The Secure Internet (SI)

Birds of a Feather Proposal (BOF)

Problem Statement

The current Internet architecture relies heavily on static credentials, certificate-based trust, and user-driven authentication workflows. These models are increasingly vulnerable to session hijacking, adversary-in-the-middle attacks, and identity spoofing — especially in enterprise and zero-trust environments.

The Secure Internet (SI) proposes a new trust model where identity is derived from policy-bound cryptographic keys, anchored in TPM 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. Live Key is the core innovation of SI, enabling secure transport and identity assertion without requiring user interaction or traditional IAM mechanisms like FIDO.

Certificate-less mTLS is a secondary, optional enhancement that simplifies deployment and management. It may be adopted independently of Live Key and is discussed later in this proposal.

Goals of the BOF

- Explore the feasibility of a new IETF working group focused on identity-bound transport security.
- Discuss the technical foundations of Live Key, LIM/TIM (The Identity Machine), and MagicEndpoint.
- Evaluate the implications of non-interactive mTLS authentication using Live Key.
- Introduce the concept of a FIDO-like signature counter for behavioral integrity.
- Present fallback models using symmetric mTLS via IdP-issued session keys.
- Define a roadmap for potential RFCs under the Secure Internet umbrella.

Scope of Discussion

- Live Key: A dynamic cryptographic signal tied to verified user presence and device integrity.
- LIM/TIM: The system that governs Live Key availability based on policy-defined trust conditions.
- MagicEndpoint: A trusted channel between endpoint and IdP, enabling continuous identity signaling.
- Signature Counter: A mandatory increment-by-1 mechanism to detect key misuse or cloning.
- Symmetric mTLS: Secure transport via short-lived keys issued by IdP when TPM is unavailable.
- Integration with existing protocols: TLS 1.3, OAuth, FIDO2, and enterprise IAM systems.

Live Key enables online authentication via mTLS without requiring user interaction, replacing traditional IAM mechanisms such as FIDO. It supports multiple keys per user per endpoint and provides cryptographic identity assertion embedded in the transport layer. This architecture replaces cookies, tokens, and federated flows, achieves channel binding natively, and aligns with NIST FAL3 assurance

THI NGUYEN-HUU
PROPOSER AND LEAD ARCHITECT OF THE SECURE INTERNET
CEO AND FOUNDER

levels. By authenticating both endpoints with policy-bound keys, it mitigates adversary-in-the-middle attacks at the protocol level.

Certificate-less mTLS, discussed optionally, allows direct registration of Live Key public keys and simplifies deployment. While WinMagic's MagicEndpoint product demonstrates these principles in practice, it is not part of the proposed standardization scope.

Expected Outcome

- Agreement on the need for a new working group or charter extension.
- Community feedback on the architecture and terminology.
- Identification of contributors and stakeholders (e.g., enterprise security vendors, TPM/FIDO experts).
- Initial drafts for:
  - Live Key format and transport
  - mTLS handshake extensions
  - Endpoint identity signaling protocol
  - Trust policy enforcement framework
  - Signature counter specification

Related Work

- RFC 8446 (TLS 1.3)
- RFC 9334 (OAuth 2.1)
- RFC 8894 (Remote Attestation Procedures)
- FIDO2/WebAuthn specifications
- TPM standards

Proposed Agenda

1. Introduction to the Secure Internet vision
2. Technical overview of Live Key and LIM/TIM
3. Use cases and deployment scenarios
4. Comparison with existing models (PKI, FIDO, OAuth)
5. Open discussion: scope, challenges, and next steps
6. Call for contributors and draft authors

THI NGUYEN-HUU
PROPOSER AND LEAD ARCHITECT OF THE SECURE INTERNET
CEO AND FOUNDER