

August 18, 2025

Subject: Proposal for BOF: The Secure Internet (SI)

Dear IETF Community,

The Secure Internet (SI) enables what legacy architectures deemed infeasible — and what users have long dreamed of:

- **No user action:** No passwords, no MFA, no friction.
- **Protocol-native protection:** Cryptographic defense against session hijacking and adversary-in-the-middle (AitM) attacks.

I'm writing to propose a BOF (Birds of a Feather) session for this new architectural initiative. This proposal builds on my earlier outreach and now reflects additional technical depth and deployment maturity.

The Secure Internet introduces a new trust model for Internet communications — one that replaces static credentials and certificate-based authentication with **policy-bound cryptographic keys**, anchored in hardware or software, and available only when organizational trust conditions are met. This enables **non-interactive, mutual authentication** via mTLS, transforming how endpoints and services establish trust.

Key innovations include:

- **Live Key:** A dynamic identity signal tied to verified user presence and device integrity, anchored in TPM or software.
- **LIM/TIM (The Identity Machine):** A policy engine that governs Live Key availability based on endpoint posture, OS login, encryption status, and other trust conditions.
- **MagicEndpoint:** A trusted channel between endpoint and IdP, enabling continuous identity signaling and delegated authentication.

WinMagic has already deployed mTLS with Live Key for its own applications. The client software is currently available in Beta, for Windows only at this time. Any server that supports mTLS can eliminate user authentication entirely using Live Key. This means any app or service that adopts this model becomes part of the Secure Internet.

The architecture also supports enhancements such as behavioral integrity via signature counters and fallback models using symmetric mTLS issued by the IdP — ensuring compatibility and layered trust. **Certificate-less mTLS is a secondary, optional enhancement** that simplifies deployment but is not required for the core Live Key proposal.

Given the architectural scope — spanning transport security, endpoint identity, and trust enforcement — SI does not fit neatly into existing working groups. I believe a BOF is the right venue to:

- Explore the feasibility of a new working group
- Discuss technical foundations and deployment models
- Align with existing standards (TLS, FIDO2, RATS)
- Define a roadmap for multiple RFCs under the Secure Internet umbrella

The Secure Internet architecture addresses long-standing vulnerabilities in identity and session management — replacing cookies, tokens, and federated flows with cryptographic identity embedded in the transport layer. It achieves channel binding natively and aligns with NIST FAL3 assurance levels. By authenticating both endpoints

WinMagic Corp.

11-80 Galaxy Blvd. | Toronto, ON | M9W 4Y8
Tel: +1.905.502.7000 | Toll Free: 888.879.5879

www.winmagic.com



with policy-bound keys, it mitigates adversary-in-the-middle attacks at the protocol level. While WinMagic's MagicEndpoint product demonstrates these principles in practice, it is not part of the proposed standardization scope.

This proposal is submitted with **no IPR claims and no patent intentions**. It is offered freely to the community for open standardization.

I've attached the full BOF proposal and a document with preliminary use case descriptions, and I welcome your feedback and guidance on next steps.

**Note: Live Key currently supports Windows endpoints with TPM. Support for other platforms is under consideration, including macOS, mobile devices, and Linux. These platforms typically offer hardware cryptographic capabilities (e.g., Secure Enclave, TrustZone), which may be used to anchor Live Key in a limited form. Software-based deployment is also possible, though with reduced assurance. TPM remains the preferred anchor for multi-user environments and policy-bound trust enforcement.*

Warm regards,
WinMagic Corp.

Thi Nguyen-Huu

Thi Nguyen-Huu
Proposer and Lead Architect of The Secure Internet
CEO, WinMagic Inc.
thi.nh@winmagic.com

WinMagic Corp.

11-80 Galaxy Blvd. | Toronto, ON | M9W 4Y8
Tel: +1.905.502.7000 | Toll Free: 888.879.5879
www.winmagic.com