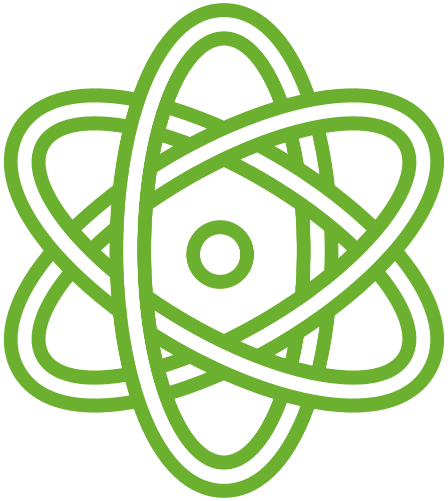
Projecting Impact of Post Quantum Cryptography on Registry Operations

Andrew Fregly

ROW11 - June 21, 2022

VERISIGN

The Quantum Threat?



The anticipated advent of Quantum Computers, capable of breaking current widely used public key cryptographic algorithms, is driving activities that will lead to development and adoption of new Post-Quantum Cryptographic algorithms within Internet security protocols.

Derivation of Mosca's Model[1]:

Threat Exposure Time = (Migration Time + Shelf Time) - Threat Timeline

Threat Timeline: Expert opinions range from 15 years to 50 years[1,2]

Migration Time: Experience indicates 10 to 15 years

Shelf Time: For encryption it can be decades. For authentication using digital signatures it can be minimal to years

How Might This Impact Registry Operations

Adoption of post-quantum cryptographic algorithms will take years and require algorithm selection, transition planning, new and evolved standards, updated crypto libraries, protocol and architecture updates, system upgrades, ecosystem collaboration and more.

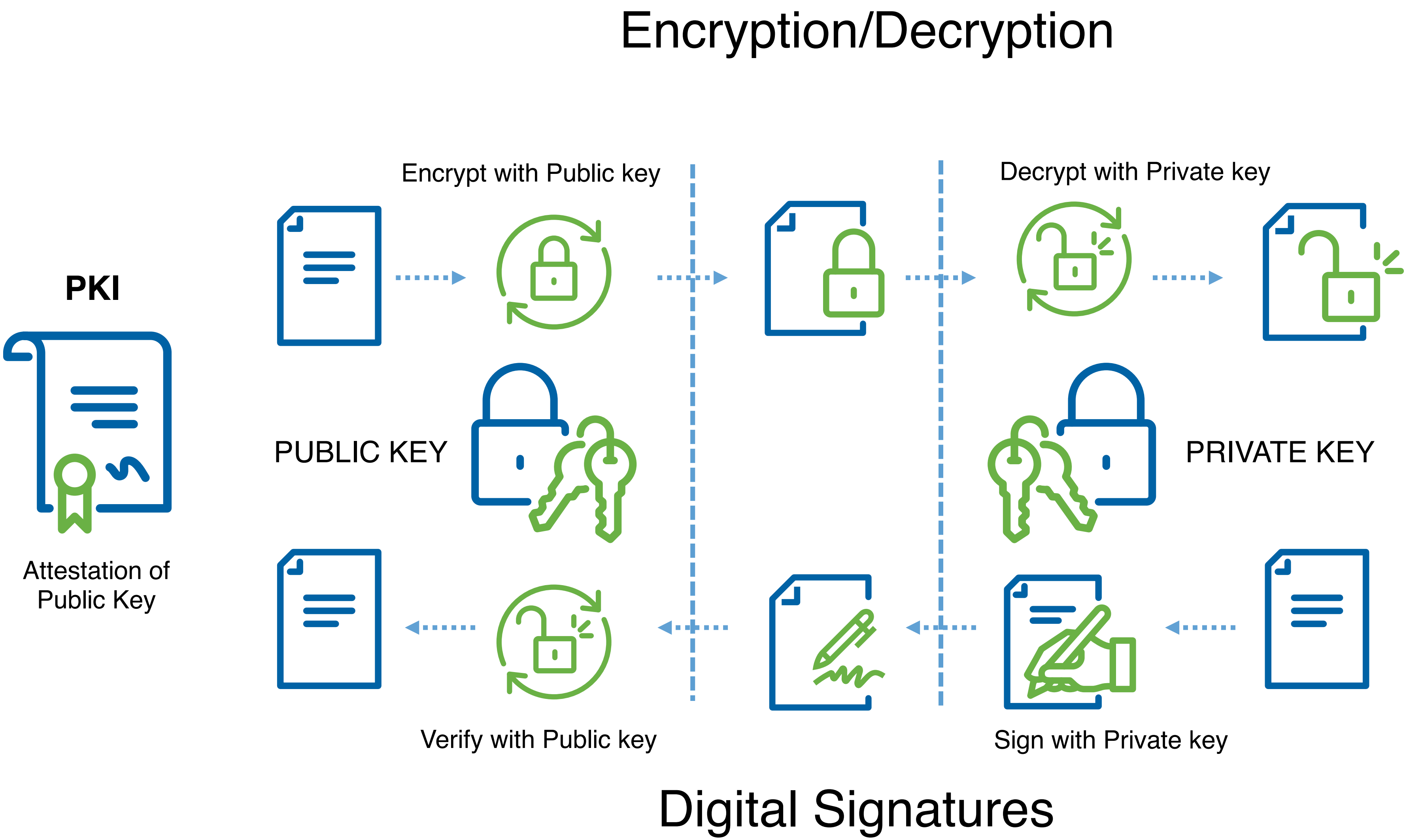
Secure Communications Protocols

- EPP: TLS transport for Secure Interaction
- Registration Data Escrow: SFTP/SCP for Encrypted File Transfer
- RDAP: TLS for Encrypted Sessions
- Other Web Access: TLS for Encrypted Sessions

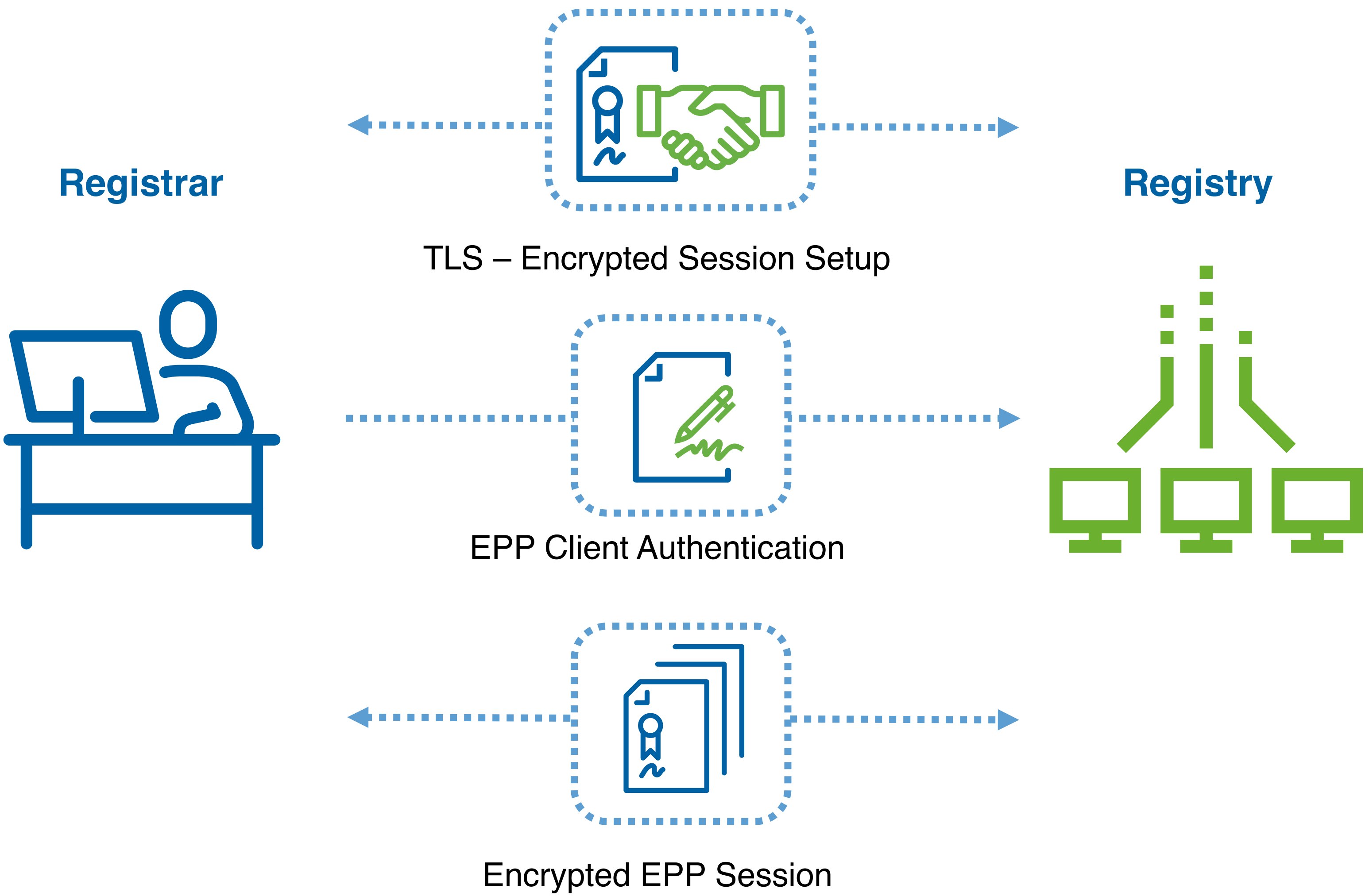
Registry/Registration Services Using Digital Signatures

- EPP: Registrar Identity Authentication using Client Certificates
- DNSSEC: DNS Response Authentication via Digital Signatures
- RDAP (Optional): OpenID Connect for Client Authentication and Authorization

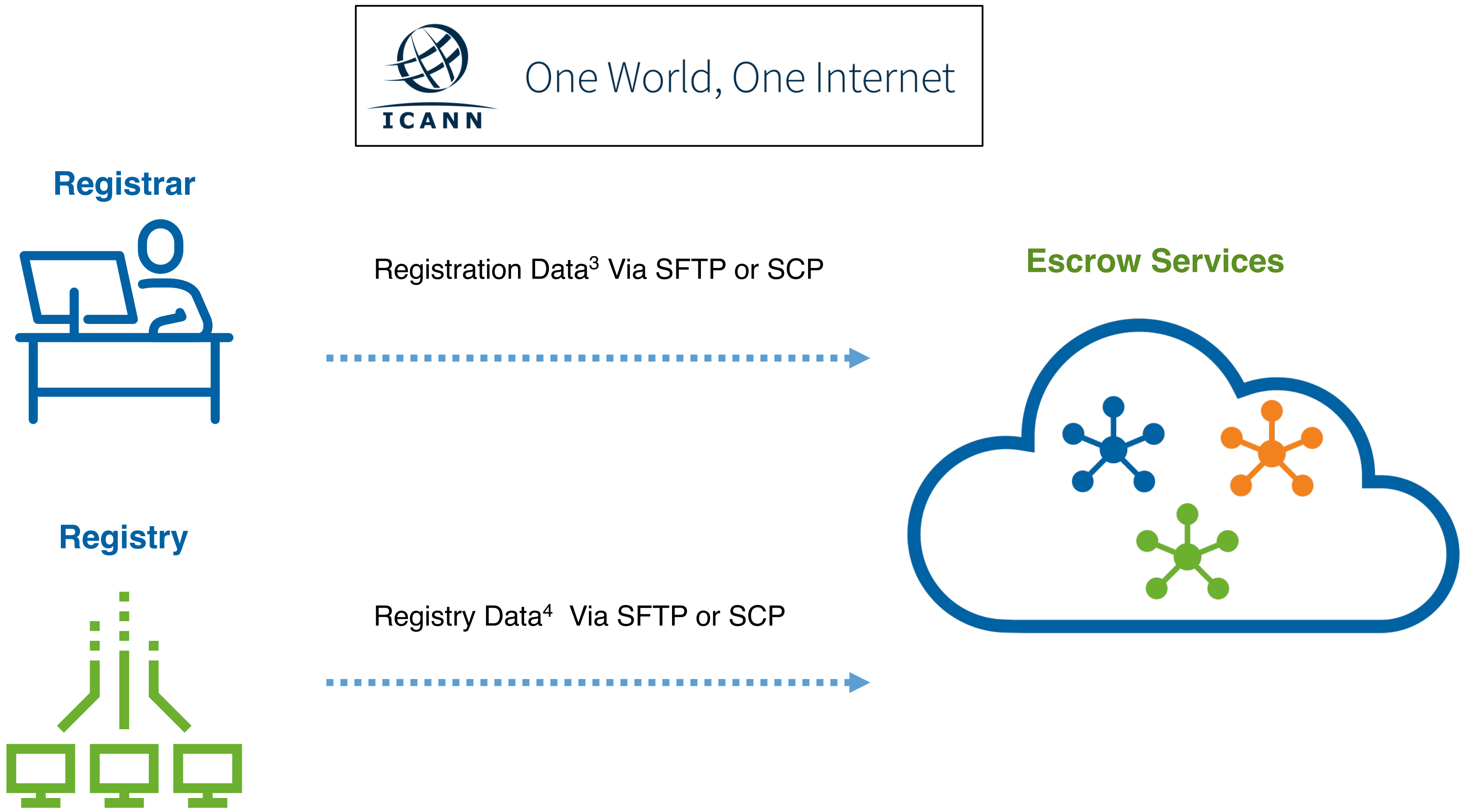
Overview of Public Key Ciphers



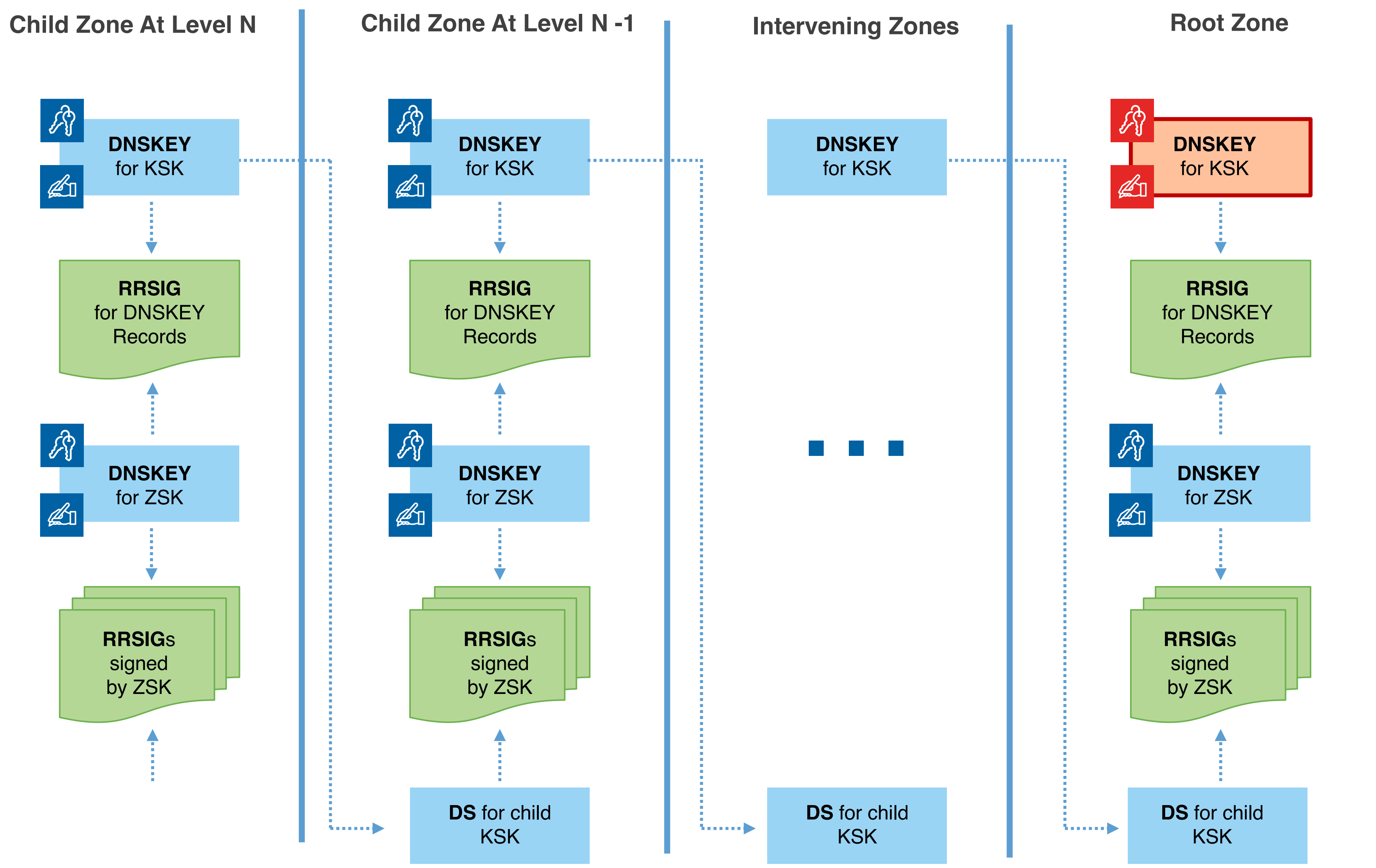
EPP Use of Public Key Cryptography



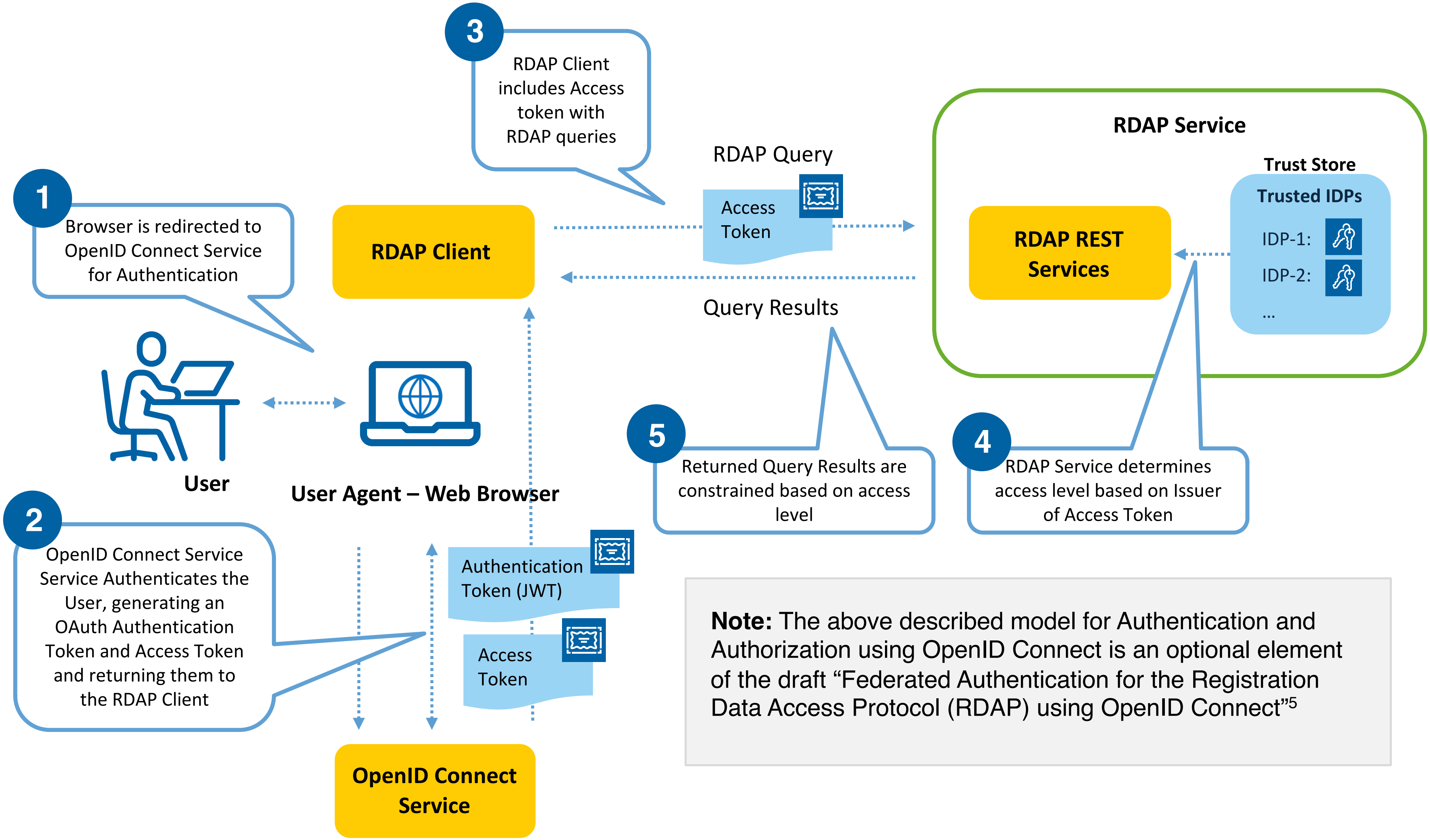
Registration Data and Registry Escrow



Keys and Signatures in DNSSEC Trust Chain



RDAP – Optional Authentication and Authorization



Note: The above described model for Authentication and Authorization using OpenID Connect is an optional element of the draft “Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect”[5]

Post Quantum Algorithms are Coming

Standardization Activities

- NIST initiated selection process for post quantum KEM and digital signature algorithms in 2016
- As of May, 2022, announcement of selected algorithms is expected soon
- Additional algorithms from ”alternates” may be selected in a Round 4 expected to last approximately 18 months
- IETF Standards are expected in this decade to follow NIST standardization in 2023 - 2025

NIST PQC Milestones and Timelines

NIST

2016
Determined criteria and requirements, published NISTIR 8105
Announced call for proposals

2017
Received 82 submissions
Announced 69 1st round candidates

2018
Held the 1st NIST PQC standardization Conference

2019
Announced 26 2nd round candidates, NISTIR 8240
Held the 2nd NIST PQC Standardization Conference

2020
Announced 3rd round 7 finalists and 8 alternate candidates. NISTIR 8309

2021
Hold the 3rd NIST PQC Standardization Conference

2022 Make 3rd round selection and draft standards

2023 Release draft standards and call for public comments

Slide Extracted from Dustin Moody Presentation at PKC 2022[6]

NIST Signature Selection Follow-On

NIST Desire for Another General Purpose Signature Algorithm

- NIST will also solicit proposals for a general purpose digital signature algorithm to provide greater variety for “plug-and-play” algorithms
- Currently only a lattice-based algorithm and SPHINCS+ are expected to be standardized
- SPHINCS+ key and signature sizes are not attractive for some use cases
- NIST therefore desires an alternative to the more general purpose lattice-based algorithm to provide algorithm diversity and resilience in case of algorithm compromise

An on-ramp for signatures

NIST

- After the conclusion of the 3rd Round, NIST will issue a new Call for Signatures
  - There will be a deadline for submission, likely Jan 2023
  - This will be much smaller in scope than main NIST PQC effort
  - The main reason for this call is to diversify our signature portfolio
  - These signatures will be on a different track than the candidates in the 4th round
- We are **most interested** in a general-purpose digital signature scheme which is not based on structured lattices
  - We may be interested in other signature schemes targeted for certain applications. For example, a scheme with very short signatures.
- The more mature the scheme, the better.
- NIST will decide which (if any) of the received schemes to focus attention on

Slide Extracted from Dustin Moody Presentation at PKC 2022[6]

NIST PQC Signature Candidates for DNSSEC

Raw Public Key and Signature Sizes – DNSKEY and RRSIG RRs are larger

Algorithm	Public Key	Signature	Notes
RSA-2048	256 bytes	256 bytes	Currently algorithm - widely used
ECDSA 256	32 bytes	64 bytes	Current algorithm. Elliptic curve
Ed25519	32 bytes	64 bytes	Current algorithm. Elliptic curve
Falcon	897 bytes	666 bytes	NIST Round 3 candidate. Lattice-based
Dilithium	1312 bytes	2240 bytes	NIST Round 3 candidate. Lattice-based. NIST Level II
SPHINCS+	32 bytes	7856 bytes	NIST Round 3 alternate. Stateless HBS

NIST's candidate algorithms have larger resource requirements that challenge DNSSEC

- Larger public keys
- Larger signatures
- CPU and memory requirements

Even with EDNS(0)[7,8], UDP may be an unreliable transport for the large keys and signatures of PQC algorithms

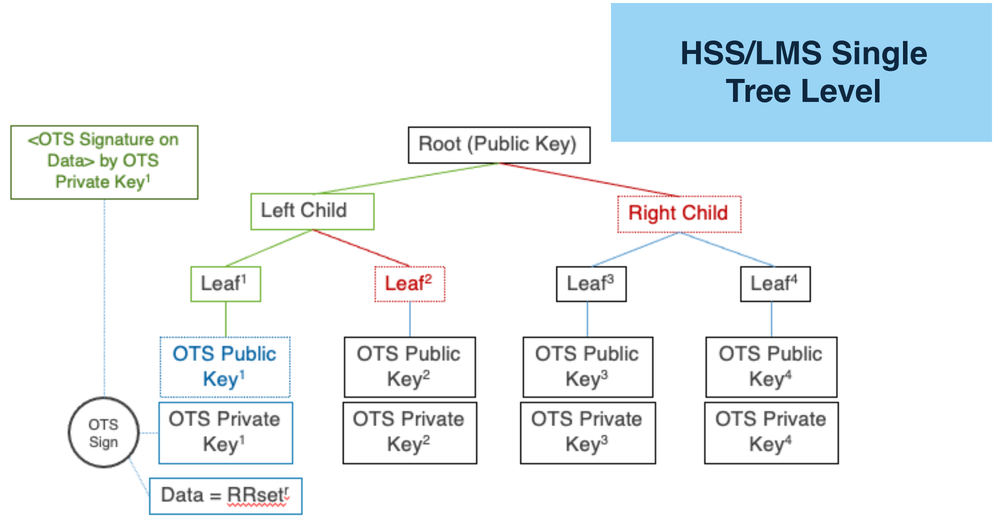
Even Falcon would present issues when multiple DNSKEYs or RRSIGs are returned in a UDP response

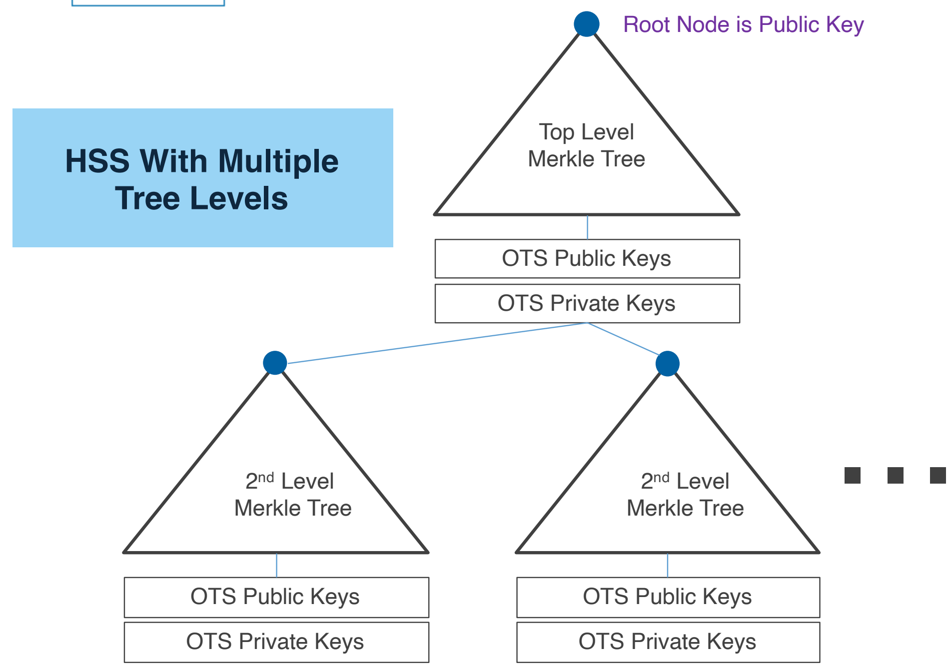
Verisign Public

powered by VERISIGN

Hash-Based Signature Schemes as an Option for PQC Transition and Resilience

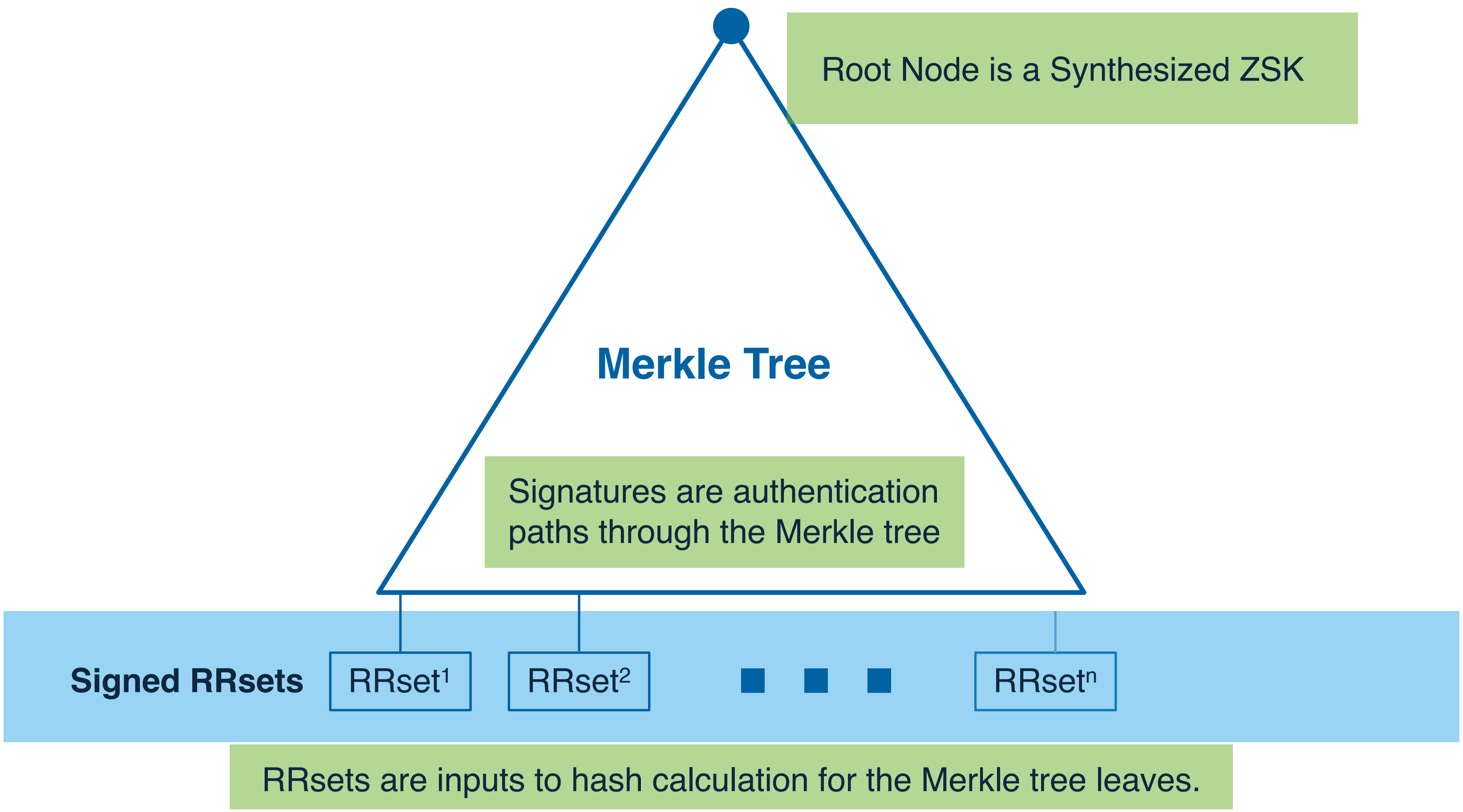
- Hash-Based Signature Schemes can provide a safe option for algorithm diversity and resilience
- Hash algorithms such as the widely used SHA256 are NIST approved PQC algorithms[9,10] that already have broad adoption.
- Draft “Stateful Hash-Based Signature Schemes for DNSSEC”[11] covers two NIST approved algorithms[12]: HSS/LMS[13] and XMSS/XMSS^{MT} [14]
    - Public Key field of DNSKEY RRs is ~60 bytes
    - Signature size varies:
        - HSS/LMS: ~1100 bytes for 1M OTS signature capability, ~3500 bytes for 1T OTS signature capability
        - XMSS^{mt}: has larger signatures
- Synthesized public keys based on Merkle Trees as proposed by Burt Kaliski[15]
    - Public Key size will be ~60 bytes
    - Signature size is reduced to being on the order of $\log_2$(Number of RRsets Signed) * 32
    - Signatures for a zone with 1M RRsets would have a signatures size of ~20 * 32 = 640 bytes





Synthesized Zone Signing Keys Using Merkle Trees[15]

Synthesized Zone Signing Keys[15] are an alternative hash-based signature scheme for DNSSEC with shorter signatures than other HBSS



Potential Activities for Transition to a Post-Quantum DNSSEC

- R&D: Algorithm characteristics; network and computing resource impact; test beds; operational experience; ecosystem readiness
- Planning: Collaborative activities; standards; transition
- Standards: IETF drafts for PQC algorithms for DNSSEC; operational guidance; NIST PQC evaluation
- Collaboration: PQC impact on DNSSEC operations; Resolver/Nameserver/Crypto Library support for PQC algorithms; legacy systems impact; DNSSEC over-the-wire analysis; test beds

Appendix: Standards and References

Some Internet Infrastructure Standards Specifying Public Key Cryptography

- The current most recommended or required algorithms are RSA 2048 and Elliptic Curve - ECDSA with curves P256 and P2545 and Edwards with curveE25519
- Some IETF RFCs that require or recommend quantum susceptible public key algorithms
  - **RFC 4033 - DNS Security Introduction and Requirements**
  - **RFC 4523 - The Secure Shell (SSH) Transport Layer Protocol**
  - **RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**
  - **RFC 5734 – Extensible Provisioning Protocol (EPP) Transport over TCP**
  - **RFC 6698 - The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol**
  - **RFC 6781 - DNSSEC Operational Practices, Version 2. IETF**
  - **RFC 7481 – Security Services for the Registration Data Access Protocol (RDAP)**
  - **RFC 7525 – Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)**
  - **RFC 8162 - Using Secure DNS to Associate Certificates with Domain Names for S/MIME**
  - **RFC 8247 – Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)**
  - **RFC 8301 - Cryptographic Algorithm and Key Usage Update to DomainKeys Identified Mail (DKIM)**
  - **RFC 8310 - Usage Profiles for DNS over TLS and DNS over DTLS**
  - **RFC 8332 - Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol**
  - **RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3**
  - **RFC 8624 – Algorithm Implementation Requirements and Usage Guidance for DNSSEC**

References

1 - M. Mosca, M. Piani, "Quantum Threat Timeline Report 2020", 2020, https://globalriskinstitute.org/download/quantum-threat-timeline-report-2020/

2 - H. Orman, “Internet Security and Quantum Computing”, December 2021, https://eprint.iacr.org/2021/1637.pdf

3 - ICANN, “Registrar Data Escrow Specifications”, November 2007, https://www.icann.org/en/system/files/files/rde-specs-09nov07-en.pdf

4 - G. Lozano, ICANN, “Registry Data Escrow Specification”, November 2020, https://datatracker.ietf.org/doc/html/rfc8909

5 - S. Hollenbeck, “Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect“, Work in Progress, Internet-Draft, draft-ietf-regext-rdap-openid-12, March 2022, https://datatracker.ietf.org/doc/html/draft-ietf-regext-rdap-openid

6 - D. Moody, "The Beginning of the End: The First NIST PQC Standards", PKC 2022, March 8-11, 2022, March 8, 2022, https://csrc.nist.gov/csrc/media/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa/images-media/pkc2022-march2022-moody.pdf

7 - O. Surý, "DNS Flag Day 2020", September 2020, https://www.isc.org/blogs/dns-flag-day-2020-2.Work in Progress, Internet-Draft, draft-ietf-dnsop-avoid-fragmentation-05, June 2021, https://datatracker.ietf.org/doc/draft-ietf-dnsop-avoid-fragmentation/

8 - K. Fujiwara, P. Vixie, "Fragmentation Avoidance in DNS", Work in Progress, Internet-Draft, draft-ietf-dnsop-avoid-fragmentation-05, June 2021, https://datatracker.ietf.org/doc/draft-ietf-dnsop-avoid-fragmentation/

9 - National Institute of Standards and Technology (NIST), "SP 800-57 Recommendation for Key Management: Part 1 – General", October 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf

10 - National Institute of Standards and Technology (NIST), "SP 800-131A Transitioning the Use of Cryptographic Algorithms and Key Lengths”, March, 2019, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

11 - A. Fregly, R. van Rijswijk-Deij, “Stateful Hash-Based Signatures for DNSSEC”, March 2022, https://www.ietf.org/archive/id/draft-afrvrd-dnsop-stateful-hbs-for-dnssec-00.txt

12 - National Institute of Standards and Technology (NIST), "SP 800-208 Recommendation for Stateful Hash-Based Signature Schemes", October 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf

13 - D. McGrew, M. Curcio, S. Fluhrer, "Leighton-Micali Hash-Based Signatures", RFC 8554, DOI 10.17487/RFC8554, April 2019, https://www.rfc-editor.org/info/rfc8554

14 - A. Huelsing, D. Butin, S. Gazdag, J. Rijneveld, J., A. Mohaisen, "XMSS: eXtended Merkle Signature Scheme", RFC 8391, DOI 10.17487/RFC8391, May 2018, https://www.rfc-editor.org/info/rfc8391

15 - B. Kaliski, "Securing the DNS in a Post-Quantum World: Hash-Based Signatures and Synthesized Zone Signing Keys”, January 2021, https://blog.verisign.com/security/securing-the-dns-in-a-post-quantum-world-hash-based-signatures-and-synthesized-zone-signing-keys/

powered by

VERISIGN®

© 2022 VeriSign, Inc. All rights reserved. VERISIGN and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.