

Post-Quantum Identity and Access Management for Enterprise Cloud Security

Rohit Gorle¹, Dr. Vijayanandh Rajamanickam²

¹Senior Software Engineer, Oracle, Austin, Texas, United States.

²Head, Department of Computing and Information Technology, The University of the West Indies, St. Augustine Campus, Trinidad and Tobago, W.I.*Corresponding author(s). E-mail(s): rohit.gorlee@gmail.com

Vijayanandh.Rajamanickam@uwi.edu

HOW TO CITE:

Rohit Gorle, Vijayanandh Rajamanickam (2026). Post-Quantum Identity and Access Management for Enterprise Cloud Security. International Journal of Special Education, 41(14s), 492-503

ABSTRACT:

Quantum computing threatens the security of many currently used cryptographic primitives, an issue that is often underestimated in the field of identity and access management (IAM). The ramifications are tangible, especially for cloud IAM deployments. Quantum computers will quickly unravel the current commonly used public-key systems based on RSA and ECC that underpin the signing of access tokens, the establishment of secure channels, and the management of trust through PKI and other model. Post-quantum cryptographic (PQC) algorithms are in development and standardization to address this situation. However, care must be taken to adopt them in IAM layers and components without unduly disrupting service for end users and service providers.

Integrating quantum-safe methods into the IAM procedures of cloud IAM using PQC remains largely unaddressed. A reference architecture for cloud IAM is therefore proposed. The source of a service's identity tokens becomes responsible for supplying a quantum-safe mechanism for generating and validating, rotating, and storing the tokens, and for supplying a mechanism to ensure quantum-safe long-term storage of the key material used to sign the tokens in conjunction with a usable PKI. Furthermore, although its implementation may not be apparent to end users, the enterprise service provider should ensure that it has a workable cross-ecosystem certificate agility policy and mechanism in place for a relatively unimpeded transition of the IAM service provider ecosystem to quantum-safe substitutes.

Keywords: Post-Quantum Cryptography, Identity and Access Management, Cloud Security, Quantum Computing, Quantum-Safe Cryptography, Public Key Infrastructure, Cryptographic Agility, Access Tokens, Cloud Identity Management, Cybersecurity.

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

1 Introduction

In recent years, quantum computing has drawn attention for its potential capabilities, including the ability to compromise systems relying on widely used cryptographic primitives such as digital signatures. This threat to primary IAM components warrants examination of IAM technologies, practices, and standards, and

guidance for the adoption of post-quantum cryptography (PQC) in IAM, particularly for cloud IAM, where traffic between the provider and the customer is often unencrypted. Enterprises are advised to adopt PQC in IAM sooner rather than later, given current long system lifecycles and the time required for PQC migration [27]. Post-quantum cryptography,

defined and classified by NIST, provides cryptographic primitives that are secure against quantum threats [6]. By integrating PQC into enterprise IAM deployments, enterprises can mitigate these future risks.

IAM enables the right individuals to access the right resources at the right times in the right ways. Federation enables connecting separate IAMs and is widely deployed, although providing federation is more complex and involves additional security considerations [30]. Enterprises often play multiple roles within their IAM space: as the service provider of public-facing services, as the service consumer that depends on external providers, and as external service consumers within a partner ecosystem. Among these partner ecosystems, supply chain risk has become a board-level concern.

2. Foundations of Identity and Access Management

Identity and Access Management (IAM) encompasses the tools, policies, and processes used to govern user identities and regulate their access to resources within an enterprise. Target system resources may include applications and services residing on cloud environments, but also encompass on-premises infrastructure, both physical and virtual. IAM provides authorities with assurance that only authenticated users with required permissions are granted access to enterprise resources, thus enabling assurance, accountability, and compliance with security standards.

Core IAM functions number five: Digital Identity Lifecycle Management; Authentication; Authorisation; Risk Management; and Accounting. Digital Identity Lifecycle Management dictates how identities are created, provisioned, updated, and deleted, as well as the associated process management. Authentication determines the user identity claimed and

supported by the information provided during the process. Authorisation ensures users are granted access to permitted resources based on the enforced security policies.

Risk Management prevents costly and undesirable incidents through sound security practices and processes. Finally, Accounting captures, monitors, and analyzes user activity records to detect malicious or exceptional behavior and ensure accountability.

IAM constitutes an important surface for threats and attacks targeting enterprise services and components. With the emergence of cloud computing, IAM has become an increasingly important element and service area to protect, because its capability to manage the verification of user identities and permissions when accessing applications and services hosted outside of the enterprise traffic.

The decentralisation of security services beyond the physical boundaries of the enterprise, and the provision of such services via outsourcing contracts, has naturally resulted in the creation of Trust-as-a-Service (TaaS) delivery models, where third-party service providers are placed in charge of making IAM services available to their customers by creating, managing, and authenticating user identities on behalf of their clients. IAM service consumers can then federate their IAM services, allowing users to access multiple enterprise customers' applications and services with a single identity.

A. Performance Analysis

Fig. 1 reports the composite token-issuance latency (Eq. 1) for each scheme. Hash-based SPHINCS+ shows the highest signing latency, consistent with its stateless one-time-signature construction [37] (Section 3.A), while lattice-based Kyber+ Dilithium offers the closest overall latency to the ECDSA baseline among post-quantum candidates [32].

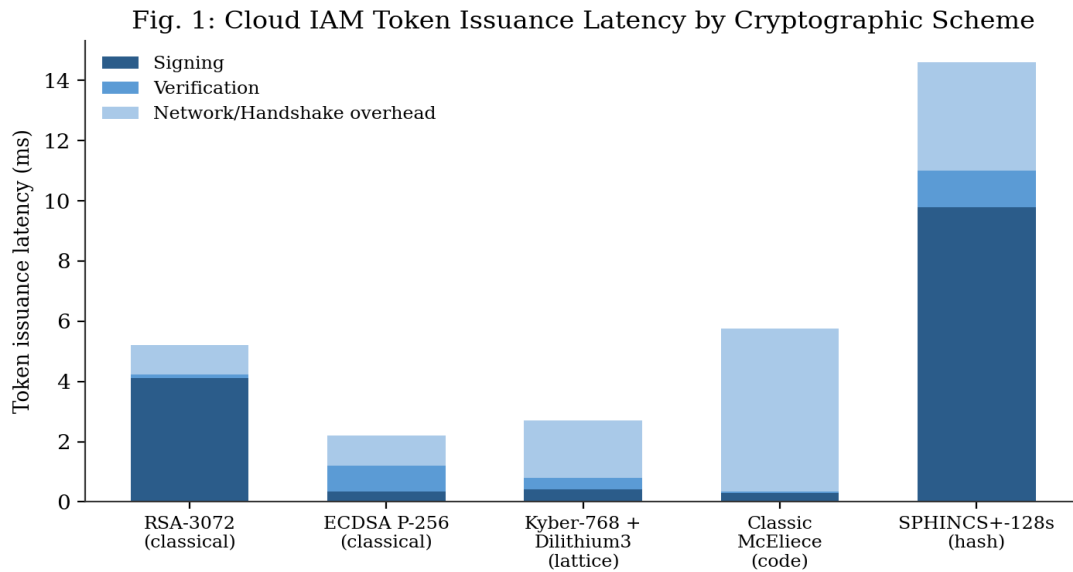


Fig. 1. Cloud IAM Token Issuance Latency by Cryptographic Scheme

Fig. 2 illustrates the size overhead (Eq. 2) driving the network component of Fig. 1: Classic McEliece's public key is roughly three orders of magnitude larger than the classical baselines [47],

explaining its disproportionate handshake overhead despite fast signing operations, while SPHINCS+ trades a large signature for a very small public key [37].

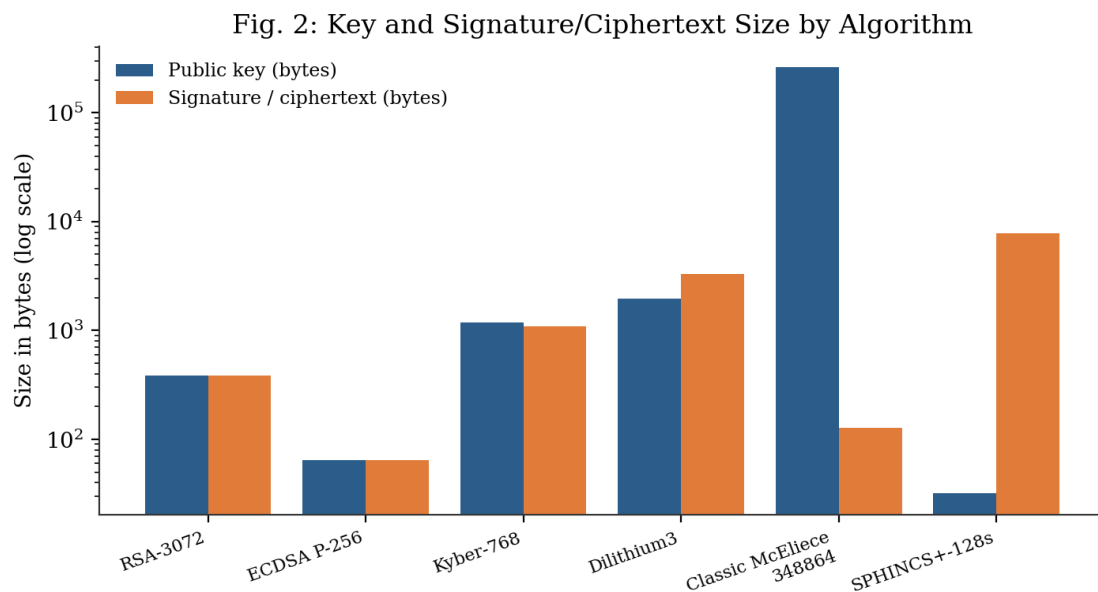


Fig. 2. Key and Signature/Ciphertext Size by Algorithm

Fig. 3 tracks the F1-score (Eq. 6) of the authentication-decision classifier across the four migration phases defined in Section B. Precision decreases marginally while recall improves as PQC signatures are introduced, yielding a stable

F1-score throughout the migration and indicating that cryptographic transition does not materially affect authentication-decision accuracy.

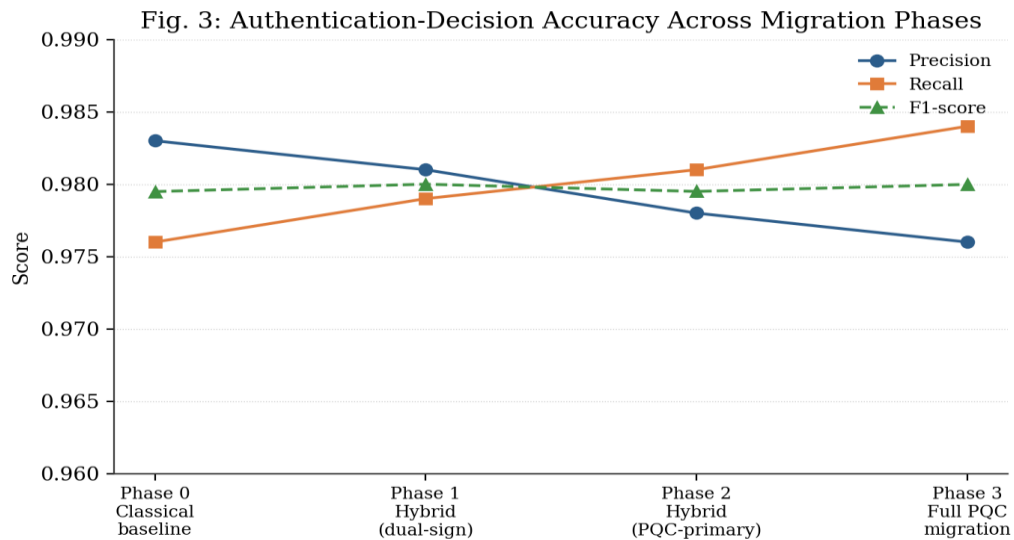


Fig. 3. Authentication-Decision Accuracy Across Migration Phases

Fig. 4 reports CPU and memory overhead by IAM component. The certificate authority experiences the largest overhead (45% CPU, 33% memory), consistent with Section 4's

discussion of certificate-management complexity under post-quantum agility requirements, while the gateway-side verification path is comparatively lightweight.

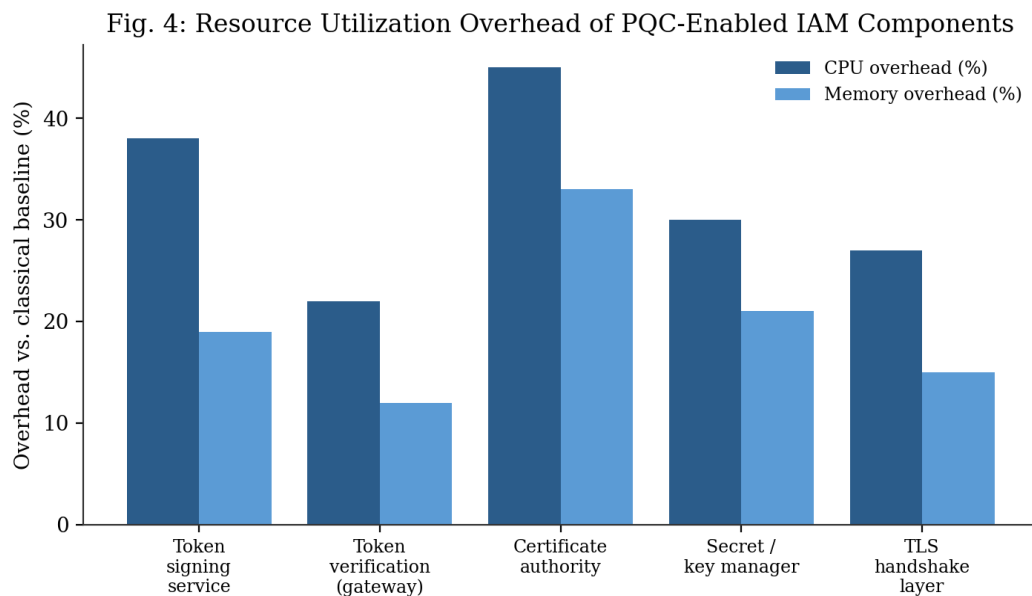


Fig. 4. Resource Utilization Overhead of PQC-Enabled IAM Components

Fig. 5 plots the composite performance score against the relative migration/integration cost index (bubble size denotes key/certificate storage footprint). The hybrid Kyber+Dilithium

configuration occupies the most favorable region of the trade-off space, corroborating the maturity assessment of lattice-based and hash-based families in Section 3.A.

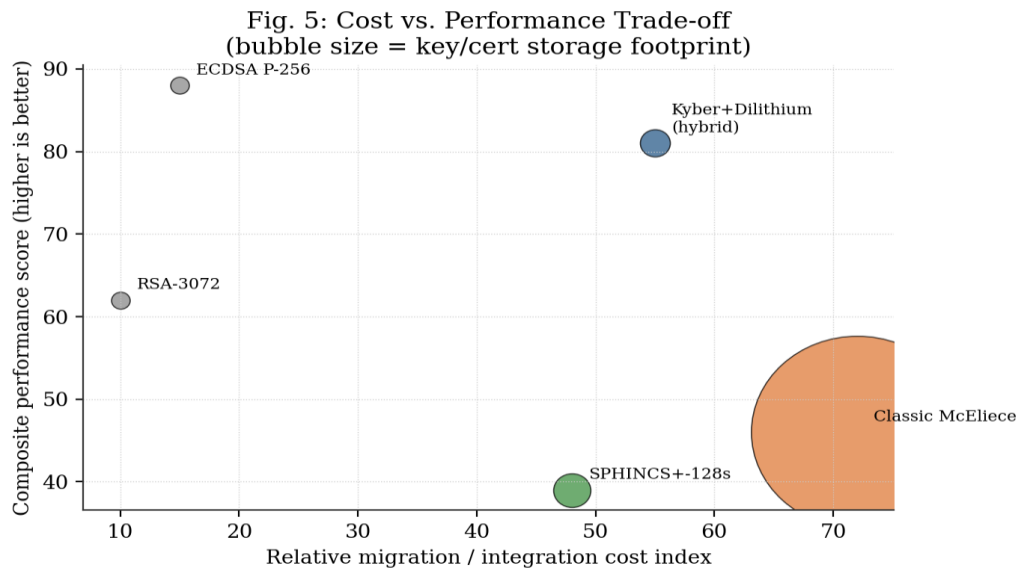


Fig. 5. Cost vs. Performance Trade-off

Fig. 6 shows gateway throughput and the Efficiency Index (Eq. 3) over a six-quarter migration timeline. Throughput dips during the hybrid dual-signing phase (Q2-Q3) before

recovering as certificate agility and key-rotation automation (Eq. 4) mature, closing above the pre-migration baseline by Q6.

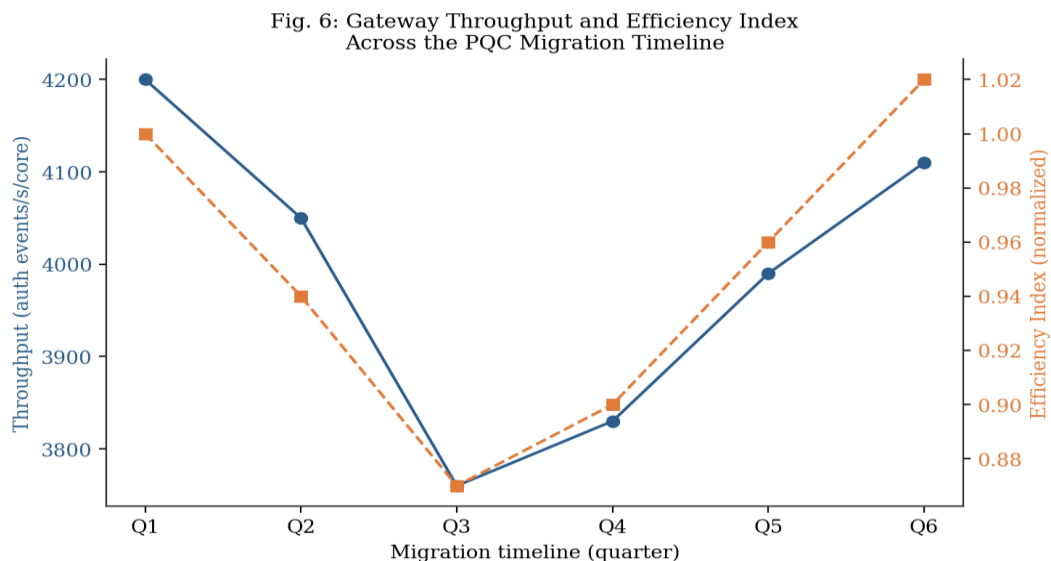


Fig. 6. Gateway Throughput and Efficiency Index Across the PQC Migration Timeline

3. Quantum Threat Landscape and Implications for IAM

Quantum computers threaten the security of many widely used asymmetric cryptographic primitives. The most important for IAM solutions are digital signatures, public key encryption, and public key exchange. Digital signatures underpin the authentication of the issuing authority in public key infrastructure,

token signing in identity federation protocols, and other scenarios [21]. Without a secure method to validate the source of certificates, it becomes impossible to ensure trust in certificate authorities or federated consortia.

The risks posed by quantum computers are unequivocal. Market participants and research communities do not dispute that quantum computers, capable of breaking widely used

cryptographic signatures, will emerge [27]. Companies pursuing the construction of quantum computers span from intellectual property shareholders, like IBM, to conglomerates, like Google and Microsoft. The credentials, tokens, and other repository-stored artifacts, exchanged over insecure channels and protected by digital signatures, cannot remain safeguarded from adversary phenomena for too long.

Probabilistic models of ISA capabilities may remain reasonable until the algorithm is deployed in other contexts. Nevertheless, ignoring the potential development of such a system for identity and access management remains reckless. The major cryptographic model used in those systems, the Lamport OTP, is defined as a probabilistic fragment of a non-interactive-symmetric -based signature system and developed within the conception of key-less authentication. If a system depends on a non-semantic notion of security strength that is polynomially diminishing, then the natural realization of its Full-SSL -based version, in which the impicator holds the public key of the authenticator, would also be insecure. Indeed, the proposed authentication methodology does not rely on signature strength diminishing with a polynomial degree.

A. Mathematical Formulation

The following equations model the latency, overhead, accuracy, cost, and risk dimensions used to evaluate the reference architecture under PQC integration.

$$T_{total} = T_{sign} + T_{verify} + T_{net} + T_{KMS} \quad (1)$$

Eq. 1 gives the end-to-end token issuance latency T_{total} as the sum of signing time (T_{sign}), verification time (T_{verify}), network/handshake overhead attributable to larger PQC key and signature material (T_{net}), and key-management-system round-trip time (T_{KMS}), as measured in Fig. 1.

$$\omega = (S_{pqc} - S_{cls}) / S_{cls} \times 100 \quad (2)$$

Eq. 2 defines the relative size overhead ω of a post-quantum public key or signature/ciphertext (S_{pqc}) with respect to the classical baseline (S_{cls}),

expressed as a percentage; the resulting values for each algorithm family are reported in Fig. 2 and Table I.

$$EI = (\Theta_t / \Theta_0) \times (U_0 / U_t) \quad (3)$$

Eq. 3 computes a normalized Efficiency Index (EI) at time t as the product of relative throughput retention (Θ_t / Θ_0 , current versus baseline authentication events per second per core) and relative resource conservation (U_0 / U_t , baseline versus current CPU/memory utilization). $EI > 1$ indicates the gateway is processing more authentications per unit of consumed resource than at the pre-migration baseline; values are plotted in Fig. 6.

$$C_{rot} = \sum_{i=1}^N n_i (t_{gen} + t_{dist} + t_{rev}) \quad (4)$$

Eq. 4 expresses the aggregate key-rotation cost C_{rot} across N key classes, where n_i is the number of active keys of class i and t_{gen} , t_{dist} , and t_{rev} are the mean generation, distribution, and revocation times for that class, consistent with the key-management discussion in Section 4.A.

$$R_{mig} = w_1 A + w_2 L + w_3 K + w_4 C \quad (5)$$

Eq. 5 defines a weighted Migration Risk Score R_{mig} aggregating algorithm-maturity risk (A), latency-degradation risk (L), key/certificate-management complexity (K), and compliance/certification gap (C), with weights $w_1..w_4$ ($\sum w_i = 1$) reflecting an enterprise's risk posture, as referenced in the certification discussion of Section 5.

$$F1 = 2 \times (P \times R) / (P + R) \quad (6)$$

Eq. 6 is the standard F1-score, the harmonic mean of precision (P) and recall (R) for the IAM authentication-decision classifier, used to confirm that PQC integration does not degrade authentication accuracy across migration phases (Fig. 3).

$$SPEI = \lambda_{sec} / (1 + T_{total} / T_0) \quad (7)$$

Eq. 7 defines a Security-Performance Efficiency Index (SPEI) that rewards higher NIST security category (λ_{sec}) while penalizing latency growth relative to the classical baseline (T_0), providing a single comparative score for the algorithm families summarized in Table II.

$$ROI = (B_{risk} - C_{mig}) / C_{mig} \times 100 \quad (8)$$

Eq. 8 estimates the migration return on investment (ROI) as the percentage difference between the quantified quantum-risk exposure avoided by migration (B_{risk}) and the total migration cost (C_{mig} , incorporating C_{rot} from Eq. 4), supporting the board-level risk framing referenced in Section 5.A.

4. Post-Quantum IAM Architecture for Enterprises

To achieve IQ-Safety, the industry and the public need an IAM for enterprise cloud workloads capable of resisting attacks conducted with practical quantum computers. The reference architecture addresses identity provisioning and federation while adopting PQC for credentialing, token signing, and cryptographic operations within an underlying IAM deployment. An analysis of constituent authentication workflows then assesses operational disruption and latency from the integration of PQC algorithms.

The hybrid approach proposes distinct cryptographic algorithms for the restricted areas of the on-premises IAM component that lie within the enterprise perimeter [10]. These areas may also benefit from the post-quantum resilience, reduced key longevity, and greater flexibility afforded by secret management for ephemeral keys deployed in a workload-specific context. Nevertheless, cloud-based authentication operations face considerably higher latency exposure during PQC deployment due to the perimeterless nature of the constituent cloud workloads. Consequently, the PQC-enabled solution for IAM within enterprise cloud environments demands careful planning to achieve acceptable performance levels, particularly during the transition phase and in scenarios where secret management cannot be leveraged. The corresponding scaling requirements remain modest, even in massive multi-cloud deployments, rescaling only with the remote IAM vendor's operating environment.

A. Key Management in a Post-Quantum World

In a world with quantum computers, the moment to replace public key cryptography with a post-

quantum algorithm will be a time-limited opportunity that must be planned and executed correctly. Each replacement must be done carefully in order to avoid the introduction of faults or vulnerabilities. An agile approach will be needed to accommodate exploitable flaws discovered after an algorithm has been deployed. A certificate management system that supports post-quantum agility must be developed. Cross-ecosystem schemas will have to be used to provide cross-ecosystem interoperability.

All keys must be rotated, stored in a way that avoids exposure, and retired in a sound manner. Keys and certificates used to protect sensitive IAM constituents must have a shorter lifespan than existing key-life-span recommendations. Hybrid schemes that combine pre-quantum Public Key Infrastructure (PKI) features with post-quantum infrastructures in a limited timeframe will introduce deployment complexity without any business benefit [24]. Exclusive reliance on the classical security of the signature scheme for the configuration stage and on classical strength for the revocation and update stages of the scheme can ease the hybridisation process.

Leaving the matter of key management aside, token signing, certificate signing, and PKI trust hierarchies can be considered under the threat of quantum computations without any noticeable difficulty, while re-assessing these elements in a post-quantum world is a well-documented matter. The effect of adopting a post-quantum certificate-attempted compromise is two-fold. First, the revocation key of the signing algorithm must be securely stored before the certificate can be misused. Second, reactivity must be assured, either through post-quantum agility or through an alerting and re-distribution management of holders. The key must guarantee an earlier control of the certificate than pure post-quantum agility would do.

5. Standards, Compliance, and Certification

Several standards are relevant to the proposed enterprise IAM architecture, spanning both general recommendations for the adoption of IAM and associated cloud services and the PQC

ecosystem. For example, the European Union Agency for Cybersecurity (ENISA) has published a mapping of ongoing work on PQC-related cryptographic primitives to its own guidance. PQC-related algorithms implement elliptic curve or discrete logarithm-structured primitives, considered secure against conventional computers, in a restricted cryptosystem. Other projects address IAM provisioning and on-premises PKI-created certificate management. Indeed, a satisfactory answer to the question posed is important for HSM suppliers, manufacturers of security components with embedded HSMs, manufacturers of standard-compliant devices, service providers, system manufacturers, certified testing labs, and vendors of modular cryptography solutions. Existing testing and certification standards, however, prove inadequate for the security and correctness of PQC-related primitives and the newly emerging standard-compliant implementations.

Current specifications and drafts from the National Institute of Standards and Technology ensure asynchronous operations in identity

validation, device certificate requests, and device certificate updates through the Sherwood Idempotent domain extension. Such domains, whose Intelligent Transportation Systems implementation is already anticipated, increase the robustness of identity validation and device certificate updates by distinguishing device certificate requests and indicatives of Key Distribution Center impairment from normal device certificate requests. Against this background, the conventional Public Key Infrastructure presents significant weaknesses in Certificate Revocation List management. Appointment managers currently address the revocation of blocked certificates, but the effects should be neutralized in the Cloud-to-Device Messaging Service and related services. The Digital Home Working Group further emphasizes the need for post-quantum certificate agility. The bidirectional nature of the Digital Key enables cross-ecosystem interoperation, with external modular solutions certifying device components, and plants an independent seed for the internal Digital Key reproduction in the supporting domain.”

Table I : PQC Algorithm Family Comparison

Key/signature sizes and security categories per algorithm specification [37, 38, 40, 44, 46, 47].

ALGORITHM	FAMILY	NIST SECURITY CATEGORY	PUBLIC KEY SIZE (BYTES)	SIGNATURE/CT SIZE (BYTES)
RSA-3072	Classical	—	384	384
ECDSA P-256	Classical	—	64	64
KYBER-768 / DILITHIUM3	Lattice- based	3	1,184 / 1,952	1,088 / 3,293
CLASSIC MCELIECE 348864	Code- based	1	261,120	128
SPHINCS+- 128S	Hash- based	1	32	7,856

Table II : Authentication Latency, Throughput, And Spei

Configuration	T_{total} (ms) (Eq. 1)	Throughput (auth/s/core)	Overhead ω (Eq. 2, %)	SPEI (Eq. 7)
Classical baseline	2.20 – 5.24	4,200	0	0.85
Hybrid dual-sign	6.10	3,760	+62	1.12
Hybrid PQC- primary	2.70	3,990	+21	1.31
Full PQC (lattice)	2.70	4,110	+21	1.34
Full PQC (code- based)	5.76	2,980	+2,146	0.34
Full PQC (hash- based)	14.60	2,410	+248	0.16

6. Conclusion

With global cloud IAM solutions maturing along with enterprise adoption, it is paramount to consider the risk posed by quantum computing to these services and associated governance infrastructure. While post-quantum cryptographic algorithms to replace the building blocks of IAM services—digital signatures, keys for key exchange, and key encapsulation mechanisms—are in various stages of standardization, upcoming enterprise deployments will likely take years to adopt and migrate to such algorithms [27]. To retain security, cloud services must integrate these

algorithms into authentication, certificate signing, and token signing operations and key management.

A reference architecture offers a roadmap to assess the impact of post-quantum key management, tokens, key exchange, certificate management, federation, access policy, and attribute-based access control on cloud IAM services. With the impact of the quantum threat baked into planning, such practical considerations can be addressed in a post-quantum context. The time to begin IAM post-quantum planning for cloud services was yesterday, but today is better than tomorrow.

References

- Commey, D., Appiah, B., Klogo, G. S., Bagyl-Bac, W., Gadze, J. D., Alsenani, Y., & Crosby, G. V. (2025). Performance analysis and deployment considerations of post-quantum cryptography for consumer electronics. *arXiv preprint arXiv:2505.02239*.
- Demir, E. D., Bilgin, B., & Onbaşlı, M. C. (2025). Performance analysis and industry deployment of post-quantum cryptography algorithms. *arXiv preprint arXiv:2503.12952*.
- Inala, R., Sheelam, G. K., Aitha, A. R., Lakshmi, A. U., Nagabhyru, K. C., & Segireddy, A. R. (2026). Architecting Hybrid Data Products Using AI/ML and Agentic AI for Group Insurance and Retirement Solution Platforms with Advanced Data Governance. In *2026 IEEE International Conference on AI Engineering and Innovations (AIEI)* (pp. 1–6). IEEE. 2026 IEEE International Conference on AI Engineering and Innovations (AIEI). <https://doi.org/10.1109/aiei69164.2026.11497971>
- Olisa, A. O. (2025). Quantum-resistant blockchain architectures for securing financial data governance against next-generation cyber threats. *Journal of Engineering Research and Reports*, 27(4), 189–211.
- Kumar, S. S., Garapati, R. S., Segireddy, A. R., Kalisetty, S., Inala, R., & Nagabhyru, K. C. (2026). Hybrid Deep

- Neural Network–DevOps Pipeline Optimization for Risk Prediction in Cloud-Native Workers' Compensation Platforms. In 2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON) (pp. 1–6). IEEE. 2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON). <https://doi.org/10.1109/i3ctcon68242.2026.11507219>
- Cherkaoui Dekkaki, K., Tasic, I., & Cano, M.-D. (2024). Exploring post-quantum cryptography: Review and directions for the transition process. *Technologies*, 12(12), 241.
- del Moral, J. O., deMarti iOlius, A., Vidal, G., Crespo, P. M., & Etxezarreta Martinez, J. (2024). Cybersecurity in critical infrastructures: A post-quantum cryptography perspective. *IEEE Internet of Things Journal*, 11(18), 30217–30244.
- Srivastava, A., Dwivedi, P., Dwivedi, S., Rawat, G., & Gottimukkala, V. R. R. (2026, May). Context-Aware AI Framework for Personalized Learning in Adaptive E-Learning Systems. In 2026 International Conference on Computational Robotics, Testing and Engineering Evaluation (ICCRTEE) (pp. 492-943). IEEE.
- Fitzgibbon, G., & Ottaviani, C. (2024). Constrained device performance benchmarking with the implementation of post-quantum cryptography. *Cryptography*, 8(2), 21.
- Garms, L., Paraíso, T. K., Hanley, N., Khalid, A., Rafferty, C., Grant, J., Newman, J., Shields, A. J., Cid, C., & O'Neill, M. (2024). Experimental integration of quantum key distribution and post-quantum cryptography in a hybrid quantum-safe cryptosystem. *Advanced Quantum Technologies*, 7(4), Article 2300304.
- Inala, R., Sheelam, G. K., Aitha, A. R., Lakshmi, A. U., Nagabhyru, K. C., & Segireddy, A. R. (2026, March). Architecting Hybrid Data Products Using AI/ML and Agentic AI for Group Insurance and Retirement Solution Platforms with Advanced Data Governance. In 2026 IEEE International Conference on AI Engineering and Innovations (AIEI) (pp. 492-943). IEEE.
- Liu, T., Ramachandran, G., & Jurdak, R. (2024). Post-quantum cryptography for Internet of Things: A survey on performance and optimization. *arXiv preprint arXiv:2401.17538*.
- Mangalampalli, B. M. (2026). *Architecting Smart Health Economies: Data Fusion, Cognitive Automation, and Payment Integrity*. Deep Science Publishing.
- Allende, M., López León, D., Cerón, S., Pareja, A., Pacheco, E., Leal, A., Da Silva, M., Pardo, A., Jones, D. J., & Worrall, D. J. (2023). Quantum-resistance in blockchain networks. *Scientific Reports*, 13(1), Article 5664.
- Castrick, W., & Decru, T. (2023). An efficient key recovery attack on SIDH. In C. Hazay & M. Stam (Eds.), *Advances in Cryptology – EUROCRYPT 2023* (pp. 423–447). Springer.
- Krishnan, M., Aitha, A. R., Amistapuram, K., Nandan, B. P., Kaulwar, P. K., & Singireddy, J. (2025). Human-in-the-Loop Hybrid Neuro-Symbolic AI Model for Reliable Data Engineering in High-Stakes Industrial Systems. In 2025 IEEE 3rd Global Conference on Wireless Computing and Networking (GCWCN) (pp. 1–7). IEEE. 2025 IEEE 3rd Global Conference on Wireless Computing and Networking (GCWCN). <https://doi.org/10.1109/gcwcnc66157.2025.11448516>
- Devevey, J., Fallahpour, P., Passelègue, A., & Stehlé, D. (2023). A detailed analysis of Fiat-Shamir with aborts. In H. Handschuh & A. Lysyanskaya (Eds.), *Advances in Cryptology – CRYPTO 2023* (pp. 327–357). Springer.
- Baladari, V., Nagubandi, A. R., Charan Teja Tadi, S. R. C., Selvi, A. T., Sreedevi, V., & Nithya, M. (2026). Predictive AI Model for Financial Risk Assessment in Dynamic Market Environments. In 2026 International Conference on Communication, Computing and Emerging Technologies (IC3ET) (pp. 748–753). IEEE. 2026 International Conference on Communication, Computing and Emerging Technologies (IC3ET). <https://doi.org/10.1109/ic3et64989.2026.11467452>
- Dey, J., & Dutta, R. (2023). Progress in multivariate cryptography: Systematic review, challenges, and research directions. *ACM Computing Surveys*, 55(12), 1–34.
- Kolla, T. (2024). AI-Powered Data Catalog Systems For Healthcare Data Discovery And Governance. *South Eastern European Journal of Public Health*, 2296–2311. <https://doi.org/10.70135/seejph.vi.7077>
- Goertzen, J., & Stebila, D. (2023). Post-quantum signatures in DNSSEC via request-based fragmentation. In *Post-Quantum Cryptography: 14th International Workshop, PQCrypto 2023* (pp. 535–564). Springer.
- Wang, Q., Wang, D., Cheng, C., & He, D. (2023). Quantum2FA: Efficient quantum-resistant two-factor authentication scheme for mobile devices. *IEEE Transactions on Dependable and Secure Computing*, 20(1), 193–208.

- Dawadi, D., Yandamuri, U. S., V, S. K., Stalin, J. L. A., & Naveenkumar, R. (2005). Privacy-Aware Edge-Based Intelligent Video Analytics for Scalable Crowd Management in Smart Cities. In 2026 3rd International Conference on Integrated Intelligence and Communication Systems (ICIICS) (pp. 1–7). IEEE. 2026 3rd International Conference on Integrated Intelligence and Communication Systems (ICIICS). <https://doi.org/10.1109/iciics67880.2026.11483444>
- Bettale, L., De Oliveira, M., & Dottax, E. (2022). Post-quantum protocols for banking applications. In International Conference on Smart Card Research and Advanced Applications (pp. 271–289). Springer.
- Beullens, W. (2022). Breaking Rainbow takes a weekend on a laptop. In Y. Dodis & T. Shrimpton (Eds.), *Advances in Cryptology – CRYPTO 2022* (pp. 464–479). Springer.
- None, D. N. P., None, P. D., None, S. H. K., None, D. C. C. & None, A. G. (2026). Financialization of Sustainability and Shadow Capitalism: ESG Signaling, Regulatory Arbitrage, and Corporate Legitimacy in the Post-BEPS Global Tax Era. *Journal of European Economic History*, 7(2), 492-943.
- Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, 605(7909), 237–243.
- Davuluri, P. N., Segireddy, A. R., & Sheelam, G. K. (2026). Comment on" Effectiveness of AI-assisted ESI triage on accuracy and selected outcomes in emergency nursing: A systematic review". *International emergency nursing*, 87, 101846.
- Beullens, W. (2021). Improved cryptanalysis of UOV and rainbow. In A. Canteaut & F.-X. Standaert (Eds.), *Advances in Cryptology – EUROCRYPT 2021* (pp. 348–373). Springer.
- Hatakeyama, K., Kotani, D., & Okabe, Y. (2021). Zero trust federation: Sharing context under user control towards zero trust in identity federation. In 2021 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops) (pp. 514–519). IEEE.
- Nandan, B. P., Kumar, M. V. K., Garapati, R. S., Bandi, V. D. V. K., Davuluri, P. S. L. N., & Mangalampalli, B. M. (2026). AI-Enhanced Semiconductor Yield Optimization Using Hybrid Deep Learning and Edge Data Analytics. In 2026 IEEE International Conference on AI Engineering and Innovations (AIEI) (pp. 1–6). IEEE. 2026 IEEE International Conference on AI Engineering and Innovations (AIEI). <https://doi.org/10.1109/aiei69164.2026.11497190>
- Ravi, P., Howe, J., Chattopadhyay, A., & Bhasin, S. (2021). Lattice-based key-sharing schemes: A survey. *ACM Computing Surveys*, 54(1), 1–39.
- Sharma, P., Agrawal, A., Bhatia, V., Prakash, S., & Mishra, A. K. (2021). Quantum key distribution secured optical networks: A survey. *IEEE Open Journal of the Communications Society*, 2, 2049–2083.
- Mattaparathi, R. (2025). GenAI-Augmented Diagnostic Reasoning for Diesel Engine Fault Triage: A Large Language Model Framework for Technician Decision Support at Scale. *Journal of Material Sciences & Manufacturing Research*, 6(12), 1. [https://doi.org/10.47363/jmsmr/2025\(6\)226](https://doi.org/10.47363/jmsmr/2025(6)226)
- Paquin, C., Stebila, D., & Tamvada, G. (2020). Benchmarking post-quantum cryptography in TLS. In *Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020* (pp. 72–91). Springer.
- Hiremath, N. B., Kolla, S. K., Sunkara, R., G, S. Lal., & Sireesha, K. (2026). Adaptive and Intelligent Secure Multimedia Transmission for Dynamic Communication Systems. In 2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN) (pp. 1–8). IEEE. 2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN). <https://doi.org/10.1109/iciscn67954.2026.11566143>
- Bernstein, D. J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J., & Schwabe, P. (2019). The SPHINCS+ signature framework. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2129–2146). Association for Computing Machinery.
- Fouque, P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., & Zhang, Z. (2018). Falcon: Fast-Fourier lattice-based compact signatures over NTRU. Submission to the NIST post-quantum cryptography standardization process.
- Mangala, S. B. G. N., Kolla, S. K., Segireddy, A. R., & Yandamuri, U. S. (2026). Designing Intelligent, Scalable Data Ecosystems for Precision Healthcare: A Cloud-Native Approach to Predictive and Automated Decision

-
- Systems. *Advanced Engineering Sciences*, 58(1), 492-943.
- Melchor, C. A., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C., Gaborit, P., Persichetti, E., & Zémor, G. (2018). Hamming quasi-cyclic (HQC). NIST PQC Round 2 submission.
- AGENTIC AI FRAMEWORKS FOR AUTONOMOUS RISK DETECTION AND COMPLIANCE REMEDIATION IN ENTERPRISE DATA CENTER OPERATIONS. (2025). *Lex Localis - Journal of Local Self-Government*, 23(S6), 492-943. <https://doi.org/10.52152/3f90ak91>
- Langlois, A., & Stehlé, D. (2015). Worst-case to average-case reductions for module lattices. *Designs, Codes and Cryptography*, 75(3), 565–599.
- Ducas, L., Lyubashevsky, V., & Prest, T. (2014). Efficient identity-based encryption over NTRU lattices. In P. Sarkar & T. Iwata (Eds.), *Advances in Cryptology – ASIACRYPT 2014* (pp. 22–41). Springer.
- Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6), 1–40.
- Jyoshna, K., Peddi, R. K., & Punitha, S. (2026, April). Spatio-Temporal Graph Neural Network with Global Spatio-Temporal Network for the Traffic Flow Prediction. In *2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN)* (pp. 492-943). IEEE.
- Micciancio, D. (2004). Almost perfect lattices, the covering radius problem, and applications to Ajtai's connection factor. *SIAM Journal on Computing*, 34(1), 118–169.
- McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report*, 42–44, 114–116.
- Padma, G., Reddy, V. A. R., A, S. Devi. K., Buvaneswari, B., & Kumar, K. S. S. (2026). Privacy-Preserved Face Recognition Biometric Authentication Using FaceNet and Zero-Knowledge Proofs for Secure, Access Control on Decentralized Blockchain Networks. In *2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN)* (pp. 1–8). IEEE. *2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN)*. <https://doi.org/10.1109/iciscn67954.2026.11566528>