



HOLogram

Human Obfuscation Layer

AI sees a reflection, never the original



Whitepaper

Version 1.0 (March 2026) - BaffiSan

info@hologramprotocol.org

www.hologramprotocol.org

Index

Abstract	1
1. Introduction	1
2. The Problem	1
3. Architecture	1
4. Operation	2
5. Security	2
6. Compliance	2
7. Ecosystem & HOLoToken	3
8. Hashing / Notarization	3
9. Conclusion	3

Abstract

Behavioral signals generated during digital interaction—typing rhythm, pointer trajectories, scroll dynamics—enable user identification even in the absence of cookies, logins, or traditional fingerprinting. HOLogram introduces a Human Obfuscation Layer: a local system that obfuscates, normalizes, and reduces the granularity of such signals before they reach page scripts or AI systems, preserving natural usability while reducing identifiability. The protocol operates entirely locally, stores no data, does not manipulate user intent, and is conceived as an open standard supported by a non financial reputation system (HOLoToken) based on Proof of Contribution.

Its objective: to recognize the right *not* to be identified by one's own behavior.

1. Introduction

Behavioral biometrics constitute a unique, stable, and difficult to alter signature that emerges from how we type, move the pointer, and scroll through pages. Existing solutions (VPNs, private mode, device anti fingerprinting) do not shield the dynamics of human gestures. HOLogram inserts itself between user and page as a behavioral protection layer, reducing the fidelity of exposed signals without altering content or intent. It is human centric, *local only*, transparent (minimal HUD), and open to implementations and variants.

2. The Problem

High frequency events (keyboard, pointer, scroll) are silently collected via scripts and, when combined with models, enable re identification, cross site correlation, and undesired inferences (e.g., hesitation, stress). The user remains exposed because their behavioral signature is intrinsic and reappears in every session. What is needed is an intermediate layer that transforms the form of behavior while preserving the function of interaction.

3. Architecture

1. **ShadowDOM** Input Vault — isolates input events (keydown/keyup/keypress) and forwards normalized events (input/change) without micro timing.
2. **Pointer & Scroll Normalizer** — applies sampling, quantization, and controlled smoothing to movements and scroll signals, maintaining human plausibility while reducing uniqueness.
3. **Persona Mixer (session consistent)** — assigns each session a synthetic persona with parameters within plausible, partially overlapping ranges, preventing both inter session correlation and obfuscation fingerprinting.
4. **Behavioral Differential Privacy Engine** — applies calibrated noise and stabilization to reduce output sensitivity to micro variations in input (final mathematical barrier).
5. **Behavioral Privacy Budget** — measures and controls how much behavioral information is exposed; triggers escalation (more smoothing/quantization, less frequency) as budget decreases; regenerates gradually (idle/low intensity events) and resets at session reset. Event cost considers type, frequency, geometric complexity, and entropy.

6. **Exposure HUD** — displays protection level, budget status, module activity.

Flow: Input → Vault → Normalizer → Persona Mixer → DP Engine → Privacy Budget → Output projected to the site.

4. Operation

- **Acquisition:** interception of events before the page (no storage).
- **Normalization:** frequency reduction, quantization, smoothing, timing homogenization.
- **Personalization:** synthetic persona consistent within the session, variable across sessions.
- **Protection:** DP Engine + Privacy Budget escalation.
- **Emission:** the page receives plausibly human signals, not the user's real behavioral signature.
- **Closure:** full reset; no state persists.

5. Security

Objectives: reduce identifiability; preserve usability; prevent obfuscation from becoming a fingerprint; zero telemetry; detection resistance.

Threats: page level fingerprinters; cross site correlation; aggressive anti bot systems; targeted adversaries.

Defenses: Vault (removal of micro timings), Normalizer (downsampling, quantization, smoothing), Persona Mixer (session consistent variability within plausible ranges), DP Engine (noise + stabilization), Privacy Budget (exposure control), HUD (transparency).

Limits: does not anonymize network; does not protect against non behavioral fingerprinting; “compatibility profiles” may be required for highly time sensitive apps.

6. Compliance

HOLogram does **not** process personal data: it collects nothing, stores nothing, transmits nothing, and performs no profiling.

It is *local only*, zero retention, non manipulative, and neutral.

The HOLoToken reputation system is non financial (non transferable, non tradable, no economic value) and measures only technical contribution (HRL/HCS), with no link to the identity of the protected user.

Non binding note: the architecture reflects the general principles of major European digital rights regulations without generating processing or legal bases.

7. Ecosystem & HOLOToken

Open protocol with reference implementation, HLP specification, HCT compliance tests, and RFC process. Variants and forks are welcome if transparent and compatible with an HLP version, with the possibility of reintegration via RFC.

HOLOToken (HRL/HCS) assigns badges/roles/permissions based on contributions (code, security, testing, docs, i18n...), with versioned policies, anti gaming measures, and auditability. No economic component.

8. Hashing / Notarization

Each version is distributed with its SHA 256 hash, published on GitHub (commit/tag), IPFS (CID), and optionally via distributed timestamping. Version history stored in HASHES.txt, immutable tags, verifiable chain (v1.0 → hash → CID). Authorship under the pseudonym BaffiSan is attested through hash + public publication + optional commit signing. Verification is open to the community.

9. Conclusion

HOLogram does not alter what the user does, but how the behavior is exposed. It projects a hologram of the real gesture to the web: functional, natural, non identifying. It is a deterministic, AI free, local protocol, designed to evolve as an open standard.

Its mission: **protect behavioral freedom as a digital right.**