H33 Publishes H33-PQ Verified, a Continuous, Independently Verifiable Post-Quantum Attestation Standard

H33-PQ Verified is a post-quantum verification standard that enables independently verifiable evidence, portable audit artifacts, and cryptographic proofs

H33 Logo

RIVERVIEW, FL, UNITED STATES, June 10, 2026 /EINPresswire.com/ -- H33.ai, Inc. ("H33") today announced the publication of **H33-PQ Verified**, a continuous post-quantum attestation standard designed to help organizations demonstrate cryptographic readiness, governance maturity, privacy protections, evidence preservation, and independent verification capabilities through portable, machine-verifiable evidence.

> H33-PQ-Verify is a live proof system that allows organizations to prove they are protecting their clients, and allows those clients to independently verify that protection”
> *-Eric Beans - CEO - H33.ai, Inc.*

The standard is available immediately at:

https://h33.ai/standards/post-quantum-verified/

H33-PQ Verified is not a cybersecurity badge. It is a continuously updated signal that an organization can prove its cryptographic posture, authority chain, evidence trail, privacy controls, and verification capabilities without requiring trust in the organization making the claim.

Why This Matters

Much of the cryptography protecting the world's data, financial systems, communications, identities, and critical infrastructure was never designed to withstand large-scale quantum computing.

Governments, standards bodies, and technology leaders have spent years preparing for that reality. In 2024, NIST finalized its first post-quantum cryptography standards. Major technology providers have already begun establishing migration timelines. Google has publicly stated that

organizations should complete migration away from vulnerable cryptographic systems by 2029.

The challenge is that most organizations still do not know where they stand.

Boards ask whether the company is prepared.

Customers ask whether their data will remain protected.

Regulators ask for evidence.

Insurers ask about cryptographic risk.

Procurement teams ask vendors whether they are post-quantum ready.

The answers are typically delivered through questionnaires, spreadsheets, screenshots, and self-attestations that are difficult to verify and often outdated the moment they are produced.

Consumers, enterprises, regulators, insurers, and investors increasingly need a way to distinguish between organizations that are actively preparing for the post-quantum transition and those that are not.

H33-PQ Verified was created to solve that problem.

H33.ai - The World's First Complete Quantum-Proof Security Platform

Cachee.ai — Autonomous Predictive Caching Platform by H33.ai, Inc.

The standard provides a continuous, independently verifiable signal of an organization's cryptographic readiness, governance posture, privacy protections, evidence preservation capabilities, and verification maturity.

Organizations that invest in protecting their customers, data, and operations should be able to prove it.

Organizations that do not should not be able to hide behind marketing claims.

At the center of the standard is a simple principle:

Large systems produce large amounts of evidence, but verification should remain portable.

H33-PQ Verified evaluates whether organizations can reduce complex cryptographic, governance, privacy, and verification states into independently verifiable artifacts that remain usable years later.

The objective is simple:

Prove what is true. Make the proof portable. Allow anyone to verify it independently.

What H33-PQ Verified Solves

For Security Teams

* Eliminate annual cryptography readiness spreadsheets.
* Continuously monitor post-quantum migration progress.
* Detect cryptographic regressions before audits.
* Demonstrate NIST-aligned readiness through machine-verifiable evidence.

For Procurement Teams

* Compare vendors using a common evaluation framework.
* Verify cryptographic claims without relying on self-attestations.
* Reduce vendor review cycles.
* Establish objective cryptographic requirements in RFPs and onboarding processes.

For Boards and Executives

* Gain a live signal of organizational cryptographic readiness.
* Track progress toward post-quantum migration goals.
* Reduce exposure to long-horizon cryptographic risk.
* Replace point-in-time reporting with continuous verification.

For Auditors and Assessors

* Review portable evidence instead of screenshots and spreadsheets.
* Independently verify findings without relying on the issuer.
* Reconstruct cryptographic posture years later.
* Validate remediation activities over time.

For Insurers

* Quantify cryptographic controls using objective evidence.
* Monitor improvement or deterioration between policy periods.
* Reduce reliance on self-reported questionnaires.
* Support underwriting and claims investigations using independently verifiable artifacts.

For Regulators

* Assess cryptographic readiness using a common framework.
* Verify evidence without direct access to production systems.
* Evaluate migration progress consistently across organizations.
* Reduce dependence on vendor-specific reporting formats.

For Customers

* Evaluate supplier cryptographic readiness.
* Verify security claims independently.
* Reduce vendor lock-in risk.
* Preserve confidence during technology migrations.
* Confirm that critical evidence remains verifiable even when systems change.

The Five Pillars

H33-PQ Verified evaluates participating organizations across five pillars. Each pillar represents a measurable property and a corresponding operational outcome.

H33-PQ Verified evaluates organizations across five pillars:

Cryptography — Organizations must demonstrate the deployment and use of quantum-resistant cryptography across signing, verification, key exchange, privacy-preserving computation, and proof generation. The objective is to ensure security systems remain resilient through future cryptographic transitions.

Evidence — Organizations must produce portable evidence artifacts that preserve important decisions, events, and outcomes in a form that remains independently verifiable over time. The objective is to ensure audit records remain usable for years rather than being trapped inside a specific vendor, platform, or database.

Governance — Organizations must maintain verifiable records of authority, approvals, policy decisions, and accountability. The objective is to ensure critical decisions remain explainable and traceable to the individuals or systems authorized to make them.

Privacy — Organizations must demonstrate the ability to protect sensitive information while still

supporting computation, analysis, compliance, and verification activities. The objective is to ensure sensitive data remains protected during processing rather than only at rest.

Verification — Organizations must enable independent validation of results, evidence, and outcomes by third parties. The objective is to ensure multiple reviewers can reach the same conclusion without relying on trust in the original issuer.

Organizations satisfying the criteria earn **H33-PQ Verified** status.

The attestation itself is a cryptographic artifact—not a logo, marketing claim, or self-assertion.

What Gets Evaluated

H33-PQ Verified examines a broad set of operational artifacts and controls, including:

* TLS configurations
* Certificate inventories
* Signing systems
* Key management systems
* Software Bills of Materials (SBOMs)
* Cryptographic libraries
* Evidence systems
* Governance and authority records
* Verification artifacts
* Post-quantum migration status

Every measurement produces evidence.

Every evidence artifact can be independently verified.

Every result can be reproduced by an independent third party.

Separating the Standard From the Runtime

H33-PQ Verified is published as an open standard.

H33's own **HATS (H33 AI Trust Standard)** serves as the reference implementation, but the standard itself is deliberately implementation-neutral.

The standard defines what must be proven. HATS is one implementation. Any implementation that satisfies the verification requirements can participate.

This distinction is intentional.

The market often collapses the difference between standards and products.

When the same vendor defines the rules, performs the evaluation, hosts the verifier, and issues the badge, customers are ultimately left trusting the vendor.

H33-PQ Verified separates those concerns.

The standard defines the requirements.

Implementations provide the evidence.

Verification remains independent.

A Live Signal, Not an Annual Snapshot

H33-PQ Verified operates as a continuous lifecycle.

Assessed

An organization has completed an evaluation and produced verifiable evidence.

Verified

The organization currently satisfies all five pillars under active evaluation.

Certified

The organization has maintained Verified status across the required validation period and demonstrated sustained compliance with the standard.

Each state transition produces portable cryptographic evidence that can be independently validated without contacting H33 or the participating organization.

Verify It Yourself

Any third party can install the open **h33-verify** command-line tool and independently replay an attestation.

Verification does not require trust in H33, the issuing organization, or any proprietary service.

The same evidence should produce the same conclusion regardless of who performs the verification.

The goal is simple:

Independent parties should reach the same answer.**

H33 Has Applied the Standard to Itself

H33 is both the publisher of the standard and the first participant.

The H33 self-attestation includes downloadable evidence bundles for every pillar and can be independently verified using the same tooling available to all participants.

A standard whose publisher refuses to measure itself against its own requirements is a proposal.

H33-PQ Verified is published and operating.

Why It Matters

The transition to post-quantum cryptography is not simply a technology migration.

It is a trust migration.

Organizations increasingly need to answer questions such as:

* How do we prove cryptographic readiness without relying on vendor claims?
* How do we verify security posture continuously rather than annually?
* How do we preserve evidence when systems change?
* How do we demonstrate governance without exposing sensitive information?
* How do we reward organizations that proactively protect customer data?
* How do we ensure verification survives the lifespan of any single product, cloud provider, database, blockchain, or vendor?

H33-PQ Verified was designed to answer those questions through independently verifiable evidence rather than trust alone.

Availability

Standard: https://h33.ai/standards/post-quantum-verified/

H33 Self-Attestation:** https://h33.ai/standards/post-quantum-verified/h33-self-attestation/

Reference Runtime (HATS): https://h33.ai/hats/

Open Verifier: https://h33.ai/verifier-cli/

Standards Index: https://h33.ai/standards/

About H33

H33.ai builds infrastructure for portable evidence, portable authority, privacy-preserving computation, independent verification, and post-quantum security.

Its technologies are designed to enable independently verifiable outcomes across artificial intelligence, cybersecurity, regulated industries, governance, enterprise software, and digital trust systems.

H33 is the publisher of the H33-PQ Verified standard and maintains a growing patent portfolio focused on evidence preservation, authority preservation, post-quantum security, privacy-preserving computation, and independent verification.

For more information, visit https://h33.ai.

Media Contact

Eric Beans
CEO, H33.ai
[eb@h33.ai)
https://h33.ai

Eric D Beans
H33.ai, Inc.
+1 813-464-0945
email us here
Visit us on social media:
LinkedIn
YouTube
X
