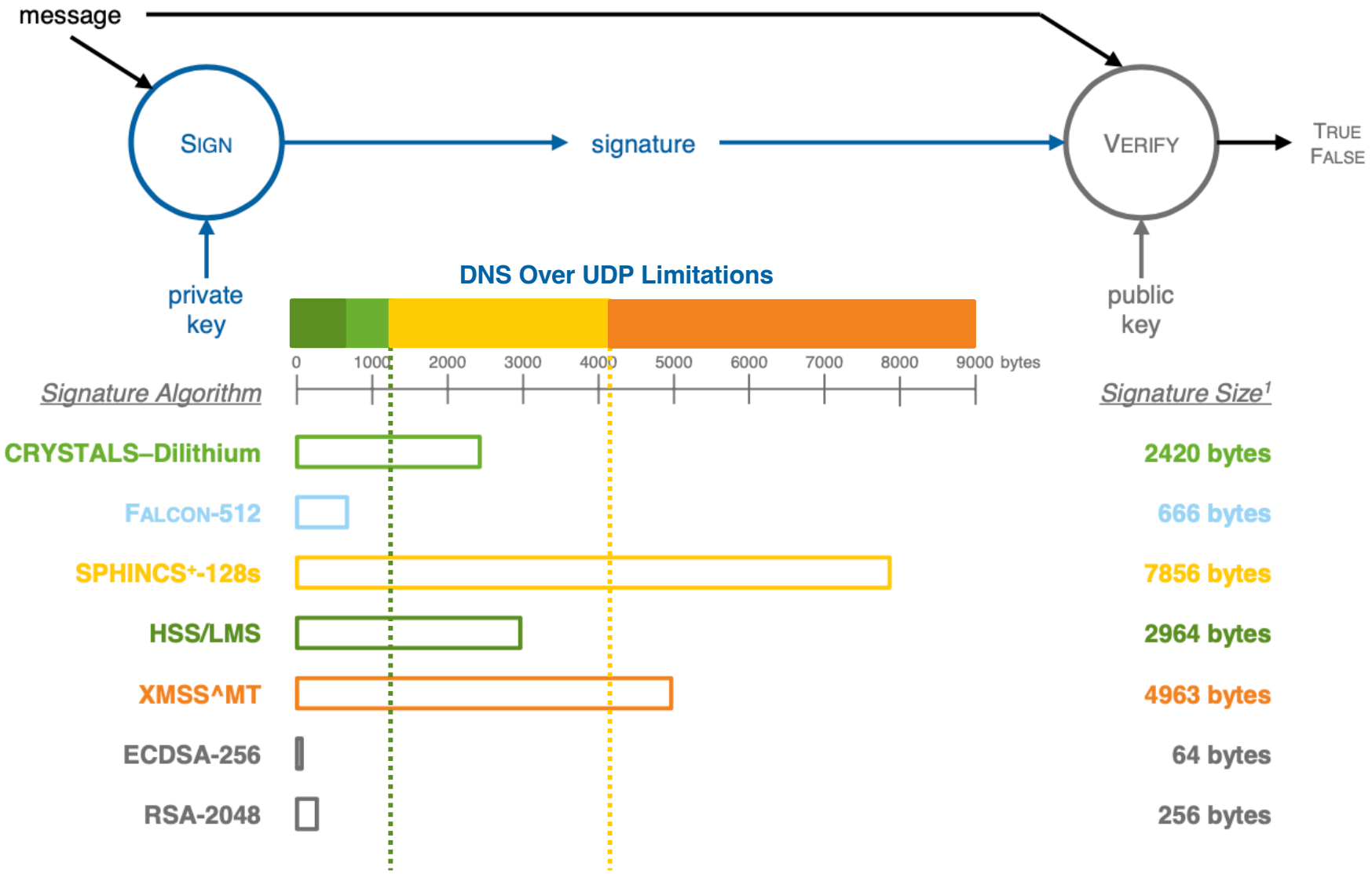
NIST's chosen Post Quantum Cryptographic (PQC) signature algorithms may have significant size impact on DNSSEC, transport, memory and processing

There are multiple approaches for addressing the issues PQC algorithms present to DNSSEC with significant pros and cons for these approaches

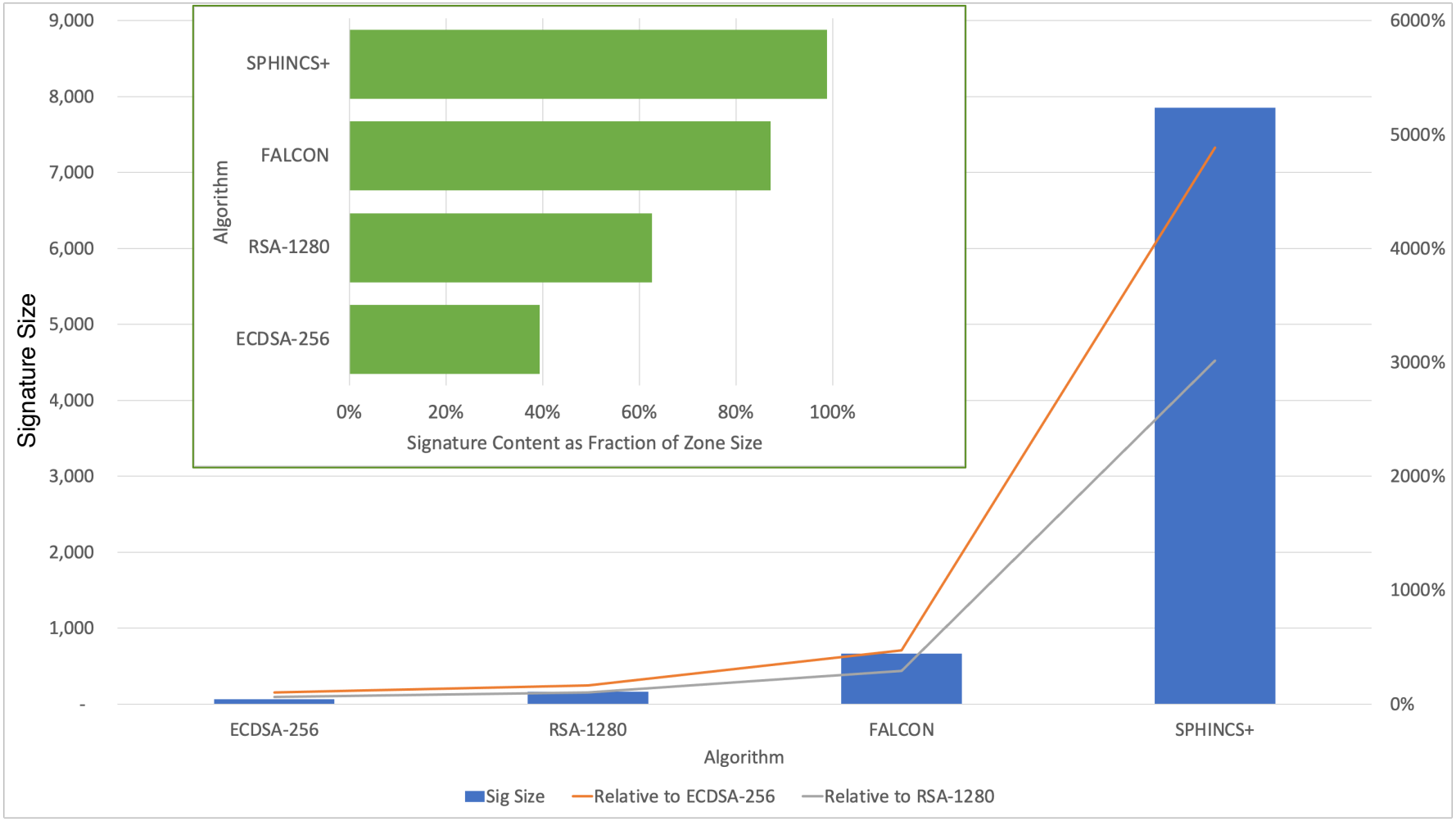
Collaborative multi-stakeholder involvement in research and modeling is needed to inform the DNSSEC PQC standardization and transition agenda

NIST PQC Signature Algorithms Relative to UDP MTUs

666- to 7856-Byte Minimum Signature Sizes with Example Parameters[1]



Signature Size Impact on Example Fully Signed TLD Zone



Approaches to Minimize Size Impact on UDP Transport

Smaller - Merkle Tree Ladder Mode of Operation for Small Signature Size Impact[3]

Selective - Algorithm Negotiation*

Shift - Out-of-Band Retrieval of Keys and/or Signatures

Skip - Proactive Caching

Split - Split Large Keys/Signatures Across RRs**

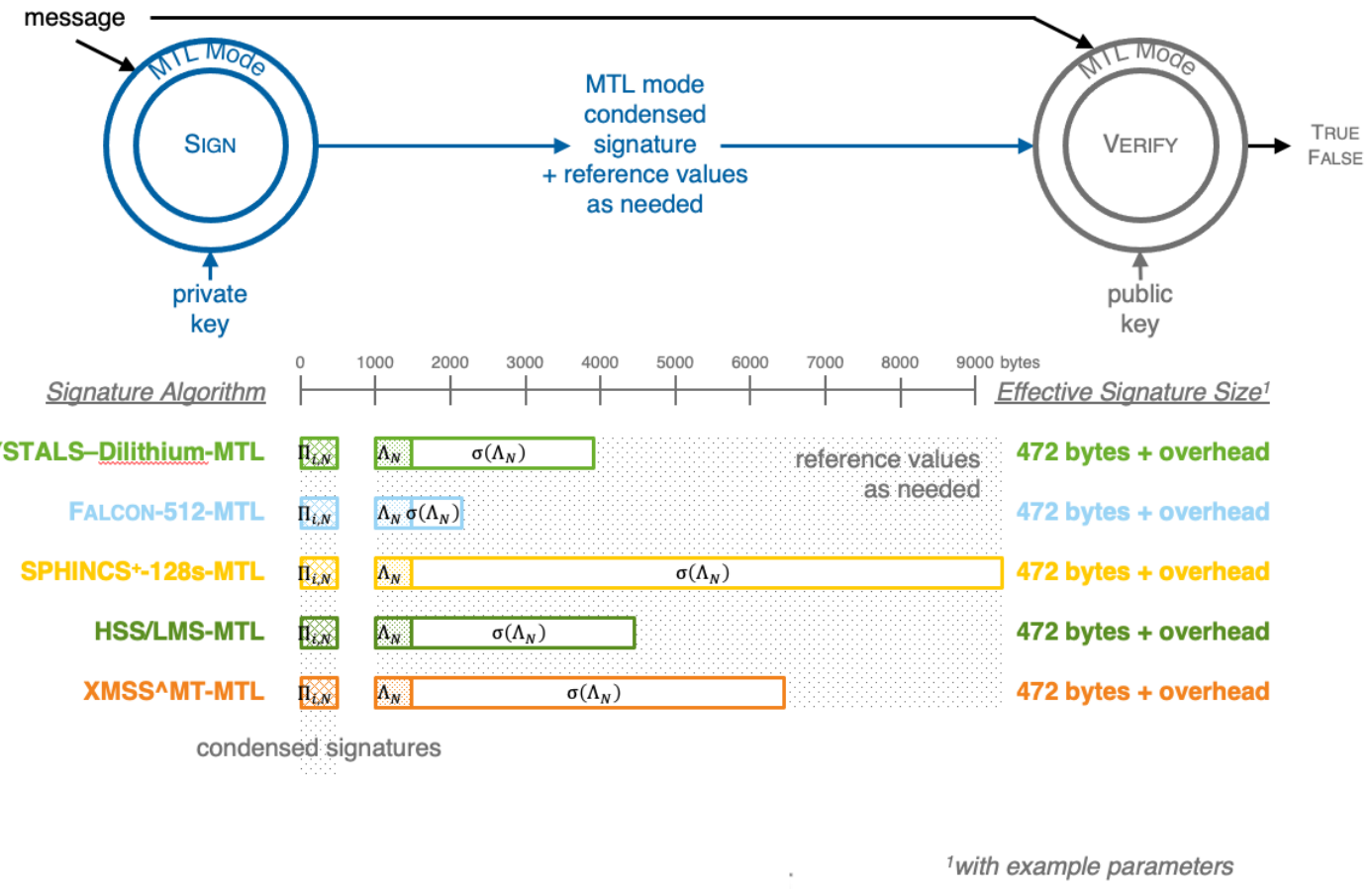
* Based on expired draft “Algorithm Negotiation in DNSSEC”[2]
**One proposed approach is “Post-Quantum Signatures in DNSSEC via Request-Based Fragmentation”[3]

Signature Size Impact Reduction using Merkle Tree Ladder Mode of Operation

See Burt Kaliski's Talk for the NIST Fourth PQC Standardization Conference[4]

Summary: Reducing Effective Size Impact with MTL Mode

Send Condensed Signatures, Look Up Reference Values As Needed



Research Agenda: DNS Ecosystem Metrics

Deployment Analytics: device types and characteristics; roles (stub, resolver, authoritative nameserver); algorithms; environmental constraints such as network limitations; software used for resolution and nameserver operations; resolver in-memory cache sizes; authoritative nameserver in-memory database sizes; supportable transports

UDP Networking Path MTU Analytics: stub to resolver; resolver to resolver; resolver to authoritative

Analyze DNS/DNSSEC Query and Response Traffic: stub to resolver; resolver to resolver; resolver to authoritative interactions

- Composition, size, and response times of DNS queries and responses: including details for overall traffic and DNSSEC-related traffic
- DNS response time impact on use cases (browsing, web services, mobile, IoT,...)
- Truncation and Fragmentation Analysis: overall traffic; DNSSEC related traffic; failures; retries
- Session Based Protocols: percentage of traffic; response times; session setup and teardown metrics; failures

Analyze Zones Based on Domain Level (root, TLD, lower levels)

- DNSSEC related RRs; signature algorithms; frequency of updates; zone signing metrics

Research Agenda: Modeling for Projected Impact of PQC Algorithms and DNS Protocol Changes

- **Base on DNS Ecosystem Metrics Research**
- **Project Impacts:** to processing, network requirements, costs, and dependencies
  - Model impact of PQC algorithms
  - Model impact of proposed protocol changes
- **Modeling to Create Snapshot Projections:**
  - Base on transition timelines for DNS ecosystem components

References

1 – NIST CSRC, “PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates”, NIST, July , https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4.

2 – S. Huque, H. Shulman, S. Kerr, "Algorithm Negotiation in DNSSEC", July 2018, https://datatracker.ietf.org/doc/draft-huque-dnssec-alg-nego/03/.

3 – J. Goertzen, D. Stebila, “Post-Quantum Signatures in DNSSEC via Request-Based Fragmentation”, University of Waterloo, November 2022, https://s3.amazonaws.com/files.douglas.stebila.ca/files/research/papers/EPRINT-GoeSte22.pdf

4 – B. Kaliski, “Merkle Tree Ladder Mode: Reducing the Size Impact of NIST PQC Signature Algorithms in Practice”, NIST Fourth PQC Standardization Conference, December 2022, https://csrc.nist.gov/Presentations/2022/merkle-tree-ladder-mode

powered by

VERISIGN®