VERIFIED PRESENCE PROTOCOL™ (VPP™)

Manifesto

Status: Foundational Statement
Document Type: Public Reference
Version: 1.0

Digital systems increasingly mediate actions with real-world consequences.

Yet most systems still lack a fundamental capability:

the ability to establish explicit, accountable human authorization before an action occurs.

Verified Presence is not concerned with who acted.

It is concerned with who explicitly authorized an action — and when — before execution.

The Trust Gap

Modern digital environments verify identity, credentials, and access. They generate logs, permissions, and audit trails. But these mechanisms largely operate after the fact.

They do not reliably establish whether a real human was consciously present and accountable at the moment an action was authorized. As delegation increases — to software, agents, and AI-mediated systems — this gap becomes a systemic risk.

Presence Is Not Identity

Verified Presence does not seek to identify individuals. It seeks to establish accountable human presence at a specific moment in time, independent of identity systems, platforms, or applications.

- **Presence is temporal.**
- **Identity is persistent.**

Conflating the two weakens accountability and erodes trust

Authorization Before Execution

Verified Presence is anchored in a simple principle: **No delegated or mediated action should occur without explicit human authorization beforehand.**
This authorization must be:

- intentional
- time-bound
- verifiable
- auditable
- and independent of content, outcomes, or execution mechanisms

Accountability cannot be reconstructed solely from logs or inferred from access rights.It must be explicitly established before execution.

Institutional Integrity

Verified Presence is designed for environments where trust is non-negotiable.

It prioritizes:

- neutrality over optimization
- governance over convenience
- accountability over automation

Its purpose is not speed or scale — but legitimacy.

The Role of VPP™

The Verified Presence Protocol™ defines institutional semantics and governance expectations — not software, applications, or enforcement mechanisms.

It exists to ensure that digital actions remain anchored to real, accountable human authorization — even as systems become increasingly autonomous.

A Protocol, Not a Product

The Verified Presence Protocol™ (VPP™) is not a platform, application, or service.

It is a protocol-level reference that defines:

- institutional semantics
- governance expectations
- and accountability boundaries

VPP™ does not prescribe implementations, architectures, or technologies. It provides a neutral foundation upon which institutions may establish verifiable human authorization across systems, jurisdictions, and execution environments.

AI and Delegated Systems

As AI systems increasingly mediate, recommend, or initiate actions, traditional notions of digital trust become insufficient.

Verified Presence does not seek to control AI systems.

It establishes human accountability before AI-mediated execution, without capturing content, decision logic, or personal data.

Verified Presence Protocol™

A governed trust protocol for accountable execution.