**Subject:** Proposal for Discussion: The Secure Internet – Embedding Trust into the Protocol Layer

Dear IETF and W3C Working Group Members,

I’m writing to propose a discussion around a new architectural model we call **The Secure Internet**—a vision that reimagines how identity and trust are established online by embedding them directly into the transport layer.

At the core of this model is a cryptographic identity signal called the **Live Key**, derived from the user presence, security posture and anchored in TPM hardware. This signal is long-lived, non-exportable, and accessible only when specific security conditions are met—such as active user’s OS login, full disk encryption, and up-to-date system patches. These conditions are **policy-defined**, allowing organizations to enforce dynamic, context-aware trust requirements beyond simple user presence.

Furthermore, the Live Key enables **mutual TLS (mTLS)** without requiring client-side certificates. Instead, the client registers its Live Key directly with the server, similar to the FIDO model. This simplifies trust establishment, eliminates the need for certificate authorities, and enables personalized, cryptographically assured sessions.

The Secure Internet aligns with the goals of both **TLS** and **WebAuthn/FIDO2**:

* It complements mTLS by enabling certificate-less client authentication.
* It enhances FIDO2 and Passkeys by offering a transport-level trust mechanism that can eliminate user interaction and additional policy-defined signals check while maintaining strong assurance.
* It inherently satisfies and exceeds **NIST FAL3-level assurance** without tokens, or channel binding. The architecture can eliminate the need for federated authentication entirely. In this model, the identity provider (IdP) evolves into a real-time, CA-like trust authority—capable of informing the relying party (service provider) when a previously registered public key is no longer trusted.

**Importantly, this model does not require changes to existing standards—at least not initially.** It builds on them, offering a new way to express identity and trust natively within the protocol layer. In the future, optional client certificates may be considered as part of evolving standards. We believe this approach could be of interest to working groups focused on TLS, OAuth, WebAuthn, and identity federation.

We would welcome the opportunity to present this concept, share open specifications, and explore how it might align with ongoing efforts across both IETF and W3C.

Thank you for your consideration.

Sincerely,
**Thi Nguyen-Huu**
CEO
WinMagic Inc.
thi.nh@winmagic.com

2025/8/11 [www.winmagic.com](http://www.winmagic.com)