KERI's Strategy for Post-Quantum Security

October 2025
Daniel Hardman — Provenant — daniel@provenant.net
Sam Smith, PhD — Prosapien — sam@prosapien.com

Introduction: The Ticking Clock

An adversary does not need a quantum computer to threaten your most sensitive data. They only need storage. In a strategy known as "Harvest Now, Decrypt Later" (HNDL), attackers are quietly intercepting and stockpiling encrypted data today — private messages, corporate secrets, classified communications — with the full expectation of decrypting it tomorrow, once a sufficiently powerful quantum computer is built. This silent harvest transforms a future technological breakthrough into a current, and invisible, data security liability. Because the goal is simply to gather and wait, there are no immediate signs of intrusion, and no corrupted files or ransom notes. Organizations live with a false sense of security while their long-term risks accumulate. [NIST 2024; Curtiss-Wright 2025; Palo Alto Networks 2025; Hashicorp 2023]

Data with a long shelf-life is the prime target. Intellectual property, government secrets, and personally identifiable information such as social security numbers retain value for many years, making them ideal candidates for this patient attack. [Cellcrypt 2023] The threat is especially acute in sectors like aerospace and defense, where systems operate for decades, and the data they generate remains sensitive for just as long. Every piece of long-lived data encrypted with today's standard algorithms incurs "quantum debt" — a latent vulnerability that will come due on the day a cryptographically relevant quantum computer arrives.

This threat is not theoretical or far-off, and experts are concerned. NIST finalized the first set of post-quantum cryptography (PQC) standards in August 2024 — FIPS 203, 204, and 205. [NIST 2024] NIST has also established a firm timeline for the transition away from today's widely used public-key algorithms, such as RSA and Elliptic Curve Cryptography (ECC). They are scheduled to be deprecated by 2030 and disallowed after 2035. [Moody et al. 2024; NIST 2024] White House National Security Memorandum 10 (NSM-10) mandates that U.S. federal systems comply with the second NIST deadline. [White House 2022] In Europe, ENISA has published substantive studies and integration guidance for PQC, and the European Commission has urged a coordinated Member-State roadmap for migration and common milestones [ENISA 2024a; ENISA 2024b], India's Telecommunication Engineering Centre and CERT-In released a technical report and whitepaper advising organizations to begin PQC migration planning [TEC 2025], and South Korea has run a national KpqC

program to select local PQC candidates as part of its national PQC master plan. [PQShield 2025] GSMA's regional survey and telecom-sector guidance note active PQC initiatives across many other countries. [GSMA 2025]

Navigating this ambitious transition requires defending against a two-front war. The first front is the HNDL attack on confidentiality, which attempts to crack encrypted data in transit and at rest. [Entrust 2023] The second is a "surprise quantum attack" on control and authenticity. In this scenario, an adversary with a quantum computer could instantly break the signing keys that govern digital identities and assets, allowing them to forge signatures and seize control. [Bernstein & Lange 2017; Augot et al. 2015] Any robust solution must address both threats.

This whitepaper explains how the Key Event Receipt Infrastructure (KERI) provides a comprehensive, architectural defense against the full spectrum of quantum threats. KERI is not a speculative future system; its design offers a secure and practical foundation for digital trust that is resilient against quantum attacks today, while providing an elegant path to adopt tomorrow's cryptographic standards.

	Surprise Quantum Attack	Harvest Now, Decrypt Later (HNDL)
Primary Target	Control & Authenticity	Confidentiality & Secrecy
Asset Attacked	Digital Identity / Asset Control	Encrypted Communications & Data
Vulnerable Component	Asymmetric Signing Keys (e.g., ECDSA, RSA)	Asymmetric Key Exchange (e.g., Diffie-Hellman)
Adversary's Goal	Forge signatures, issue fraudulent events, and take control of an identity.	Intercept and store encrypted traffic to decrypt it in the future.
KERI's Mitigation	Architectural: Pre-rotation mechanism using quantum-safe digests.	Application-Layer: Enables hybrid KEMs or OOB key establishment.
Outcome	Attack is detectable and recoverable. Control of identity is preserved.	Communications are secured against both present and future decryption.

A New Foundation for Trust: The KERI Approach

KERI is a decentralized key management infrastructure (DKMI) designed around the principle of minimal sufficiency. Unlike many contemporary identity systems that rely on exotic cryptography or complex, total-ordered distributed consensus ledgers (blockchains and the like), KERI adopts a more direct and efficient ledgerless approach. Its trust basis is

rooted in data structures made verifiable with straightforward cryptographic primitives, rather than the social and algorithmic consensus of a distributed network. [Smith 2024]

This commitment to simplicity has profound security benefits. By de-emphasizing consensus protocols, KERI deprives hackers of a single, easy-to-find, globally relevant target and eliminates entire classes of blockain vulnerabilities, such as 51% attacks or smart contract exploits. It also replaces claims about theoretical soundness with building blocks that have already been rigorously audited, formally verified, and accepted by governments and industry for years.

The architecture of KERI is built upon two core concepts: Autonomic Identifiers (AIDs) and Key Event Logs (KELs).

Core Concepts: AIDs and KELs

An Autonomic Identifier (AID) is a persistent, self-certifying identifier that serves as a control mechanism for an entity engaged in cryptographic interactions. [Smith 2024]

- The term self-certifying means that the identifier itself contains all the information needed to verify its authenticity. It is cryptographically derived from its controlling public keys, eliminating any dependency on a central registry, trusted third party, or blockchain to establish its validity.
- The term persistent means that the identifier can endure over a long period, even as its controlling keys change. The controller of an AID can "rotate" their cryptographic keys — for example, to upgrade to a stronger algorithm or recover from a compromise — without ever changing the identifier itself. This stability is essential for long-term identity and to KERI's resilience.

A Key Event Log (KEL) is the complete, verifiable history of an AID's evolving key state. It is a simple, append-only data structure where each entry, or "event," is cryptographically linked to the previous one, forming a hash chain. This log records all significant key management operations, starting with the identifier's creation (its inception event) and including every subsequent key rotation. Because the KEL is a self-contained, end-verifiable data structure, anyone, anywhere, at any time can replay the log to cryptographically verify who controlled the AID at any point in its history. [Smith 2024]

This design leads to a powerful outcome: the portability of trust. Because KELs are self-validating, they can be stored and served by any "ambient infrastructure" — a simple web server, a distributed hash table, or even an ordinary USB drive could be used. The underlying infrastructure becomes a replaceable commodity. The trust is not vested in a specific network or service provider, but in the immutable, cryptographic proof contained within the data structure itself. This decouples the root of trust from any single point of

failure, providing a form of future-proofing that is essential for an identity system meant to last for decades.

Thwarting a Quantum Coup: KERI's Pre-Rotation Defense

The most direct threat a quantum computer poses to a digital identity system is a "surprise attack" on control. This attack targets the asymmetric signing keys, such as ECDSA or Ed25519, that are used to prove authority over an identifier. [Bernstein & Lange 2017; Augot et al. 2015] With a sufficiently powerful quantum computer, an adversary could use Shor's algorithm to take a public signing key — which is, by design, visible to the world — and derive the corresponding private key in a matter of hours or minutes. [DHS 2025] With this stolen key, the attacker could forge signatures, issue fraudulent credentials, and hijack the identity.

Most key management systems are brittle in the face of such an attack. If an identity's root key is compromised, control is lost catastrophically and irrevocably. Such systems must migrate to post-quantum algorithms before an attack occurs; if they are compromised first, it is too late to recover. [NIST 2024] KERI, by contrast, is designed for resilience. It anticipates the possibility of key compromise and provides an elegant, built-in mechanism for active, verifiable recovery. This mechanism is called pre-rotation.

The Pre-Rotation Mechanism: A Royal Succession

To understand pre-rotation, it is helpful to use an analogy from history: the rules of royal succession. In KERI, the authority to sign messages and the authority to change the controlling keys are separated.

- The current signing key is like the reigning monarch. Its public key is visible to all, and its signature is law for everyday "interaction events" like signing a message or authenticating to a service.
- The rotation key is the authority that determines the line of succession. It cannot act as a monarch, but it has the power to "crown" a new monarch.

In a traditional system, the public key of the monarch and the public key of the entity with rotation authority might be one and the same, or at least both publicly known. An attacker who overthrows the monarch gains full control.

KERI's pre-rotation works differently. When an identity is first created, or at the moment of any subsequent key rotation, the controller makes a binding commitment to the next set of rotation keys. However, they do not publish the public keys of this heir apparent. Instead, they publish only a cryptographic digest — a hash — of those public keys. [Smith 2024]

This digest acts as an unbreakable royal seal on a secret decree of succession. It provides a verifiable, forward cryptographic commitment to the identity of the next in line, but it does so without revealing who that heir is. This is the critical step. The security of this commitment rests on the one-way nature of the hash function. Modern cryptographic hashes like SHA-256 are considered post-quantum safe; while Grover's algorithm provides a theoretical speedup for finding preimages, simply using a 256-bit hash provides an effective 128 bits of post-quantum security, a level of strength that remains far beyond the reach of any feasible attack. [Bernstein & Lange 2017; Augot et al. 2015] The line of succession is therefore sealed with quantum-resistant cryptography from the very beginning.

Recovery and Invalidation

Now, consider the surprise attack. An adversary with a quantum computer breaks the key of the reigning monarch (the current signing key). They can now issue fraudulent decrees in the monarch's name — forged interaction events.

However, the legitimate controller, who is expected to monitor their own identity's history via a local "watcher," will detect this forgery. [Smith 2024] Upon detection, the controller can initiate a planned and orderly succession. They publish a formal rotation event. This event does two things:

1. It reveals the public key of the heir apparent (the next rotation key), which was previously hidden.
2. It is signed by the corresponding private key of that heir, proving they are the legitimate successor.

Anyone can verify this transfer of power. They simply take the newly revealed public key, hash it, and confirm that the resulting digest matches the "royal seal" that was published in the previous key event. The attacker cannot perform this rotation because they do not possess the private rotation key and therefore cannot produce a valid signature from the rightful heir. They are locked out of the line of succession.

Once the legitimate rotation event is published and witnessed, it invalidates all fraudulent events signed by the compromised key. The coup is thwarted, and the identity is secured under a new ruler. And because KERI is cryptographically agile, this new ruler can be a key pair based on one of the new, NIST-standardized post-quantum algorithms. [Smith 2024]

The genius of this design is its timing: commitment precede exposure. The commitment to the next key is made far in advance, when the system is secure, using a quantum-safe primitive (the hash). The quantum-vulnerable public rotation key is only revealed at the exact moment it is used, after which authority has already passed to a new, secret successor. The attacker is always one step behind. This makes KERI’s chain of control authority fundamentally resilient, not just resistant, to quantum attack.

Securing the Conversation: Addressing "Capture Now, Decrypt Later"

While pre-rotation secures the control of an identity, it does not address the second front of the quantum war: the "Harvest Now, Decrypt Later" attack on confidentiality. This threat targets not the signatures that prove identity, but the encrypted conversations between identities.

The weak point in modern secure communication is not the symmetric encryption itself. Algorithms like AES-256, used for encrypting the bulk of data, are considered relatively quantum-safe. [Palo Alto Networks 2025; NIST 2024; Bernstein & Lange 2017] The vulnerability lies in the "handshake" — the key exchange protocol, typically based on Diffie-Hellman (DH), that two parties use to agree on a shared symmetric key at the start of a session. This exchange relies on quantum-vulnerable asymmetric key pairs. An adversary can record this public key exchange today, store it, and use a future quantum computer to solve the underlying math, derive the shared session key, and decrypt the entire conversation retroactively. [NIST 2024; Entrust 2023]

KERI's architecture provides a powerful advantage here. KERI is a protocol for managing identity, not for encrypting communications. This deliberate separation of concerns is a key strength. It allows KERI to provide a stable, post-quantum-secure root of trust for identity, while allowing the application layer above it to adopt the most appropriate and up-to-date solutions for ensuring confidentiality. For systems built on KERI, two pragmatic, quantum-safe solutions are available.

Solution 1: Out-of-Band Key Exchange (No PQC Required)

The most straightforward way to defeat an HNDL attack on a key exchange is to avoid a public, asymmetric key exchange altogether. Two parties can establish a shared secret — a "salt" — through an out-of-band (OOB) channel, such as during an in-person meeting or by exchanging a physical token. [Entrust 2023] This shared secret can then be used with a deterministic key derivation function to generate any number of symmetric encryption keys for secure communication. Because no quantum-vulnerable public-key cryptography is used to establish the secret, there is nothing for an HNDL adversary to capture and later decrypt. This approach is particularly practical because many highly secure systems already require some form of OOB step to bootstrap trust and prevent man-in-the-middle attacks. [NIST 2017; Sethi, Sarikiya & Garcia-Carillo 2025]

Solution 2: Hybrid Key Encapsulation (The Pragmatic Path)

For the vast majority of online interactions where an OOB exchange is not feasible, a hybrid approach has emerged as the clear industry standard. This method combines a well-established classical key exchange algorithm (like Elliptic Curve Diffie-Hellman using

the X25519 curve) with one of the new post-quantum key encapsulation mechanisms (KEMs), such as the NIST-standardized ML-KEM. [Moody et al. 2024]

The final shared secret key is derived from the outputs of both algorithms. This "belt and suspenders" approach provides a robust defense against uncertainty.

- If the new PQC algorithm is one day found to have an unforeseen flaw, the connection remains secure thanks to the classical algorithm.
- If a quantum computer breaks the classical algorithm, the connection remains secure thanks to the PQC algorithm.

This hybrid model is not merely theoretical; it is already being deployed in the wild as the most responsible path forward. OpenSSH, the software that secures countless remote connections across the internet, began deploying a hybrid PQC key exchange by default in version 9.0, released in April 2022. [OpenSSH Project 2022] IETF has formally documented the approach [Friedl, Mojzis & Josefsson 2025], and GitHub recently adopted it as well. [Carlson & Blau 2025] This implementation combines Streamlined NTRU Prime, a PQC algorithm, with the classical X25519 algorithm. The fact that foundational pieces of internet infrastructure has adopted this model is a powerful validation of its security and practicality.

This approach effectively de-risks the transition to post-quantum cryptography. The new NIST-selected algorithms are promising, but they have not yet withstood the decades of intense public cryptanalysis that RSA and ECC have. The hybrid model provides a crucial safety net, ensuring that the early adoption of PQC to defend against future threats does not inadvertently introduce new risks from the novel algorithms themselves. For systems using KERI for identity, adopting a battle-tested, hybrid-capable communication protocol like the latest version of OpenSSH is a direct and effective way to secure the channel against HNDL attacks.

Conclusion: Crypto-Agility as the Ultimate Defense

The history of cryptography is a story of continuous evolution, punctuated by occasional revolutions. The transition to a post-quantum world is the most significant of these revolutions in a generation. In such a dynamic and uncertain landscape, the ultimate defense is not a premature bet on a single algorithm, but an architecture built for adaptation. KERI's true quantum-readiness lies in its foundational cryptographic agility.

KERI was designed from the outset to treat specific cryptographic algorithms as pluggable components, not as immutable dependencies. The protocol itself is an abstract state machine for managing keys; the signature and hashing schemes are simply the tools it uses. This means that as new, better tools become available, they can be incorporated with minimal effort. A proof-of-concept that integrated one of the NIST PQC finalist algorithms

from the Open Quantum Safe (OQS) library into keripy, KERI's reference implementation in Python, took only a couple of hours to complete. [Personal communication with Sam Smith, Oct. 7, 2025] This is not a happy accident; it is the result of a deliberate design philosophy that prioritizes architectural flexibility over algorithmic specificity.

This approach allows KERI to avoid the twin perils of a premature switch to PQC: the significant performance overhead of larger keys and signatures, and the security risk of relying on algorithms that have not yet been fully "hardened" by years of rigorous analysis.[11] Instead, it provides a multi-layered defense that is effective today and prepared for tomorrow:

1. **For Control**: It uses quantum-safe hash functions — a mature and trusted technology — to protect the chain of authority via its pre-rotation mechanism, making identity control resilient and recoverable even if current signing keys are broken.
2. **For Confidentiality**: Its modular separation of identity and communication allows applications to seamlessly integrate the industry-standard solution for HNDL attacks: hybrid, quantum-safe key exchange mechanisms.
3. **For the Future**: Its innate crypto-agility ensures that as the new NIST standards mature and gain widespread adoption, they can be integrated as first-class citizens within the KERI ecosystem.

KERI, therefore, offers a practical and secure bridge from the classical cryptographic world to the post-quantum future. It uses the best of the old world (hardened hashes) to protect against the threats of the new, while providing a clear and low-friction path to adopt the next generation of cryptographic standards as they become ready. It is an architecture designed not just to survive the quantum transition, but to thrive in it.

Works Cited

Augot, D., Batina, L., Bernstein, D., Bos, J., Buchmann, J., Castryck, W., Dunkelman, O., Güneysu, T., Gueron, S., Hülsing, A., Lange, T., Mohamed, M. S. E., Rechberger, C., Schwabe, P., Sendrier, N., Vercauteren, F., and Yang, B.-Y.. 2015. *Initial Recommendations of Long-Term Secure Post-Quantum Systems.* PQCRYPTO EU Horizon 2020. https://pqcrypto.eu.org/docs/initial-recommendations.pdf

Bernstein D., and Lange T. 2017. *Post-quantum cryptography: Dealing with the fallout of physics success.* IACR Cryptology ePrint Archive 2017/314. https://eprint.iacr.org/2017/314

Carlson, B., and Blau, T. 2025. *Post-quantum security for SSH access on GitHub.* https://t.ly/9VdOl

Cellcrypt. 2024. *Store Now, Decrypt Later (SNDL) Threats.* https://bit.ly/43pyXVe

Curtiss-Wright Defense Solutions. 2025. *Harvest Now, Decrypt Later Strategy: Why Aerospace & Defense Must Lead in Post-Quantum Cryptography.* https://t.ly/GV_Vw

Department of Homeland Security (DHS). 2025. *Post-Quantum Cryptography Resources.* https://www.dhs.gov/quantum

Entrust. 2023. *Harvest Now, Decrypt Later – Fact or Fiction?* https://www.entrust.com/blog/2023/11/harvest-now-decrypt-later-fact-or-fiction

European Union Agency for Cybersecurity (ENISA). 2024a. *Cryptographic Products and Services Market Analysis.* https://bit.ly/4oMeYZt

European Union Agency for Cybersecurity (ENISA). 2024b. *Report on the State of Cybersecurity in the Union (Condensed Version).* https://bit.ly/3WHwodw

GSMA. 2025. *Post-Quantum Government Initiatives by Country and Region.* https://bit.ly/3KXPlGj

HashiCorp. 2023. *Harvest Now, Decrypt Later: Why Today's Encrypted Data Isn't Safe Forever.* https://bit.ly/4hfMVPg

Friedl, M., Mojzis, J., & Josefsson, S. 2025. *Secure Shell (SSH) Key Exchange Method Using Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: sntrup761x25519-sha512.* Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/draft-ietf-sshm-ntruprime-ssh-06

Moody D., Perlner R., Regenscheid A., Robinson A., Cooper D. 2024. *Transition to Post-Quantum Cryptography Standards.* NIST IR 8547 ipd. https://doi.org/10.6028/NIST.IR.8547.ipd

National Institute of Standards and Technology (NIST). 2017. *Digital Identity Guidelines: Authentication and Lifecycle* (NIST Special Publication 800-63B). https://pages.nist.gov/800-63-3/sp800-63b.html

National Institute of Standards and Technology (NIST). 2024. *Post-Quantum Cryptography Project: Timeline and Standards* (FIPS 203–205). https://csrc.nist.gov/projects/post-quantum-cryptography

OpenSSH Project. 2022. *Release 9.0 Notes.* https://www.openssh.com/txt/release-9.0

Palo Alto Networks. 2025. *What Is Quantum Computing's Threat to Cybersecurity?* https://bit.ly/48DamzY

PQShield. 2025. *South Korea Announces Winners of KpqC Competition.* https://pqshield.com/south-korea-announces-winners-of-kpqc-competition

Sethi, M., Sarikaya, B., & Garcia-Carrillo, D. 2025. *Terminology and processes for initial security setup of IoT devices*. Internet Research Task Force (IRTF). https://datatracker.ietf.org/doc/draft-irtf-t2trg-security-setup-iot-devices/05/

Smith, S. 2024. "Key Event Receipt Infrastructure (KERI): Specification." Draft v0.9. Trust Over IP Foundation. https://trustoverip.github.io/kswg-keri-specification/

Telecommunication Engineering Centre (TEC). 2025. *Migration to Post-Quantum Cryptography: Technical Report* (TEC 910018:2025). https://bit.ly/3KUYRKo

White House. 2022. *National Security Memorandum 10 (NSM-10): Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems.* https://www.congress.gov/crs-product/IN11921