EINPRESSWIRE

H33 Launches HATS: A New Standard for Proving How Sensitive Data Is Handled — Continuously

And whether it was ever exposed—across AI systems, financial infrastructure, and enterprise environments.

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

RIVERVIEW, FL, UNITED STATES, April 27, 2026 /EINPresswire.com/ -- H33 today announced the release of HATS (H33 Attestation Trust Standard), a cryptographic attestation framework designed to continuously prove how sensitive data is handled-and whether that data was ever exposed-across artificial intelligence systems, financial infrastructure, and enterprise environments.

HATS introduces what H33 describes as a new category of system assurance: verifiable decision infrastructure. In this model, systems do not rely solely on logs, policies, or periodic audits to describe behavior. Instead, they produce independent, mathematical proof of how decisions were executed and whether sensitive data remained protected throughout processing.

Background

> Trust is expensive. We're replacing trust in AI and compliance with real-time mathematical proof."
>
> *Eric Beans*

Modern software systems increasingly rely on distributed architectures, third-party services, and automated decision-making. Sensitive data flows through AI pipelines, APIs, cloud platforms, and partner ecosystems at a scale and velocity that make traditional audit and reporting mechanisms difficult to apply in real time.

Organizations typically rely on a combination of:

-system logs

-internal policies
-external audits
-compliance certifications to demonstrate that sensitive data is handled appropriately.

These mechanisms provide documentation and intent, but they do not provide independent proof of what actually occurred during execution. In particular, they do not establish whether sensitive data was exposed at any point in a system's operation. As systems become more complex and more automated, the distinction between reported behavior and verifiable behavior becomes more significant, particularly in regulated industries and environments where data exposure carries financial, operational, or legal consequences.

The HATS Standard:

HATS is designed to address this gap by generating cryptographic attestations tied directly to system execution. Rather than attempting to control or restrict how systems operate, HATS focuses on producing verifiable evidence of behavior. For each decision or operation, the system generates a proof that can be independently evaluated.

This proof is intended to establish:

-what data was involved (without exposing the data itself)
-how the data was processed
-whether the data remained protected or was exposed
-which policies were applied during execution
-the resulting output

Because sensitive data is not exposed in plaintext during processing, the system is designed to maintain protection even when data is handled by automated workflows or artificial intelligence systems. The resulting attestations are continuous, cryptographic, and independently verifiable.

AI Agent Attestation

As organizations deploy autonomous AI agents — systems that make decisions, access data, and invoke external services without direct human oversight - the gap between system behavior and verifiable behavior becomes acute.

AI agents present a distinct attestation challenge. Unlike traditional software, agents may:

- access sensitive data dynamically based on context
- make decisions that affect downstream systems and workflows
- invoke external APIs, tools, or other agents in multi-step chains

- operate across organizational boundaries with delegated authority

In these environments, after-the-fact logging is insufficient. Logs describe what an agent reported doing. They do not independently prove what actually occurred, what data was accessed, or whether access policies were enforced during execution.

HATS addresses this through agent-level attestation. Each agent action - data access, computation, delegation to another agent, external API call - generates a cryptographic attestation that is:

- bound to the specific agent identity and its delegated authority
- chained to the previous attestation in the execution sequence
- independently verifiable without access to the agent, its host system, or the data it processed

In multi-agent pipelines, HATS produces a provenance chain: Agent A attests its output, Agent B verifies A's attestation before proceeding, and Agent C verifies B's attestation before delivering results. Each handoff is cryptographically bound. If any agent in the chain is compromised, tampers with data, or exceeds its delegated authority, the chain breaks at the point of deviation.

This model is designed to allow organizations to deploy AI agents in sensitive environments - healthcare, financial services, legal, government -
with continuous, verifiable proof of agent behavior rather than trust in agent self-reporting.

Technical Approach

HATS combines several cryptographic components to produce a verifiable attestation:
-H33-74 attestations — fixed-size post-quantum proofs that bind execution context, computation, and output into a compact record
-Zero-knowledge STARK proofs — used to validate that computations were executed correctly without exposing underlying data
-Post-quantum digital signatures (ML-DSA / Dilithium) — applied to ensure long-term integrity of the attestation
-Each attestation is generated as a self-contained object that can be verified independently. Verification does not require access to H33 systems, internal APIs, or the underlying data used in the computation.
-According to H33, this structure allows third parties—including auditors, regulators, insurers, and business partners—to verify system behavior without relying on the system operator or the platform provider.

Independent Verification

A core feature of the HATS model is that verification is not dependent on trust in the originating system.

Each attestation contains sufficient information to allow independent validation of:
-computation integrity
-policy adherence
-data handling state

This is intended to enable external parties to evaluate system behavior directly, rather than relying on reported summaries or internal controls.
In this model, verification shifts from:

“trust what is reported”
to:
“verify what can be proven”

Potential Applications

HATS is designed for use in environments where sensitive data is processed and where verifiable assurance of data handling is required.

These environments may include:

-AI systems, where organizations seek to demonstrate how training data, prompts, and inference pipelines handle sensitive information financial infrastructure, where transaction processing and risk models require auditability and integrity
-cyber insurance workflows, where insurers evaluate system state during underwriting, renewal, and claims enterprise systems, where internal controls and access policies must be continuously validated
-regulated environments, where compliance obligations require demonstrable evidence of system behavior

In these contexts, HATS is intended to provide a mechanism for producing verifiable evidence that complements existing controls and reporting processes.

Operational Model

HATS operates alongside existing infrastructure and integrates with systems such as identity providers, endpoint protection platforms, cloud services, and access management tools. The framework is designed to observe system state and execution behavior without requiring:

-access to underlying sensitive data
-changes to core application logic
-additional agents or infrastructure components

Attestations are generated continuously and anchored to specific time windows, allowing system state to be referenced at the moment of execution rather than reconstructed after the fact.

If a system deviates from expected behavior- such as processing sensitive data in a way that violates defined controls—the deviation is captured and reflected in the attestation.

Implications

H33 describes HATS as a shift from documentation-based assurance to proof-based assurance. In traditional models, organizations demonstrate compliance and security through documentation, certifications, and retrospective analysis. In the HATS model, system behavior is evaluated through cryptographic proof generated during execution. This distinction becomes more relevant as organizations deploy automated systems in environments where:
decisions must be auditable data exposure carries measurable risk system behavior must be validated across organizational boundaries

Availability

HATS is available as part of the H33 platform and is designed to integrate with existing systems without requiring infrastructure changes or access to sensitive data.

The HATS standard is publicly available at:

https://h33.ai/standards/hats

Live demonstrations are available at:

https://h33.ai/hats/demo

H33 noted that HATS provides verifiable evidence of system behavior and does not make underwriting, pricing, or claims decisions.

About H33

H33 is a post-quantum cryptography and encrypted compute platform focused on enabling systems to process sensitive data without exposing it. The platform integrates cryptographic primitives, zero-knowledge proofs, and post-quantum signatures to support secure and verifiable computation.
With the introduction of HATS, H33 extends this model to include continuous, independently

verifiable attestation of how data is handled during system execution.

Six patents are pending, covering more than 250 claims related to encrypted computation, attestation, and verification.

Learn more at https://h33.ai

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