

LifeCorp Research

Project VEIL: Protocol Architecture

VEIL-S-25 · Verified Engagement & Impression Layer: placement, policy and reporting boundaries.

Scope and actors

VEIL separates publisher placement requests from browser-owned advertising execution. The design identifies a publisher, a browser mediator, a delivery service, a policy authority and an independent assurance function. The browser enforces the exposure policy; the policy authority determines permitted exposure.

This specification defines an evaluation architecture. Deployment depends on interoperable implementations, an agreed certification process and the resolution of the reporting questions set out below. Managed workforce environments associated with Project Continuity provide a reference for administrative relationships; the specification reports no new cohort statistics or adoption result.

Placement requests and identifiers

A publisher requests a placement by supplying dimensions, a content category and a resource envelope through a standardized browser interface. The mediator checks the request against its execution limits and policy state. Each accepted request receives an opaque identifier scoped to that placement context.

The identifier supports request handling and later settlement review. It carries no direct declaration of individual suppression state. Identifier lifetime, reuse and association across contexts require independent review to prevent a new tracking channel from forming around the replacement interface.

Browser-owned delivery and resource budgets

The mediator owns retrieval, isolated rendering and the decision to suppress a placement. Delivery executes within a restricted environment with limits on computation, memory, network activity and presentation behavior. Failure of a resource check ends that delivery attempt through the defined failure path.

The design aims to replace arbitrary publisher-supplied execution with a bounded service. Native rendering and isolation reduce the opportunities for third-party scripts to inspect unrelated page or device state. Certification would examine the enforcement of the resource envelope across supported devices.

Entitlement policy interface

Certified implementations expose a policy-distribution interface for an authorized administrator. The policy record identifies its authority, validity period, supported service environment and the resident preference levels available under the governing arrangement. The browser applies a user's selected level within that permitted set.

LifeScore, membership status and contribution history can inform the levels offered by an institutional service authority. The architecture leaves the selection among available levels with the resident. Disputes about eligibility or assignment follow the responsible authority's review route, while the browser maintains the current valid policy.

Mediation integrity and bypass

Mediation bypass means client modification that alters a certified implementation's delivery or suppression decisions outside its approved policy interface. This definition describes an integrity boundary spanning both delivery and withholding. The proposed certification profile records detected deviations and the corresponding implementation state.

The protocol proposes a prohibition on bypass as part of maintaining comparable implementations. The competent policy process must determine the scope of that restriction, the treatment of user extensions and the available exception or appeal routes. This specification grants no legislative force to the proposal.

Observable state and side channels

Publisher access to opaque placement references limits direct preference disclosure. Timing, geometry, network behavior and repeated requests may still reveal differences between delivery and suppression. Testing should cover colluding participants and repeated observations across browsing contexts.

Indistinguishability remains an evaluation objective with an explicit threat model. The design should publish which observations an implementation conceals, which it exposes and which depend on device or network conditions. A uniform interface alone supplies insufficient evidence about inference risk.

Measurement, settlement and assurance

Settlement records distinguish a placement request, an attempted retrieval, a render event and a verified view under the relevant measurement definition. A suppressed advertisement receives no verified-view record. Withheld placements must remain separate from impressions used for billing.

Fraud prevention, audit access and privacy constraints create competing evidence requirements. The specification reserves the settlement profile for further evaluation. Independent reviewers require enough information to test implementation claims without assembling cross-site individual histories.

Supporting publications

<https://lifecorp.org/archive/veil-fragmented-attention>

<https://lifecorp.org/archive/continuity-agreement>