WINMAGIC

Authenticate. Encrypt. Achieve.

Secure Internet Use Cases

Supplementary BOF Material

Use Case 1: Online Authentication Without User Interaction (IAM/CIAM)

Problem Statement

IAM and CIAM systems rely on user-driven authentication workflows — passwords, MFA, FIDO challenges — introducing friction, delay, and abandonment. These mechanisms assume the user must actively prove their identity, even when the endpoint is already trusted and capable.

This reliance on user action reduces conversion rates, complicates UX, and shifts responsibility away from the systems best equipped to enforce trust.

Live Key Solution

The Secure Internet enables seamless online authentication without user interaction. The Live Key, available only when trust conditions are met, is used during the mTLS handshake to assert identity. This eliminates the need for passwords, tokens, or biometric prompts, enabling frictionless login experiences for both enterprise users and consumers.

Authentication becomes automatic, cryptographic, and policy-bound — not procedural.

Philosophical Shift

We often hear that the user is the weakest link. But perhaps the real weakness is asking the user to authenticate at all.

The endpoint — capable of public key cryptography, local MFA, and real-time posture checks — is in the best position to verify the user securely and resiliently. It should act as the **self-driving vehicle** of trust, guiding the user through the online world without friction.

The endpoint is the user's natural companion — already required for access, already capable of enforcement.

Endpoint access should unlock everything else.

This also enables continuous verification. Unlike SSO, which grants **long-lived, questionable access** after a single check, Live Key-based authentication can occur silently and frequently — without burdening the user.

No user action means trust can be verified as often as needed.

And if your solution doesn't offer "**no user action**", maybe it's time to say no.

Secure Internet Use Cases

Supplementary BOF Material

Use Case 2: Replacing Cookies and Tokens for Web Authentication

Problem Statement

Web authentication today relies heavily on cookies and bearer tokens—mechanisms that are vulnerable to theft, replay attacks, and session hijacking. Attackers increasingly target these artifacts to bypass authentication entirely, even in environments protected by leading identity platforms.

Recent breaches involving **MGM Resorts**, **Caesars Entertainment**, **Microsoft**, and **Okta** have underscored the systemic risk of token-based authentication. These incidents demonstrate that possession-based identity is no longer sufficient, and that session integrity must be anchored in something stronger than a stolen token.

Live Key Solution

The Secure Internet replaces cookies and tokens with cryptographic identity embedded directly in the transport layer. During the mTLS handshake, the **Live Key** asserts both user and device identity, and the resulting session key is cryptographically bound to the endpoint. This eliminates the need for bearer tokens or cookies, prevents session hijacking, and simplifies authentication by making it non-interactive and policy-bound.

Unlike traditional authentication, which relies on server-side validation of opaque tokens, Live Key shifts trust to the endpoint. The identity signal is ephemeral, policy-governed, and anchored in hardware (TPM), ensuring that only verified users on trusted devices can initiate secure sessions.

Philosophical Shift

The transition from cookies and tokens to Live Key represents a **fundamental rethinking of identity and trust** on the web:

- **From possession to presence**: Traditional tokens prove possession (e.g., a cookie stored in the browser). Live Key proves presence—of the user, the device, and the trust conditions—at the moment of connection.
- **From static credentials to dynamic signals**: Cookies and tokens are static artifacts that persist beyond their intended context. Live Key is a dynamic, ephemeral signal that exists only when trust conditions are met, reducing attack surface and eliminating stale credentials.
- **From server-centric to endpoint-centric trust**: Instead of relying solely on server-side logic to validate identity, Live Key empowers the endpoint to assert identity securely and autonomously, shifting the trust anchor closer to the user.
- **From authentication as an event to authentication as a state**: With Live Key, identity is continuously verified throughout the session, not just at login. This enables persistent trust and real-time enforcement of policy changes.
- **From workaround to architecture**: Cookies and tokens were invented as workarounds for a stateless web. Live Key is not a workaround—it's a foundational building block for a secure, stateful, and identity-aware Internet.

Secure Internet Use Cases

Supplementary BOF Material

Use Case 3: Zero Trust Continuous Access Control — Redefining 'Verify Before Use'

Problem Statement

Zero Trust architectures demand continuous verification of user and device trust. Yet most implementations rely on static credentials, one-time authentication, or procedural checks that occur before access is granted. This model assumes trust is a discrete event — verified once, then used — which creates timing gaps and leaves sessions vulnerable to drift or misuse.

Even modern Zero Trust frameworks often misinterpret the principle, stating: "verify user and device for each transaction." But this implies a flawed sequence: verify first, then use — as if trust can be checked and then forgotten.

Live Key Solution

The Secure Internet introduces a cryptographic enforcement model that corrects this flaw. It does not verify before use — it verifies through use.

- The Live Key is the private key used during the mTLS handshake, enabling mutual authentication and session key derivation.
- The Live Key is only accessible when the endpoint meets real-time trust conditions — such as OS patch level, disk encryption status, user presence, and device integrity.
- If any condition fails (e.g., the user logs out or the device posture changes), the Live Key becomes unavailable.
- Without the Live Key, a new mTLS session cannot be initiated — access is cryptographically denied.

Philosophical Shift

Traditional Zero Trust models rely on repeated checks — verify, then allow. But this procedural mindset introduces friction, delay, and vulnerability.

The Secure Internet reframes trust as a **cryptographic presence**. The Live Key is not just a credential — it is a signal of trust. If conditions falter, the key vanishes. And with it, access.

This is not access control. It is **access disappearance** — enforced by policy, anchored in hardware, and embedded in the protocol itself.

If encryption is possible, trust is verified.

No prompts. No tokens. Just presence.

Secure Internet Use Cases

Supplementary BOF Material

Use Case 4: Native Channel Binding — Fixing a Fundamental Flaw

Problem Statement

Industry efforts such as Token Binding, OAuth channel binding, and Zero Trust verification flows attempt to solve a narrow problem: ensuring that the endpoint used during authentication is the same one used for the session. These mechanisms are designed to defend against adversary-in-the-middle (AitM) attacks — but they do so by layering complexity on top of TLS, without addressing the root cause.

The fundamental flaw, discovered during the foundational work on The Secure Internet in 2023, is this:

Identity verification is often decoupled from session establishment. The session key — the cryptographic anchor of the channel — is established without binding it to a verified identity. This leaves a gap that attackers can exploit.

Live Key Solution

The Secure Internet solves this flaw elegantly and directly:

- Identity is verified within the mTLS handshake using the Live Key.
- The session key is derived from this handshake, meaning identity and channel are cryptographically inseparable.
- There is no need for separate channel binding mechanisms — the channel is the identity assertion.

This is not a workaround. It's a clean architectural correction that replaces fragile overlays with protocol-native trust.

Philosophical Shift

Security frameworks often treat channel binding as a complex add-on — layering mechanisms atop TLS to patch a deeper flaw. But complexity is not assurance.

The Secure Internet begins with a simple insight: **the root cause of channel binding failures is the separation of identity and transport**. Once this is understood, the solution becomes elegant.

By embedding identity directly into the mTLS handshake via the Live Key, channel binding is no longer a work-around — it is **native**. This simplicity enables **FAL3-grade assurance** without ceremony.

Knowing the root cause doesn't just fix the problem — it dissolves it.

If encryption is possible, trust is verified.

Secure Internet Use Cases

Supplementary BOF Material

Use Case 5: Short-Lived Key Deployment for TPM-less Endpoints

Problem Statement

Many endpoints lack TPMs or full-featured hardware key storage, excluding them from secure identity frameworks that rely on attestation and policy-bound key availability. This creates a gap in trust coverage—especially for BYOD devices, legacy systems, non-Windows platforms, and lightweight clients—which often fall back on less secure or more manual authentication methods.

Importantly, **most modern devices do include some form of hardware-based cryptographic capability**—such as Secure Enclave (Apple), TrustZone (ARM), or embedded secure elements in mobile and IoT platforms. These can be used to store keys and perform cryptographic operations, but they often lack the full attestation, policy enforcement, and lifecycle control offered by TPM.

Live Key is designed to **embrace this diversity**. It supports TPM-less endpoints through flexible models that still enforce ephemeral, policy-governed identity signals. TPM remains the preferred anchor for its completeness and trust guarantees, but Live Key ensures that **security is not gated by hardware exclusivity**. Instead, it adapts to the capabilities of each endpoint, enabling broad participation in The Secure Internet.

Live Key Solution

The Secure Internet supports short-lived key deployment for TPM-less endpoints, enabling secure participation without requiring specialized hardware. Several models are supported:

1. **Pre-Shared Short-Lived Key Model**

   A short-lived symmetric key is distributed to both the endpoint and the service provider, enabling mTLS with pre-shared key (PSK) authentication.

2. **Delegated Asymmetric Key Model**

   A short-lived asymmetric key pair is generated by a trusted authority (e.g., the IdP) and distributed securely to both parties.

3. **Endpoint-Generated Key Model**

   The endpoint generates its own key pair and registers the public key with a trust authority, which validates and propagates trust.

4. **FIDO2-Based Session Key Establishment**

The endpoint uses FIDO2 to authenticate directly with the service provider. The resulting authentication can be used to derive a short-lived session key. This model does not require an IdP and is ideal for direct trust relationships.

Secure Internet Use Cases

Supplementary BOF Material

Note: TLS would need to support mid-session key rotation or derivation to fully enable this model. This may require a future RFC proposal to extend TLS capabilities.

These models ensure that even TPM-less endpoints can participate in cryptographically secure sessions, with keys that are ephemeral, policy-bound, and governed either centrally or locally.

Philosophical Shift

This use case reflects a shift from hardware exclusivity to inclusive trust:

- From exclusion to inclusion: Security frameworks often exclude endpoints without TPMs. Live Key embraces them by offering flexible, policy-bound alternatives.
- From static trust anchors to dynamic trust orchestration: Trust is orchestrated dynamically, whether by an IdP or through direct authentication mechanisms like FIDO2.
- From rigid infrastructure to adaptive architecture: The Secure Internet accommodates diverse environments, ensuring that security is not gated by hardware availabilty.

Secure Internet Use Cases

Supplementary BOF Material

Use Case 6: Machine-to-Machine (M2M) Communication

Problem Statement

M2M communication often relies on static credentials, long-lived API keys, or embedded secrets. These are difficult to rotate, prone to leakage, and lack dynamic trust enforcement. As systems scale and interconnect, managing these credentials becomes a security and operational burden.

Live Key Solution

The Secure Internet enables dynamic, policy-bound authentication for M2M communication. Each machine uses a **Live Key** to authenticate via **mutual TLS (mTLS)**, with trust governed by the Identity Provider (IdP) based on posture, configuration, and policy.

Live Key ensures that:

- Only verified machines can initiate secure sessions.
- Keys are ephemeral and bound to current trust conditions.
- Authentication is cryptographically enforced without manual credential management.

This replaces static secrets with **real-time identity signals**, enabling secure automation across distributed systems, microservices, and edge devices.

Philosophical Shift

This use case reflects a transformation in how machines participate in secure ecosystems:

- **From static identity to dynamic presence**: Machines no longer rely on embedded secrets or long-lived credentials. They assert identity only when trust conditions are met.
- **From credential management to trust orchestration**: The Secure Internet replaces manual provisioning and rotation with policy-bound key availability, governed by posture, configuration, and context.
- **From passive endpoints to active trust agents**: Machines become aware of their trust posture and assert identity as living signals—ephemeral, contextual, and policy-driven.

This shift enables secure automation and infrastructure at scale, without relying on human intervention or static credentials. It lays the foundation for a trust-aware digital ecosystem, where machines interact securely and autonomously.

Optional Deployment Enhancements

The Secure Internet architecture supports optional enhancements that simplify deployment and improve compatibility. These features are modular and can be adopted incrementally:

Certificate-less mTLS

Certificate-less mTLS allows endpoints to authenticate using raw public keys or short-lived symmetric keys, eliminating the need for traditional certificate infrastructure. This simplifies deployment, aligns with FAL3 principles, and supports emerging models like Passkeys.

Behavioral Integrity

Behavioral Integrity leverages strict signature counters and real-time endpoint telemetry to detect anomalies, enforce behavioral trust, and prevent key misuse or cloning. This enables continuous verification beyond cryptographic assurance.

Privacy Consideration: Per-SP Live Key

To enhance privacy, endpoints may use distinct Live Keys for different servers or service providers. This prevents cross-service correlation and supports privacy-preserving authentication. While this capability is already implemented using TPM, our initial focus is on workforce scenarios where the IdP is the sole server. Broader applications will be discussed in future documents.

Role of the IdP

The IdP may act as a real-time trust authority, dynamically informing service providers of endpoint events—such as screen lock status—to signal potential absence of the user. This enables adaptive access control. The IdP can remain dormant for extended periods, activating only during critical events or incidents.

These enhancements are optional and modular, allowing organizations to adopt Secure Internet principles incrementally. Each feature supports specific deployment goals—whether reducing complexity, enhancing privacy, or enabling real-time trust signaling—without requiring wholesale infrastructure changes.

Closing Perspective: The Secure Internet Vision

The Secure Internet is more than a set of use cases—it is a **new trust architecture** for the digital world. It redefines identity, authentication, and access across users, machines, and services. Whether applied to endpoint login, web authentication, remote access, or machine-to-machine communication, the core principle remains the same: **trust must be dynamic, policy-bound, and cryptographically enforced**.

Built for Machines, Not Just Users

While Live Key enables seamless user authentication, the architecture is fundamentally designed for **machine-to-machine (M2M) communication**. Machines assert identity autonomously, governed by posture and policy, without relying on static credentials or manual provisioning. This makes The Secure Internet ideal for automation, orchestration, and secure infrastructure at scale.

Reverse AI: A New Paradigm

Traditional AI seeks to make machines behave like humans. The Secure Internet introduces **Reverse AI**—a paradigm where machines do not impersonate humans—they **earn trust like humans**.

Each machine becomes a dynamic identity signal, asserting its presence, integrity, and compliance with policy. This transforms M2M communication from static automation into **trust-aware interaction**, where machines behave as responsible actors in a secure ecosystem.

Resilience Against Modern Threats

The Secure Internet is inherently resistant to:

- **Phishing**: There are no passwords, tokens, or user prompts to exploit.
- **AI-driven impersonation**: Deepfakes, synthetic identities, and impersonation attacks rely on tricking users. The Secure Internet removes user interaction entirely, closing that attack surface.
- **Session hijacking**: Keys are ephemeral and bound to verified endpoints, eliminating replay risk.

Inclusive, Adaptive, and Future-Proof

Live Key adapts to the capabilities of each endpoint. TPM is preferred for its completeness, but Secure Enclave, TrustZone, and even software-based deployments are supported. The architecture is inclusive—designed to evolve with hardware, standards, and operational models.

The best solution is the simplest — but not simpler.

The Secure Internet embodies this principle: reducing complexity for users and developers, while elevating the integrity of trust.

Thi Nguyen-Huu

Proposer and Lead Architect of The Secure Internet

CEO, WinMagic Corp.

thi.nh@winmagic.com