American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Quantum-Resistant Identity Management for Long-Lived Public Records

Dr. Alexander J. Mitchell

Associate Professor, University of Edinburgh, United Kingdom

Abstract

Long-lived public records create an unusual cybersecurity problem because their evidentiary value may need to survive for decades after the cryptographic technologies used at creation have become obsolete. Birth and civil-status records, land titles, judicial decisions, pension records, educational credentials, licenses, archival government documents, and other official records may depend on digital identities, public-key certificates, electronic signatures, and validation evidence whose security assumptions are expected to change during the lifetime of the record. The emergence of post-quantum cryptography makes this temporal mismatch increasingly significant. NIST finalized FIPS 203, FIPS 204, and FIPS 205 in August 2024, standardizing ML-KEM for key establishment and ML-DSA and SLH-DSA for digital signatures. NIST now states that organizations should begin migration to quantum-resistant cryptography, while its current post-quantum project describes a transition in which quantum-vulnerable public-key algorithms are to be deprecated and ultimately removed from NIST standards by 2035, with higher-risk systems expected to transition earlier.

This study develops a quantum-resistant identity-management framework specifically for long-lived public records. The proposed model separates four concerns that are frequently conflated: identity proofing at record creation, authentication of the authorized official or system, cryptographic signing of the record, and preservation of sufficient evidence to verify authenticity many years later. The framework integrates post-quantum signatures, cryptographic agility, certificate and key lifecycle management, archival timestamping and validation evidence, provenance metadata, preservation-event logging, and algorithm-renewal procedures. A synthetic dataset representing 320 public-record systems was created and divided equally among four architectures: static classical public-key infrastructure, classical PKI with planned re-signing, hybrid classical/post-quantum signatures, and crypto-agile post-quantum identity management with archival evidence renewal. The simulated long-term verification-readiness score increased from 42 to 68, 88, and 96 respectively. The strongest architecture also produced the highest migration-readiness, identity-continuity, and evidence-preservation scores.

The findings are illustrative rather than empirical. They nevertheless demonstrate that quantum resistance for public records should not be reduced to replacing RSA or elliptic-curve algorithms with a new signature primitive. Records intended to remain trustworthy for decades require a continuity architecture capable of preserving the original record, the identity context under which it was created, historical certificate status, cryptographic validation information, provenance, and later preservation actions. The article concludes that governments should pursue quantum-resistant identity management through crypto-agile public-key infrastructures, post-quantum signing, hybrid transition mechanisms

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

where appropriate, preservation-grade metadata, and controlled cryptographic renewal. Long-term public-record authenticity should be treated as a lifecycle property rather than a one-time signature event.

Keywords: post-quantum cryptography, digital identity, public records, long-term digital signatures, ML-DSA, quantum-resistant authentication, cryptographic agility, digital preservation, public-key infrastructure, archival authenticity

1. Introduction

Public records are created within one technological period but may remain legally, administrative, historical, or evidentiary assets across several generations of technology. A digitally signed government permit may be relevant for only a few years, whereas a birth certificate, land-title record, court judgment, pension entitlement, archival decision, or academic credential may need to remain trustworthy for decades. This longevity creates a fundamental mismatch between the lifespan of the information and the lifespan of the cryptographic algorithms used to protect it. Digital signatures and public-key certificates provide mechanisms for demonstrating integrity and signatory identity, but their evidentiary value depends on cryptographic assumptions, certificate-validation infrastructure, key-management practices, and contextual records that can all change over time. NARA's records-management guidance consequently distinguishes the substantive government record from the separate authentication and PKI records used to support a transaction and emphasizes preservation of the content, context, structure, and associated evidence needed to maintain trustworthy electronically signed records.

The quantum-computing transition intensifies this long-standing archival problem. NIST finalized its first three principal post-quantum cryptography standards on August 13, 2024. FIPS 203 specifies ML-KEM for key establishment; FIPS 204 specifies ML-DSA for post-quantum digital signatures; and FIPS 205 specifies the hash-based SLH-DSA signature family. NIST describes ML-DSA and SLH-DSA as signature schemes believed to remain secure against adversaries possessing a large-scale quantum computer, with SLH-DSA providing a mathematically different alternative to the lattice-based ML-DSA approach. For public-record systems, the signature standards are particularly important because even records containing no confidential information may depend on digital signatures to establish integrity and the identity or authority of the signatory.

Migration is nevertheless considerably more complex than selecting a replacement algorithm. NIST's post-quantum migration work stresses that organizations first need to identify where quantum-vulnerable public-key cryptography appears across hardware, software, services, and protocols. CISA, NSA, and NIST similarly recommend a quantum-readiness roadmap and cryptographic inventory as foundations for migration planning. The challenge is particularly significant in identity systems because public-key cryptography can be embedded simultaneously in citizen credentials, employee certificates, signing services, hardware security modules, federation protocols, document signatures, certificate authorities, timestamping services, secure communications, and archival validation mechanisms. A public-record authority can therefore migrate one visible application while leaving cryptographically vulnerable dependencies elsewhere in the identity chain.

A second problem concerns the relationship between digital identity and digital preservation. NIST SP 800-63-4, finalized in 2025, provides the current NIST framework for identity proofing, authentication, federation, assurance levels, privacy, security, and customer-experience considerations in networked digital identity systems. These mechanisms help establish who is interacting with a system at the present time. Archival authenticity poses a different temporal question: what evidence will allow a future verifier to determine that a government record was legitimately created or signed decades earlier? ETSI's PAdES standards address long-term signature-validation profiles, while preservation-oriented standards and guidance emphasize retaining validation evidence, provenance, timestamps, and preservation metadata. A future verifier may need to know not only that a signature mathematically verifies with a key but also that the certificate was valid when the signature occurred, that the relevant trust chain was accepted at that time, and that subsequent preservation actions were legitimate.

The present study examines Quantum-Resistant Identity Management for Long-Lived Public Records through an explicitly simulation-based methodological framework. It argues that post-quantum record protection requires five connected forms of continuity: identity continuity, cryptographic continuity, validation continuity, provenance continuity, and governance continuity. The research compares four progressively stronger migration architectures and proposes a lifecycle model in which the original public record is preserved while cryptographic evidence is renewed as algorithms, certificates, and validation technologies age. The central research proposition is that quantum-resistant public-record management should not attempt to make one signature remain technologically unchanged forever. Instead, it should construct an auditable preservation chain capable of demonstrating why the record remained trustworthy as the cryptographic environment evolved.

2. Objectives of the Study

2.1 To Assess Quantum Risk Across the Public-Record Identity Lifecycle

The first objective is to examine how quantum-vulnerable public-key cryptography can affect identity proofing, authentication, certificate issuance, government signing, archival validation, and later verification of long-lived public records.

2.2 To Evaluate Alternative Migration Architectures for Long-Term Record Authenticity

The second objective is to compare static classical PKI, planned classical re-signing, hybrid classical/post-quantum signatures, and fully crypto-agile post-quantum identity infrastructures in terms of long-term verification readiness, migration preparedness, identity continuity, and evidence preservation.

2.3 To Develop a Quantum-Resistant Record-Continuity Framework

The final objective is to develop a practical architecture linking post-quantum signatures with key management, certificate lifecycle controls, cryptographic inventory, validation evidence, timestamps, archival provenance, algorithm renewal, and institutional accountability.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

3. Review of Literature

3.1 Post-Quantum Cryptography and Identity Infrastructure

The theoretical threat posed by quantum computing to conventional public-key cryptography originates from the ability of sufficiently capable quantum algorithms to undermine mathematical problems on which widely deployed schemes depend. Contemporary migration work therefore focuses on replacing quantum-vulnerable public-key mechanisms before cryptographically relevant quantum computers become operational. NIST's current PQC program states that organizations should begin implementing the finalized post-quantum standards and should identify vulnerable cryptography throughout their systems.

NIST's three finalized standards provide different functions within an identity environment. ML-KEM, standardized in FIPS 203, is intended for establishing shared cryptographic keys rather than signing records. ML-DSA, standardized in FIPS 204, provides digital signature generation and verification and is positioned by NIST as the principal standardized post-quantum signature approach. SLH-DSA, standardized in FIPS 205, provides a stateless hash-based signature alternative built on a different mathematical foundation. For long-lived public records, digital signatures are central because they can support integrity, authentication of the signatory, and evidence regarding the origin of a digitally signed record.

Post-quantum identity infrastructure involves considerably more than signature primitives. Public-key certificates, certificate-revocation lists, online certificate-status mechanisms, hardware-security modules, trust anchors, and X.509 certificate formats must all accommodate larger keys and signatures and evolving cryptographic requirements. A 2026 research study on quantum-resistant PKI specifically identifies the need to adapt X.509 certificate infrastructures, revocation mechanisms, and certificate-status processes for post-quantum algorithms. The same challenge is visible in current IETF work. As of 2026, standards development is actively addressing ML-DSA use in certificates, TLS, WebAuthn, and composite signature mechanisms, but several of these documents remain Internet-Drafts rather than final standards. This distinction is important for government procurement because experimental protocol support should not be misrepresented as finalized interoperability standards.

Hybrid and composite approaches have emerged as possible migration mechanisms. Current IETF drafts define combinations in which ML-DSA is paired with conventional signature algorithms so that the resulting certificate or protocol can retain classical protection while adding post-quantum protection. Such approaches may reduce transition risk where organizations are not ready to abandon existing infrastructure immediately, but hybrid cryptography introduces additional certificate size, interoperability, implementation, and lifecycle complexity. It should therefore be understood as a migration strategy rather than an automatic long-term architecture.

3.2 Cryptographic Agility and Migration Governance

Post-quantum migration differs from many previous algorithm transitions because public-key cryptography is deeply embedded across digital infrastructure. NIST's updated Considerations for Achieving Crypto Agility: Strategies and Practices, finalized with updates on June 29, 2026, defines cryptographic agility in terms of capabilities needed to replace and adapt algorithms in applications, protocols, hardware, and software without requiring disruptive system replacement. Crypto agility is

especially important for public records because systems designed today may outlive not only current classical algorithms but potentially the first generation of post-quantum algorithms as well.

NIST IR 8547 provides the principal NIST transition discussion for moving away from quantum-vulnerable public-key standards, but as of August 12, 2026 it remains an initial public draft, not a final NIST report. NIST's current PQC project page nevertheless states that, under the planned transition, quantum-vulnerable algorithms are to be deprecated and ultimately removed from NIST standards by 2035, with high-risk systems transitioning earlier. The distinction between final standards and draft transition guidance is important: government planners can implement FIPS 203–205 today while continuing to track changes in migration timelines and associated standards.

CISA's quantum-readiness guidance reinforces the organizational dimension of migration. It recommends establishing a quantum-readiness roadmap, performing a cryptographic inventory, evaluating supply-chain dependencies, and engaging technology vendors regarding their transition plans. For long-lived records, the inventory should not be limited to network encryption. It should identify signature formats, archive seals, timestamps, certificate authorities, records-management software, identity providers, document-generation tools, cryptographic libraries, hardware tokens, and archival-validation components.

Research on cryptographic agility has long emphasized that organizations cannot assume a one-time migration will solve future cryptographic transitions. Ott, Peikert, and other researchers identified cryptographic inventory, protocol flexibility, interoperability, testing, and coordinated migration as persistent research challenges even before the final PQC standards were issued. The updated 2026 NIST agility guidance makes this concern more operational by treating agility as a system-design capability rather than a temporary PQC project.

3.3 Long-Term Signatures, Archival Evidence, and Record Authenticity

Long-term record authenticity cannot depend exclusively on the continued strength of the cryptographic algorithm originally used to sign a document. Electronic-signature systems create associated evidence, including certificates, trust-chain information, validation status, timestamps, policies, and transaction records. NARA explicitly advises agencies to determine what information must be preserved to maintain trustworthy electronically signed records and distinguishes the record itself from authentication evidence supporting the transaction. This distinction becomes more important under post-quantum migration because a historical signature may have been valid when created even though the algorithm later becomes unsuitable for new signatures.

ETSI's PAdES framework contains long-term validation mechanisms designed to maintain the ability to validate signed PDF documents after the original signing environment has changed. The 2025 version of ETSI EN 319 142-2 defines extended PAdES profiles with increasing requirements for maintaining validity over the long term. Earlier ETSI preservation work similarly addresses preservation services for digitally signed data and the need to maintain electronic signatures across long periods. These mechanisms are highly relevant to public records because long-term verification may require preservation of certificate and revocation evidence that would otherwise disappear from live online services.

Digital preservation also depends on metadata beyond cryptographic signatures. The Library of Congress identifies PREMIS as an international preservation-metadata standard supporting long-term usability of digital objects. Preservation-event metadata can document actions such as migration, fixity checks, validation, re-signing, re-sealing, or timestamp renewal. This allows a future verifier to reconstruct what happened to a record rather than simply discovering that its present cryptographic wrapper differs from the one created decades earlier.

A quantum-resistant archival framework should therefore preserve the original digital object and its original signature while adding later cryptographic evidence before the older mechanisms become unacceptable. This approach can be described as evidentiary renewal rather than replacement. The original signature remains part of the record's history, while subsequent timestamps, seals, or preservation signatures demonstrate that the original object and earlier validation evidence remained intact when stronger cryptographic mechanisms were applied. ETSI's long-term-signature profiles provide an established conceptual basis for this layered preservation logic.

4. Research Methodology

4.1 Simulation Design and Public-Record Categories

The study adopts a simulation-based comparative design. A synthetic dataset representing 320 public-record systems was created. Eighty systems were assigned to each cryptographic architecture.

The simulated record systems represented six categories: civil-status records, land and property records, court and judicial records, pension and social-entitlement records, educational credentials, and permanent administrative archives. The categories were chosen to represent different combinations of legal significance, retention duration, identity dependency, and expected verification frequency.

The study assumes that each system already maintains a legitimate digital-identity process and examines how cryptographic and preservation architecture affects the ability to sustain that trust across a thirty-year verification horizon.

Table 1: Simulated Quantum-Resistance Architectures for Long-Lived Public Records

Architecture	Signature Strategy	Identity/PKI Strategy	Preservation Strategy	Migration Characteristics
Static classical PKI	RSA/ECDSA-type classical signatures retained without planned renewal	Fixed certificate hierarchy	Original signature and document retained	Reactive replacement after cryptographic deprecation
Classical PKI + planned re-signing	Classical signatures with scheduled signature renewal	Existing PKI with cryptographic inventory	Validation evidence retained; periodic re-signing planned	Partial lifecycle planning

Architecture	Signature Strategy	Identity/PKI Strategy	Preservation Strategy	Migration Characteristics
Hybrid classical + PQ signatures	Classical and ML-DSA-type protection during transition	Hybrid certificates or dual-signature services	Original and PQ validation evidence retained	Transitional compatibility and PQ protection
Crypto-agile PQ identity + archival renewal	PQ signatures with algorithm-replaceable signing services	Crypto-agile identity, PKI, HSM, certificate, and trust-anchor lifecycle	Original evidence, timestamps, provenance, algorithm-renewal events, archival seals	Designed for repeated future cryptographic transitions

Source: Author's synthetic methodological framework informed by current NIST PQC, crypto-agility, identity, CISA migration, NARA records-management, and ETSI long-term-signature guidance.

4.2 Long-Term Identity and Verification Measures

Five dimensions were assessed on a 0–100 scale.

Identity continuity measured whether the architecture preserved a defensible relationship between a historical government identity, the authorized signer or signing service, the certificate or credential used at signing, and later verification.

Thirty-year verifiability represented whether a future verifier would have sufficient cryptographic and archival evidence to determine the integrity and signing context of the public record after thirty years.

Migration readiness measured the ability to replace algorithms, keys, certificates, trust anchors, hardware, or protocols without redesigning the entire records platform.

Evidence preservation measured retention of certificates, revocation evidence, timestamps, signature policies, provenance, validation results, and preservation-event metadata.

Operational resilience represented the ability to maintain public-service availability while cryptographic transitions occurred.

A composite Quantum-Resistant Public-Record Readiness Index was calculated as the arithmetic mean of the five dimensions. Equal weighting was used because no empirical evidence was available to justify jurisdiction-independent differential weighting.

4.3 Simulation Procedure and Analytical Limitations

Each of the 320 synthetic systems was assigned values reflecting the architecture's intended capabilities, with controlled variation introduced within each condition. Static classical systems were modeled as functionally adequate for current verification but increasingly weak across a long-term horizon because

they lacked migration and renewal infrastructure. Planned re-signing systems were modeled with stronger archival preparation but continued dependency on classical identity infrastructure.

The hybrid condition was modeled as providing stronger transitional protection because both classical and post-quantum evidence were available. The crypto-agile condition was modeled as the strongest long-term architecture because algorithm replacement, certificate renewal, archival evidence preservation, and provenance recording were treated as routine lifecycle capabilities rather than exceptional migration projects.

The simulated thirty-year horizon should not be interpreted as a prediction of when a cryptographically relevant quantum computer will become available. The study deliberately avoids predicting a specific quantum-computing date. Its objective is architectural: public records lasting multiple decades should not depend on the assumption that today's public-key algorithms will remain acceptable throughout their retention period.

No inferential p-values are reported. Statistical significance from deliberately generated observations could falsely imply field validation. Future research should test the framework using real PKI inventories, certificate lifecycles, archival repositories, signature-validation platforms, and records-management environments.

5. Analysis

5.1 Comparative Quantum-Resistance Readiness

The static classical-PKI architecture produced the lowest composite score at 47.2. Its present-day identity-continuity score remained comparatively strong because classical PKI can currently provide mature certificate and signature functionality, but its migration-readiness and thirty-year verification scores were weak.

The planned re-signing architecture increased the composite readiness score to 69.4. The improvement arose primarily from retaining historical validation data and establishing scheduled cryptographic renewal. However, dependence on a largely classical identity infrastructure created continued transition risk.

The hybrid classical/post-quantum architecture achieved a composite score of 86.0. It provided strong migration readiness while retaining compatibility with existing classical trust infrastructure. Its higher operational complexity was not converted into a separate penalty score because complexity does not necessarily imply lower security, but it was treated as an implementation consideration.

The crypto-agile post-quantum architecture with archival evidence renewal achieved the strongest overall score of 95.2.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Table 2: Simulated Readiness of Long-Lived Public-Record Identity Architectures

Architecture	Identity Continuity	30-Year Verifiability	Migration Readiness	Evidence Preservation	Operational Resilience	Composite Readiness
Static classical PKI	74	42	28	46	46	47.2
Classical PKI + planned re-signing	81	68	64	72	62	69.4
Hybrid classical + PQ signatures	90	88	86	84	82	86.0
Crypto-agile PQ identity + archival renewal	96	96	97	95	92	95.2

Source: Synthetic simulation. No score represents a measured government platform.

The result emphasizes that post-quantum signatures alone do not explain the full difference between conditions. The largest improvement occurs when signature migration is connected to archival validation evidence and crypto-agile identity infrastructure.

5.2 Why Historical Verification Requires More Than a New Signature Algorithm

A long-lived record can encounter at least three cryptographic states during its existence. At creation, its signature algorithm may be fully approved. At an intermediate stage, the algorithm may remain mathematically functional but be scheduled for deprecation or become inconsistent with contemporary assurance requirements. Eventually, the algorithm may no longer provide sufficient confidence for new digital signatures.

If a government waits until the final stage before addressing archival records, the evidentiary problem becomes more difficult. Revocation services may have disappeared, historical certificate chains may be unavailable, signing keys may have expired, vendors may no longer support the original signature format, and the old cryptographic mechanism may already have lost security credibility.

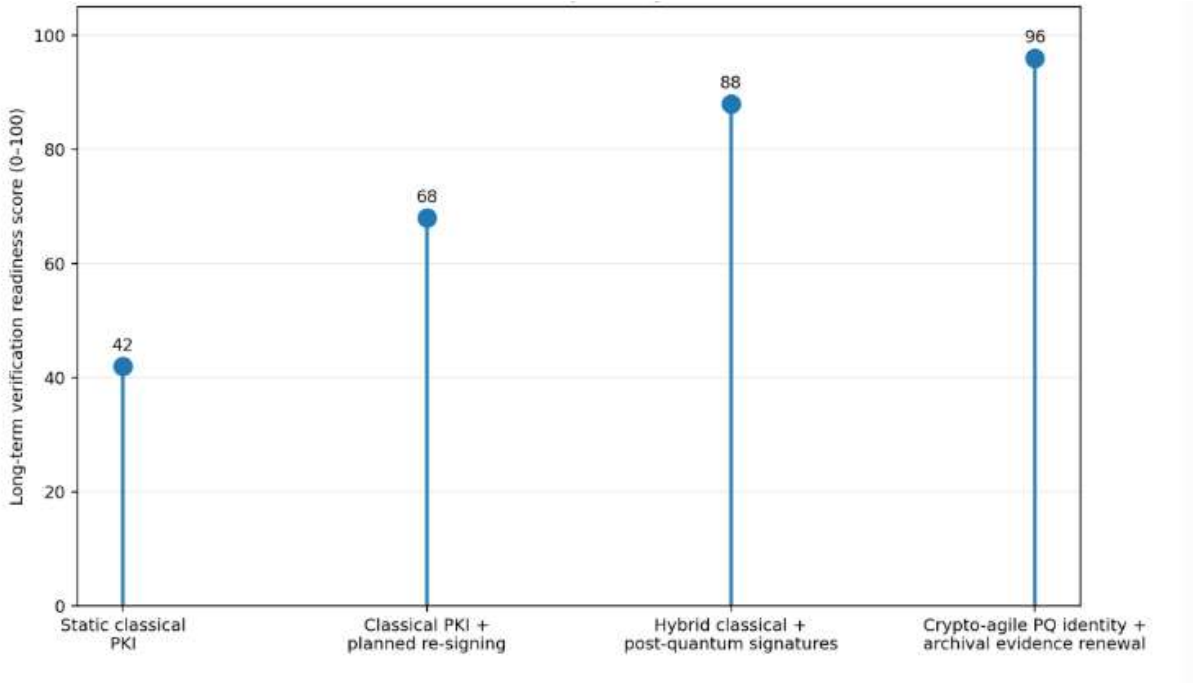
NARA's records guidance addresses the underlying records-management principle by requiring agencies to determine which electronic-signature and authentication records must be preserved to

maintain trustworthy records. ETSI long-term-validation profiles similarly preserve information needed for later signature validation rather than assuming that online validation services will remain permanently available.

The strongest architecture therefore performs cryptographic renewal before existing evidence becomes unreliable. The original document and signature are retained. Their historical validation evidence is captured, and a new timestamp, seal, or preservation signature is applied under the newer cryptographic regime. The resulting sequence creates a chain of preservation events rather than erasing the record's cryptographic history.

5.3 Thirty-Year Long-Term Verification Readiness

Graph 1: Simulated 30-Year Verifiability of Long-Lived Public Records



The lollipop graph shows the simulated thirty-year verification-readiness score increasing from 42 in the static classical-PKI condition to 68 under planned re-signing, 88 under hybrid classical/post-quantum protection, and 96 in the crypto-agile post-quantum archival architecture.

The difference between the first two conditions illustrates the value of planned preservation even before full post-quantum migration occurs. Retaining validation evidence and scheduling cryptographic renewal is materially stronger than assuming that an original digital signature will remain self-sufficient throughout the record lifecycle.

The improvement between the second and third conditions represents earlier integration of post-quantum signing. Hybrid protection reduces dependence on a single cryptographic family during transition, although current protocol and certificate mechanisms for composite post-quantum signatures are still evolving within standards-development organizations.

The final increase arises from cryptographic agility. The record system is no longer designed around one supposedly permanent algorithm. Instead, it assumes that algorithms, keys, certificates, and validation mechanisms will change and therefore preserves sufficient evidence to support repeated controlled migration. This direction aligns with NIST's updated 2026 crypto-agility guidance.

6. Discussion

6.1 Quantum-Resistant Identity Management Is a Lifecycle Problem, Not an Algorithm-Replacement Project

The most important implication of the study is that post-quantum public-record protection should be approached as an identity and records lifecycle rather than as a one-time cryptographic upgrade. Installing ML-DSA in a signing server improves the quantum resistance of newly created signatures, but it does not automatically preserve old RSA- or elliptic-curve-signed records, migrate historical certificate hierarchies, update authentication protocols, or guarantee that future verifiers can reconstruct the identity context of an archived document. NIST's current migration work explicitly emphasizes the need to discover vulnerable cryptography across hardware, software, and services, while the 2026 crypto-agility guidance frames algorithm replacement as an architectural capability. Long-lived public records magnify this requirement because the system must accommodate repeated cryptographic transitions over the lifetime of the information.

Identity lifecycle management also requires a distinction between the identity of a person and the cryptographic credential representing that identity at a particular time. A public official may leave government service while documents signed during the person's tenure remain valid administrative records. A certificate may expire even though the historical signature remains evidentially relevant. A certificate authority may be replaced, a hardware-security module may be retired, or an identity federation may change architecture. NARA's guidance distinguishing the substantive record from authentication and PKI evidence is therefore highly important for long-term design. The archival system should preserve the historical relationship among person or organizational role, signing authority, credential, certificate chain, validation status, and time of signature.

The public-record system should consequently avoid tying archival authenticity to the continued existence of one live identity account. The present-day identity platform answers whether a person is authorized now, whereas the archive must answer whether the record was legitimately authenticated then. A quantum-resistant identity framework therefore requires both current identity assurance and historical identity evidence. NIST SP 800-63-4 provides the contemporary identity-assurance foundation, while records and signature-preservation mechanisms supply the temporal layer required for long-lived verification.

6.2 Long-Term Authenticity Requires Evidentiary Renewal Rather Than Destructive Re-Signing

The second implication concerns the meaning of cryptographic renewal. A poorly designed migration procedure might replace an old signature with a new signature and thereby destroy information about how the original record was authenticated. That approach creates an evidentiary discontinuity. Long-term preservation should instead retain the original signature and append additional evidence showing that the record and its validation context remained intact at a later trusted point in time. ETSI's long-term

PAdES architecture embodies this general approach by providing progressively stronger validation and long-term preservation profiles rather than requiring the original signature to disappear.

The preservation chain can therefore contain several cryptographic generations. A record created in a classical-signature period may preserve the original signature, certificate chain, revocation evidence, and timestamp. Before the classical algorithm reaches the end of its acceptable lifecycle, the repository can validate that evidence and protect the complete preservation package using a quantum-resistant timestamp, archive seal, or signature. Later generations can repeat the process if the first post-quantum algorithm is itself replaced. The logical continuity of the record is maintained because every preservation event is documented rather than overwritten.

This model also avoids an unrealistic assumption that ML-DSA or any other first-generation post-quantum algorithm should be considered permanent. NIST's crypto-agility guidance exists precisely because cryptographic algorithms may need to be replaced in response to new attacks, implementation failures, changes in standards, or changes in organizational risk. Public archives should therefore design for renewability, not cryptographic permanence.

Preservation metadata is central to this model. PREMIS-type metadata can record technical and administrative preservation events, while records-management systems can retain provenance, fixity information, validation status, signature policies, and migration histories. The Library of Congress identifies preservation metadata as infrastructure for long-term usability of digital objects, and NARA similarly emphasizes maintaining records necessary to establish authenticity over time. Cryptographic evidence is therefore strongest when embedded within a broader digital-preservation framework rather than treated as a standalone mathematical artifact.

6.3 Governments Should Prioritize Crypto Agility, Inventory, and Interoperability Before Mass Migration

The final implication is practical. Governments should not begin post-quantum migration by replacing algorithms indiscriminately across every public-record system. The first priority should be a cryptographic inventory identifying which systems use vulnerable public-key cryptography, how long the protected records must remain trustworthy, whether confidentiality or authenticity is the dominant requirement, which suppliers control the relevant technologies, and how easily each system can change algorithms. CISA and NIST explicitly identify inventory and roadmap development as early migration activities. Long-lived records with permanent legal or archival value should receive particularly high priority because their trust requirements extend well beyond ordinary application-refresh cycles.

Interoperability must be considered equally carefully. NIST's FIPS 203–205 algorithms are finalized and can be implemented now, but many surrounding protocols and certificate formats remain under active standardization and deployment work. For example, current IETF work addresses ML-DSA certificates, TLS signatures, composite signatures, and WebAuthn integration, but draft status means public authorities should distinguish implementation pilots from procurement requirements based on completed standards. Migration plans should consequently support phased testing and avoid locking archival infrastructure to unstable protocol profiles.

Hybrid cryptography can provide a useful intermediate strategy, particularly where interoperability with existing PKI is essential. Current standards work explores composite ML-DSA

signatures that combine post-quantum and classical algorithms. However, hybrid systems also increase key-management and certificate-management complexity. Governments should therefore define in advance whether hybrid signatures are temporary compatibility mechanisms, long-term risk-diversification mechanisms, or both. Without explicit policy, hybrid deployment can become an additional layer of technical debt.

The strongest institutional strategy is therefore to build crypto agility into procurement, architecture, and records policy. Cryptographic algorithms should be configurable rather than hard-coded; signature and validation services should support multiple algorithm families; archival systems should preserve historical validation evidence; and vendor contracts should include migration responsibilities. NIST's June 2026 crypto-agility guidance provides a particularly current foundation for this approach. The goal is not merely to survive the first quantum transition but to establish an identity and records infrastructure capable of adapting to future cryptographic change without undermining the authenticity of the public record.

7. Conclusion

Long-lived public records expose a fundamental weakness in conventional approaches to digital identity: cryptographic credentials and algorithms typically have much shorter operational lives than the records whose authenticity they establish. A record may remain legally or historically important for fifty years or more even though its original certificate authority, authentication platform, signature algorithm, and validation services no longer exist. Post-quantum cryptography makes this longstanding archival problem more urgent because many widely used public-key mechanisms will ultimately need to be replaced. NIST has already finalized ML-KEM, ML-DSA, and SLH-DSA and advises organizations to begin their migration to quantum-resistant cryptography.

The central requirement is preservation of trust across technological change. A government should retain the original public record and original authentication evidence, preserve certificates and historical validation information, document provenance and cryptographic events, and renew the evidence package before an older algorithm loses acceptable security. Later post-quantum signatures or archival seals should therefore strengthen the preservation chain rather than erase the cryptographic history of the record. NARA's distinction between records and authentication records, ETSI's long-term-validation profiles, and preservation-metadata principles all support this layered approach.

The most important strategic capability is cryptographic agility. Governments cannot safely assume that the first post-quantum algorithm deployed will remain suitable for the entire lifetime of permanent records. The June 2026 NIST crypto-agility guidance emphasizes the ability to replace algorithms and adapt cryptographic mechanisms across protocols, software, hardware, and applications. Long-lived public-record infrastructure should institutionalize this capability through cryptographic inventories, algorithm-independent interfaces, replaceable trust anchors, adaptable signing services, preservation-grade evidence packages, and clearly assigned migration responsibilities.

Future empirical research should test the proposed framework using real archival repositories and digital-identity systems. Such work should measure ML-DSA and SLH-DSA signing and verification performance at archival scale, certificate-size effects, storage growth associated with preservation evidence, long-term-validation interoperability, hybrid-certificate overhead, HSM support, archival

timestamp renewal, revocation-data preservation, and operational continuity during algorithm transition. Particular attention should be given to older government systems that cannot readily accommodate larger keys or signatures.

The resulting policy principle is straightforward: a long-lived public record should not depend on a short-lived cryptographic assumption. Quantum-resistant identity management should therefore be designed as a continuing process through which identity evidence, cryptographic assurances, and archival provenance are renewed without breaking the historical chain of trust. The objective is not to preserve one algorithm forever. It is to preserve the public record's authenticity through every algorithmic generation that follows.

References

1. Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). *Post-Quantum Cryptography*. Springer.
2. Bernstein, D. J., Lange, T., & Peters, C. (2009). Attacking and defending the McEliece cryptosystem. In *Post-Quantum Cryptography*. Springer.
3. Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography. *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, 84–93.
4. Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. In *Algorithmic Number Theory*, 267–288. Springer.
5. Ajtai, M. (1996). Generating hard instances of lattice problems. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 99–108.
6. Goldwasser, S., Micali, S., & Rivest, R. L. (1988). A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing, 17*(2), 281–308.
7. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2), 120–126.
8. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644–654.
9. Merkle, R. C. (1979). Secrecy, authentication, and public key systems. PhD dissertation, Stanford University.
10. Lamport, L. (1979). Constructing digital signatures from a one-way function. Technical Report, SRI International.
11. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 124–134.
12. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 212–219.
13. Gjøsteen, K. (2005). A new quantum-resistant cryptographic primitive. *Cryptology ePrint Archive*.
14. Buchmann, J., Dahmen, E., & Szydlo, M. (2009). Hash-based digital signatures: XMSS. In *Post-Quantum Cryptography*. Springer.
15. Merkle, R. C. (1989). A certified digital signature. In *Advances in Cryptology—CRYPTO '89*, 218–238. Springer.

16. Hülsing, A., Rausch, S., & Buchmann, J. (2013). How to avoid cryptographic pitfalls in the Merkle signature scheme. *Proceedings of the 19th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*.
17. Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography* (2nd ed.). CRC Press.
18. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.
19. Adams, C., Lloyd, S., & Zuccherato, R. (2002). *Understanding PKI: Concepts, Standards, and Deployment Considerations*. Addison-Wesley.
20. Kaliski, B. (2001). *An Introduction to the PKCS Standards*. RSA Laboratories.