VERIFIED PRESENCE PROTOCOL™ (VPP™)

Protocol Definition v1.0

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

---

1. Purpose and Scope

The **Verified Presence Protocol™ (VPP™)** defines a protocol-level trust layer for establishing verified human presence, explicit authorization, and auditable responsibility in digital interactions prior to execution.

The protocol is designed to address a structural gap in modern digital systems:
while identity, authentication, and security mechanisms exist, responsibility attribution and authorization intent remain largely inferred or post-hoc.

VPP™ provides a standardized framework to ensure that actions performed directly or through AI-mediated systems can be reliably traced to an authorized human actor, within defined temporal and contextual boundaries.

2. Problem Statement

Digital environments increasingly rely on assumptions of presence based on appearance, credentials, or post-event analysis.

However:

- Visual and auditory cues are no longer reliable
- Automation and delegation obscure responsibility
- Detection-based approaches are reactive
- Identity alone does not guarantee intent or presence

This creates systemic risk in environments where accountability is foundational, including finance, compliance, legal, media, healthcare, and governance.

VPP™ addresses this risk by establishing presence and authorization before actions occur, rather than attempting to validate authenticity after the fact.

3. Design Principles

The Verified Presence Protocol™ is built upon the following foundational principles:

3.1 Explicit Authorization

No critical action is considered valid under VPP™ without an intentional, affirmative authorization event from a responsible human actor.

3.2 Presence Over Appearance

Trust is established through verifiable presence sessions, not visual resemblance or content analysis.

3.3 Temporal Boundaries

All presence and authorization states are session-based and time-limited by design.

3.4 Auditability Without Surveillance

The protocol generates event records sufficient for audit and accountability without capturing or storing content.

3.5 Technology Neutrality

VPP™ does not mandate specific authentication methods, biometric systems, hardware, or platforms.

3.6 Institutional Compatibility

The protocol is designed to align with regulatory, legal, and compliance frameworks across jurisdictions.

4. Core Concepts and Definitions

4.1 Authorized Human Actor

A natural person who holds responsibility and authority to approve actions within a defined context.

4.2 Presence Session

A time-bound, context-specific state indicating active participation by an authorized human actor.

4.3 Authorization Event

An explicit, intentional approval by an authorized human actor permitting a specific action or class of actions.

4.4 Delegation

The controlled granting of limited authority to an AI system or agent to act within predefined scope and duration.

4.5 Audit Record

A non-content-based record capturing presence sessions, authorization events, delegation states, and temporal boundaries.

4.6 Trust Mark

A visual or machine-readable indicator signaling that an interaction or output was produced under a valid VPP™ authorization regime.

5. Protocol Architecture (Conceptual)

The Verified Presence Protocol™ operates as an overlay trust layer beneath applications and platforms.

It does not replace identity systems, authentication mechanisms, or security controls.
Instead, it complements them by introducing an additional layer focused on responsibility attribution.

High-Level Components:

- Presence Session Manager
- Authorization Event Recorder
- Delegation Control Logic
- Audit Record Generator
- Trust Mark Issuance Interface

Each component may be implemented independently, provided protocol semantics are preserved.

6. High-Level Protocol Flow

Step 1: Presence Session Initiation

A presence session is established for an authorized human actor within a defined context and time window.

Step 2: Explicit Authorization

The actor performs an intentional authorization event approving one or more actions.

Step 3: Optional Delegation

Authorization may include limited delegation to AI-mediated systems, bounded by scope and duration.

Step 4: Action Execution

Approved actions are executed under the active presence session.

Step 5: Audit Record Generation

Non-content-based audit records are generated, capturing authorization provenance.

Step 6: Trust Mark Association

Outputs may carry a VPP™ Trust Mark indicating verified authorization and responsibility.

7. What the Protocol Does Not Do

VPP™ intentionally avoids the following:

- Content authenticity verification
- Deepfake detection
- Biometric enforcement
- Identity provisioning
- Surveillance or recording of communications
- Platform-specific enforcement

These exclusions preserve neutrality, scalability, and institutional trust.

8. Applicability Domains

The Verified Presence Protocol™ is applicable to any environment requiring reliable attribution of responsibility, including but not limited to:

- Banking and financial services
- Audit, compliance, and assurance
- Legal and evidentiary contexts
- Government and public administration
- Media and broadcast communication
- Healthcare and telemedicine
- AI agents, avatars, and autonomous systems
- Security, defense, and diplomatic environments

9. Governance and Stewardship

VPP™ is governed through a stewardship model that ensures:

- protocol integrity
- version control
- certification consistency
- institutional neutrality

Compliance with the protocol is determined by adherence to defined semantics and governance rules, not by implementation ownership.

10. Versioning and Evolution

This document represents **Protocol Definition v1.0**.

Future versions may introduce:

- expanded delegation semantics
- enhanced audit interoperability
- standardized trust mark schemas
- regulatory alignment extensions

Backward compatibility and institutional continuity are core considerations in all future revisions.

11. Status

The Verified Presence Protocol™ is currently in the definition and institutional anchoring phase.

12. Conclusion

The Verified Presence Protocol™ establishes a foundational trust layer for a digital environment where presence can no longer be assumed and responsibility must be explicit.

By shifting trust from appearance to authorization, and from inference to verifiable accountability, VPP™ enables institutions to operate confidently in an AI-mediated world.

Verified Presence Protocol™ (VPP™)
A protocol for verified presence, explicit authorization, and auditable responsibility.