

Westridge Assurance Partners

Project VEIL: Independent Technical Assurance

VEIL-A-26 · Technical boundaries, policy authority and unresolved implementation risks.

Engagement and evidence boundary

LifeCorp funded this review of the VEIL research and protocol architecture. Westridge Assurance Partners retained responsibility for its findings. The engagement examined the specification, administrative-policy model and controlled design materials supplied through July 2026.

The review addresses the adequacy of the architecture and its stated controls. Broad browser adoption, comprehensive side-channel resistance and a functioning statutory certification regime lie beyond the evidence supplied. Findings distinguish credible design benefits from claims requiring implementation evidence.

Benefits supported by the design

Browser-owned execution provides a coherent point for enforcing resource budgets and isolating delivery from arbitrary page scripts. Standardized requests can reduce duplicated infrastructure, and scoped opaque identifiers can limit direct disclosure of individual preference state to publishers.

These are substantive advantages over fragmented third-party execution. Their realization depends on implementation quality, identifier handling and a reporting profile that preserves the distinction between an available placement and an advertisement actually viewed.

Suppression-state inference

An opaque identifier conceals an explicit state declaration while leaving timing and rendering observations available. Repeated measurements may reveal stable differences. The assessment requires a published threat model, adversarial testing and an account of residual inference risk across devices.

The settlement design is incomplete. The evidence boundary must distinguish withheld delivery from verified views throughout reporting and billing. Independent assurance needs a testable account of those

records and access arrangements proportionate to its task.

Policy authority and fallback

The browser's enforcement role is clear. The basis on which an administrator assigns available exposure levels needs further institutional review. A valid policy record can carry an instruction that the affected user would otherwise reject.

The bypass prohibition removes user-controlled filtering as a fallback where entitlement policy is set by a third party.

The architecture should establish an effective route to contest that assignment before restricting an existing remedy. Administrative review, emergency exceptions and user control require treatment as operating safeguards rather than implementation preferences.

Certification and market access

Certification can improve confidence in resource enforcement and common reporting. Its cost, renewal burden and treatment of alternative implementations determine which browser vendors can participate. A profile built around incumbent infrastructure may narrow implementation diversity even while improving technical consistency.

Assurance access also needs protection from commercial conflicts. Operators funding evaluation should disclose the relationship and preserve reviewers' control over conclusions. A certification mark should identify its tested scope and the findings still outstanding.

Required evidence and status

Before broad adoption, the programme should publish its side-channel model, resolve the settlement evidence profile and demonstrate workable user appeals. Review should include small browser implementations, publishers with limited resources and people operating under an assigned policy authority.

The review supports continued technical work and a wider consultation. It leaves the policy legitimacy of assigned exposure, the reach of the bypass restriction and the accessibility of certification open. This report supplies no regulatory approval or comprehensive implementation certification.

Supporting publications

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

<https://lifecorp.org/archive/veil-protocol>