Cryptographic Agility and RFC 7696

August 12, 2026

William Favre Slater, III

Slater Technologies, Inc.

Chicago, Illinois, USA

Table of Contents

Table of Contents 2
Dedication 3
Executive Summary 4
Change History 5
Introduction 6
1. What RFC 7696 is about 7
2. The major principles of RFC 7696 7
3. One of RFC 7696's most important ideas 8
4. RFC 7696 anticipated the PQC problem 9
5. What changed between 2015 and 2026? 10
6. NIST has effectively validated the RFC's basic thesis 11
7. RFC 7696 versus 2026 Enterprise Crypto Agility 12
8. A particularly important evolution: from algorithm negotiation to cryptographic policy 13
10. One aspect is even more important in 2026: measuring migration 16
11. What I would retain unchanged from RFC 7696 18
12. What I would add for a 2026 program 18
Conclusion 19
Author 21
References: 22

Dedication

This brief Cryptographic Agility paper is dedicated with the greatest respect and admiration to my esteemed friend and colleague, Ms. Louise Davey, an extremely busy French-Canadian Technology and Business Leadership Evangelist and Author (Quantum How, 2025), who has generously taught me and countless others an enormous amount about speaking technology with grace and clarity to corporate leaders and Boards of Directors. Louise, you make our chaotic world make sense. I shudder to think of a world without YOU!

Merci beaucoup, Mademoiselle Davey.

Executive Summary

It's 2026, and many organizations have awoken to the fact that Post Quantum Cryptography (PQC) Migration Projects are now an crucial part of their future and must be accounted for in current and future budgets. But experts have also introduced the concept of " Cryptographic Agility ", and stressed that this is essential for an organization's first PQC Migration Project. This brief paper explains the concepts and importance of Cryptographic Agility, as well as the relevance of RFC 7696 from 2015, to PQC Migration planning in 2026. This paper will also help explain and justify the importance and inclusion of Cryptographic Agility efforts to the organization's decision makers and to the Board of Directors.

Change History

Change Number	*Change Date*	*Change*	*Reason*
0	2026 0812	Initial Version	Initial Version

Introduction

What is Cryptographic Agility (also known as " Crypto Agility ")? This is a quick summary of Crypto Agility:

Credit: National Institute of Standards and Technology, U.S. Department of Commerce

Question: Please summarize RFC 7696 and discuss if the principles and procedures written in 2015 on Cryptographic Agility remain valid for Crypto Agility efforts in 2026.

Yes. **RFC 7696 remains highly relevant in 2026**, and in several respects the post-quantum transition has made its central design principles more important than they were when Russ Housley published it in November 2015. However, RFC 7696 should now be treated as a **foundational protocol-design document**, not as a complete enterprise Crypto Agility framework. NIST's 2025–2026 work on Crypto Agility substantially extends the RFC's ideas into software, hardware, firmware, infrastructure, governance, inventory, policy, testing, and operational migration. (NIST Computer Security Resource Center).

1. What RFC 7696 is about

RFC 7696 — Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms was published by the IETF in November 2015 as **BCP 201 — Best Current Practice**.

Its central problem is straightforward:

Cryptographic algorithms do not last forever.

Protocols therefore should not be designed around the assumption that RSA, ECC, AES, SHA-2—or any other particular algorithm—will remain appropriate indefinitely.

RFC 7696 defines algorithm agility as the ability of a protocol to migrate relatively easily from one cryptographic algorithm or suite to another. It emphasizes modular implementations, explicit algorithm identification, mechanisms for determining deployment of new algorithms, and operational action to disable obsolete ones. (RFC Editor)

That is remarkably close to what we now call **Crypto Agility**.

---

2. The major principles of RFC 7696

The RFC's recommendations can be reduced to several architectural principles.

RFC 7696 principle	Meaning	2026 status
Support algorithm identifiers	Don't hard-code one cryptographic algorithm into the protocol	**Essential**
Modular cryptographic implementation	New algorithms should be insertable without redesigning the entire system	**Essential**
Mandatory-to-implement algorithms	Maintain a baseline for interoperability	**Still valid**
Allow MTI algorithms to change	The required algorithm set must evolve	**Critical**
Separate protocol specification from algorithm specification	Allows algorithms to change without redesigning the protocol	**Highly relevant**
Negotiate algorithms securely	Peers need a mechanism for selecting compatible algorithms	**Essential**
Protect negotiation against downgrade attacks	An attacker must not force selection of weaker cryptography	**Critical**

RFC 7696 principle	Meaning	2026 status
Deprecate weak algorithms	Old algorithms must eventually disappear	**Critical**
Measure deployment	Determine whether new algorithms have actually propagated	**More important than ever**
Balance cryptographic strength	Components of a suite should provide comparable security	**Still valid**
Limit excessive choices	Too many algorithms increase complexity and attack surface	**Still valid**
Plan transitions before failure	Don't wait until an algorithm is broken	**Fundamental PQC principle**

The RFC explicitly warns that algorithm identifiers alone do not create agility. People must deploy new implementations, change configurations, and actually disable obsolete algorithms. It notes that legacy systems and interoperability concerns often cause weak cryptography to survive long after experts recommend replacing it. (RFC Editor)

That observation could almost have been written specifically about the PQC migration problem.

---

3. One of RFC 7696's most important ideas

One sentence captures the entire concept:

Design the system assuming that the cryptographic algorithm will eventually have to change.

RFC 7696 warns against choosing what it calls effectively a **"one true cipher suite."** A protocol tightly coupled to one algorithm may initially look simpler, but when that algorithm becomes obsolete, the protocol itself may have to be revised, reimplemented, and redeployed. (RFC Editor)

In 2026, this is no longer theoretical.

Consider the transition:

RSA/ECC → PQC

Instead of:

the modern design objective is closer to:

The application should ideally request a security capability rather than directly depend on a particular algorithm.

---

4. RFC 7696 anticipated the PQC problem

The RFC contains several observations that are particularly prescient in 2026.

Algorithms must be replaceable

RFC 7696 says implementations should be modular enough to accommodate new algorithms or suites and should ideally provide a way to measure migration from old algorithms to new ones. (RFC Editor)

That translates directly into today's:

Crypto Discovery → CBOM → Policy → Migration → Telemetry → Deprecation

Transition before an algorithm becomes unusable

The RFC recommends transitioning mandatory algorithms **before they weaken to the breaking point**. (RFC Editor)

That principle is particularly important for PQC because organizations cannot reasonably wait for a cryptographically relevant quantum computer to appear before beginning migration.

Algorithm negotiation must resist downgrade attacks

RFC 7696 explicitly states that cryptographic algorithm selection or negotiation should be integrity protected because otherwise the migration mechanism itself can create downgrade vulnerabilities. (RFC Editor)

That remains a major design consideration for:

TLS
IPsec/IKE
SSH
QUIC
VPNs
PKI
service meshes
API gateways
hybrid PQC protocols.

Too many algorithms are dangerous

Agility does **not** mean supporting every possible algorithm.

RFC 7696 warns that excessive choices create interoperability problems, configuration complexity, rarely exercised code paths, and additional opportunities for implementation vulnerabilities. (RFC Editor)

This distinction is extremely important:

Crypto Agility ≠ cryptographic proliferation.

A well-designed agile architecture should actually make it easier to maintain a **small, governed, approved portfolio** of algorithms.

---

5. What changed between 2015 and 2026?

This is where RFC 7696 becomes insufficient by itself.

RFC 7696 is primarily concerned with **IETF protocols and algorithm negotiation**.

Modern enterprise Crypto Agility is much broader.

NIST now defines Crypto Agility as capabilities needed to replace and adapt cryptographic algorithms across:

protocols, applications, software, hardware, firmware, and infrastructures while preserving security and ongoing operations. (NIST Computer Security Resource Center)

That is a major expansion.

The evolution can be viewed as:

6. NIST has effectively validated the RFC's basic thesis

This is perhaps the strongest evidence that RFC 7696 remains relevant.

NIST established a dedicated Crypto Agility effort in 2025 and published **CSWP 39, Considerations for Achieving Crypto Agility: Strategies and Practices**, with the current version reflecting updates through June 2026. (NIST Computer Security Resource Center)

NIST Crypto Agility Project

NIST CSWP 39 — Considerations for Achieving Crypto Agility

NIST's modern definition essentially extends RFC 7696's philosophy beyond protocols.

RFC 7696 asks:

Can the protocol change algorithms?

NIST's 2026 Crypto Agility approach asks:

Can the entire organization change cryptography without disrupting business operations?

That is a much larger engineering problem.

---

7. RFC 7696 versus 2026 Enterprise Crypto Agility

I would characterize the difference this way:

Dimension	RFC 7696	2026 Crypto Agility
Primary scope	Protocols	Enterprise
Algorithm replacement	Yes	Yes
Algorithm negotiation	Major focus	One component
Interoperability	Major focus	Major focus
Downgrade protection	Yes	Yes
Cryptographic inventory	Limited	**Essential**
CBOM	No	**Important**
Automated discovery	No	**Important**
PKI migration	Discussed indirectly	**Major workstream**
HSM/KMS migration	Limited	**Major workstream**
Hybrid cryptography	Transition concept present	**Core PQC strategy**
PQC	Predates PQC standards	**Central driver**
Policy orchestration	Limited	**Essential**
Continuous testing	Limited	**Essential**
Telemetry	Deployment measurement anticipated	**Essential**

Dimension	RFC 7696	2026 Crypto Agility
Governance	Limited	**Enterprise requirement**
Vendor/supply-chain management	Limited	**Critical**
Crypto abstraction	Conceptually supported	**Architectural objective**

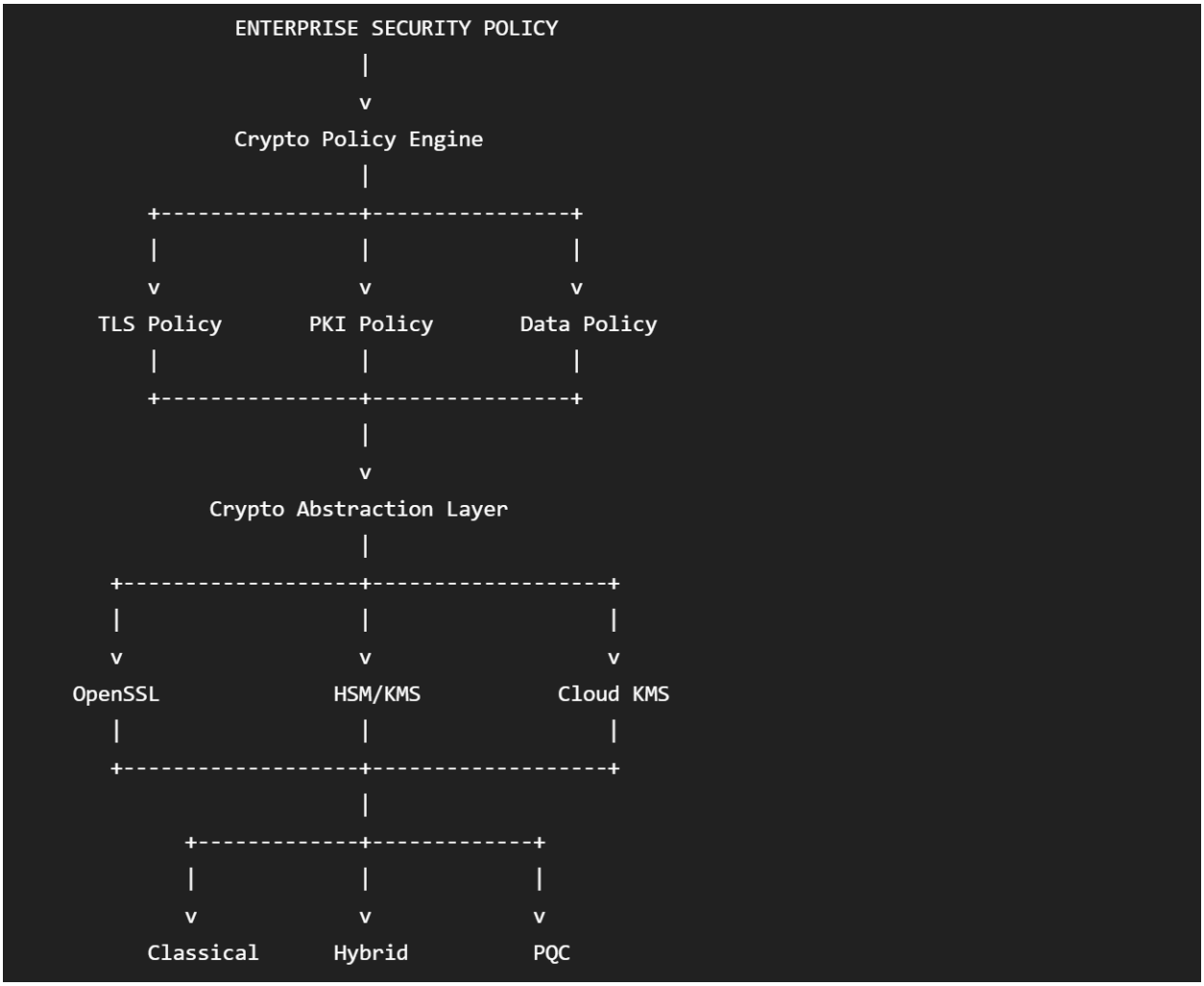
So RFC 7696 is **necessary conceptual groundwork, but not sufficient implementation guidance for an enterprise PQC program**.

---

8. A particularly important evolution: from algorithm negotiation to cryptographic policy

RFC 7696 assumes systems largely negotiate among algorithms they support.

The more sophisticated 2026 architecture is:



The algorithm is increasingly something **policy selects**, rather than something application developers permanently embed.

That is the architectural leap from **algorithm agility** to **enterprise Crypto Agility**.

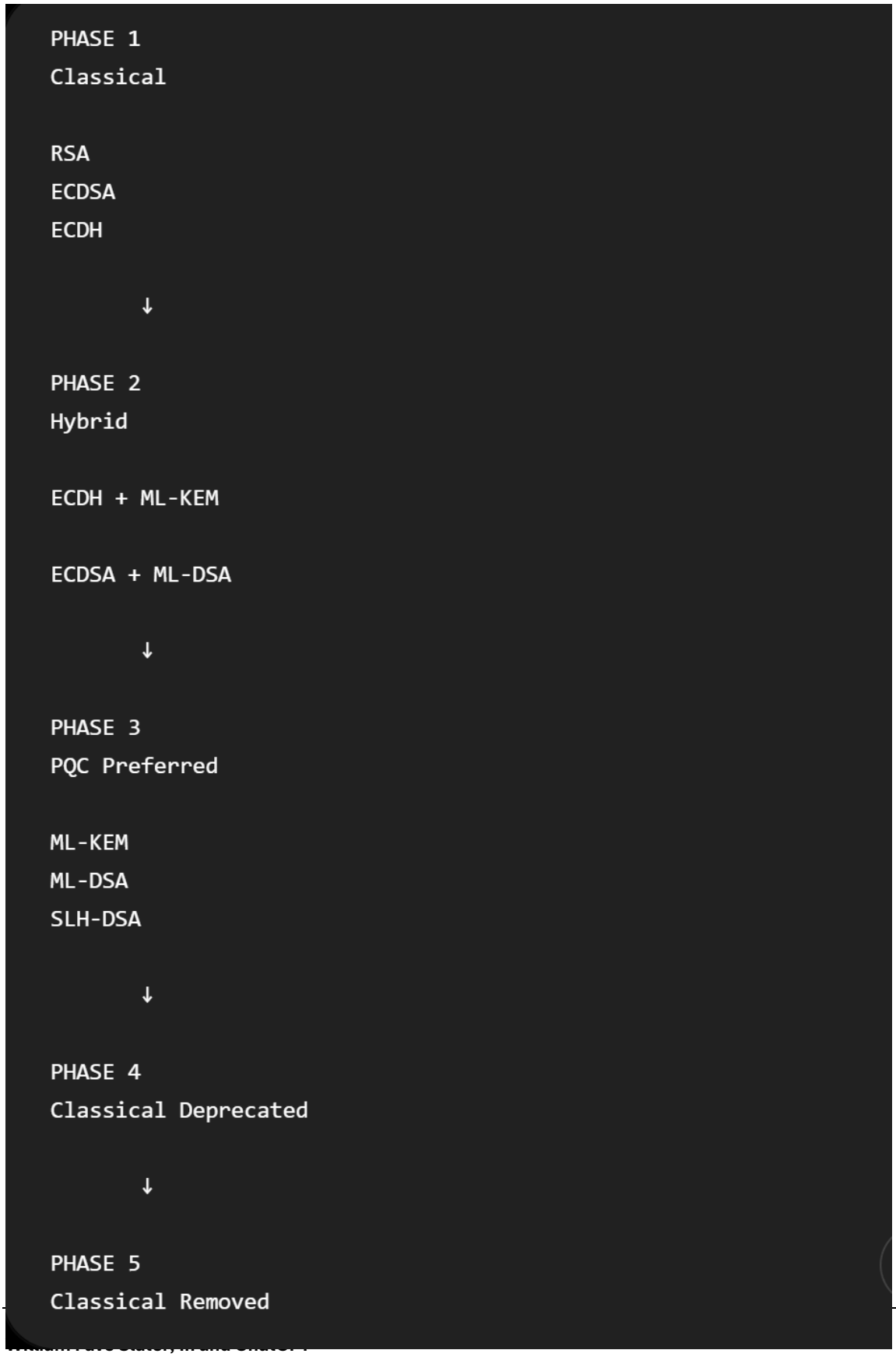
Recent research also identifies application coupling to algorithms and providers as a continuing obstacle to PQC migration, reinforcing the importance of abstraction and policy-driven selection. (arXiv).

---

9. RFC 7696's transition model maps remarkably well onto PQC

The RFC describes introducing a second signature algorithm and subsequently phasing out the original one. (RFC Editor)

That maps almost perfectly onto today's hybrid migration concept:



William Fave Slater, II and Slater
Slater Technologies, Inc.
Chicago, Illinois, USA
August 12, 2026

10. One aspect is even more important in 2026: measuring migration

RFC 7696 says implementations should ideally provide a way to measure whether deployed systems have shifted away from old algorithms. (RFC Editor)

In an enterprise environment, that concept should become **Cryptographic Observability**.

A modern Crypto Agility platform should be able to answer questions such as:

How many RSA certificates remain?

Where is RSA-2048 used?

Which systems still use ECDH?

Which applications support ML-KEM?

Which TLS endpoints support hybrid key establishment?

Which HSMs support PQC?

Which vendors have PQC roadmaps?

Which certificates expire after the migration deadline?

Which applications contain hard-coded crypto?

Which systems cannot be upgraded?

What percentage of the enterprise is PQC-ready?

This is where CBOM becomes extremely valuable.

A practical architecture becomes:

That is essentially **RFC 7696 operationalized at enterprise scale**.

11. What I would retain unchanged from RFC 7696

For a 2026 Crypto Agility program, I would preserve almost verbatim the underlying principles:

1. **Assume every cryptographic algorithm will eventually be replaced.**
2. **Do not tightly couple protocols/applications to algorithms.**
3. **Provide explicit algorithm identification and versioning.**
4. **Maintain interoperability during transition.**
5. **Protect negotiation against downgrade attacks.**
6. **Maintain a small approved algorithm portfolio.**
7. **Plan deprecation before algorithms become unsafe.**
8. **Measure migration progress.**
9. **Design implementations modularly.**
10. **Exercise alternate algorithms rather than merely having dormant fallback code.**

The last point is particularly interesting. RFC 7696 warns that fallback algorithms need to be **routinely exercised** to ensure implementation quality. (RFC Editor)

In 2026 terminology, that becomes:

Continuous Crypto Agility Testing.

---

12. What I would add for a 2026 program

RFC 7696 needs an enterprise operational layer around it:

Crypto Discovery → CBOM → Crypto Risk Register → Crypto Policy Engine → Crypto Abstraction → Hybrid Migration → Automated Testing → Telemetry → Governance

The biggest additions should be:

CBOM / Cryptographic Inventory

You cannot migrate cryptography that you cannot locate.

Crypto abstraction

Applications should depend upon cryptographic services/APIs rather than hard-coded algorithms wherever feasible.

Centralized policy

Security architecture—not individual application teams—should govern approved cryptography.

Hybrid migration capability

Organizations need the ability to operate classical and PQC mechanisms simultaneously during transition.

Automated testing

Every algorithm change needs interoperability, performance, regression, protocol, certificate, HSM, and security testing.

Cryptographic observability

The organization needs continuous evidence showing what cryptography is actually deployed.

Supply-chain visibility

Vendor products, SaaS platforms, cloud services, appliances, network equipment and embedded systems need PQC readiness tracked.

Conclusion

Bottom line

I would give RFC 7696 a very strong assessment for 2026:

Conceptual validity: 10/10

Protocol-design relevance: 9/10

PQC migration relevance: 9/10

Enterprise implementation completeness: 5/10

The RFC got the fundamental problem right:

Cryptography must be designed to change.

What has changed since 2015 is primarily the **scale of the problem**.

In 2015, the emphasis was:

"Can this protocol migrate to another algorithm?"

In 2026, the enterprise question is:

"Can we discover, govern, replace, test, deploy, monitor, and if necessary rapidly revoke cryptography across tens of thousands of applications, devices, certificates, protocols, HSMs, cloud services and vendors without disrupting the enterprise?"

That is the modern definition of Crypto Agility, and the PQC transition has transformed RFC 7696's good protocol-engineering practice into an **enterprise cybersecurity requirement**. NIST's current Crypto Agility program explicitly recognizes that migration now spans protocols, applications, software, hardware, firmware and infrastructure while preserving security and operations. (NIST Computer Security Resource Center)

For a large **five-year PQC migration program**, I would therefore place **RFC 7696 / BCP 201 near the foundation of the Crypto Agility Operating Model**, but pair it with NIST CSWP 39 and current PQC standards and migration guidance rather than treating RFC 7696 as the complete architecture. (nist.gov)

Author

William Slater is President and owner of Slater Technologies, Inc. He is also a CISO, vCISO, Program Manager / Project Manager in the areas of Quantum Technologies, Cybersecurity, Cryptography, Artificial Intelligence, Network Security, Data Centers, and everything related to these technologies. He started his professional career in Information Technology and Cybersecurity. He has a B.S. in Engineering Technology, an M.S. in Computer Information Systems, an MBA, and an M.S. in Cybersecurity, as well as 88 professional certifications, including PMP, CISSP, CISA, SSCP, and CDCP. His other writings can be viewed at https://billslater.com/writing/ and at https://billslater.com/quantum. He lives and works in Chicago, Illinois, USA. His contact information is:

.-- .. .-.. .-.. .. .- -- ... .-.. .- - . .-. .--.-. --. -- .- .. .-.. .-.-.- -.-. --- --

.---- -....- ...-- .---- ..--- -....- ...-- ....- ..--- -....- ..--- -.... ..-- - -....

References:

Arun, J. S, et al. (2025). Becoming Quantum Safe. Wiley. Hoboken, NJ.

IETF. (2015). RFC 7696 — Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms was published by the IETF in November 2015 as BCP 201 — Best Current Practice. Retrieved from https://www.rfc-editor.org/info/rfc7696.

Menezes, A. (2026). Cryptography 101. Retrieved from https://cryptography101.ca .

Powell, W. (2026). Quantum Ready, CRC Press. New York, NY.