WINMAGIC®

Authenticate. Encrypt. **Achieve.**

The case for **Deterministic Transport Identity**

Author: **Thi Nguyen-Huu, WinMagic Corp.**

US & CANADA
+1 888 879 5879 | EMEA
+49 69 175 370 530 | JAPAN
+03 5403 6950

SecureDoc™ by WinMagic

Whitepaper

The Case for Deterministic Transport Identity

Simplicity vs. Complexity: Why the Transport Layer is the Natural Home for Identity

1. The Core Conflict: Procedural vs. Deterministic

The industry has reached a crossroads in how to secure a user's session after the initial login. Various industry groups have worked—and continue to work—on numerous methods for "binding" an identity to a session. These efforts generally follow one of two paths:

- **The Procedural Approach:** Schemes such as **DPoP** (Demonstrating Proof-of-Possession), **Token/Channel Binding**, and **NIST FAL3** all share a common DNA: they attempt to bind a **session token** to a device through a series of "checks." Whether it is signing a JWT for every HTTP header or managing complex cookie-refresh loops (as seen in recent **DBSC** proposals), these methods are procedural. They require the application layer to constantly manage state and perform cryptographic "gymnastics" to prove the session is still valid—or concretely, to prove that only the correct endpoint can satisfy the various token checks.
- **The Deterministic Approach (PADIT):** This treats the identity not as an object to be checked, but as the inherent state of the connection. Instead of trying to bind a device to a token, **no token is used at all.** The identity is "baked" into the **TLS 1.3 Transport Layer**. If the verified secret is present in the handshake, the encrypted tunnel exists; if it is not, the connection simply cannot be established. This is a deterministic model: the existence of the communication is the proof of the identity.

2. What is PADIT? (Post-Authentication Device Identity in Transaction)

PADIT is the architectural realization of this deterministic model. While the industry has the ingredients for this simpler path, they have not yet been integrated into a standard flow.

The Mechanism:

1. **The Secret:** It utilizes the **FIDO2 PRF (Pseudo-Random Function) extension**—the same logic used by Microsoft Windows Hello for secure local logins (the hmac-secret).
2. **The Bridge:** After a user is verified via a FIDO2 ceremony, the authenticator outputs a unique symmetric secret.
3. **The Integration:** Instead of using this secret to sign an application-layer header or token, PADIT plugs it directly into the **External PSK (Pre-Shared Key)** slot of a standard **TLS 1.3** handshake.
4. **The Result:** No token is ever exposed. The identity moves from the vulnerable browser memory to the secure transport stack.

3. Security Analysis: Why "No Token" is the Ultimate Defense

In the procedural systems currently favored by the industry, the **Token** is a constant liability. Because a token is an object—a piece of data—it can be exposed, scraped from memory, or intercepted in transit. The "gymnastics" involved in current industry proposals are merely attempts to mitigate the risk of a target that shouldn't exist in the first place.

The PADIT Advantage:
Zero Exposure: Because PADIT utilizes a **non-exposed key** to establish the TLS session, there is no "target" for an attacker to steal.
Deterministic Isolation: In procedural models, the session keys and the tokens often sit in the same browser memory. In the PADIT model, the key remains in the protected TLS stack. The browser handles the data, but it never handles the identity.
Mathematical Proof: We move from a world of "Checking Credentials" to a world of "Enabling Communication." If the handshake succeeds, the identity is mathematically proven. There is no secondary step where a stolen token could be "replayed."

4. The "Einstein" Verdict: As Simple as Possible

In security, **complexity is a vulnerability.** Methods like DBSC require thousands of lines of new code across browsers and servers to manage an ongoing "refresh ceremony." Each new line of code is a potential failure point.

PADIT reduces the entire identity problem to a binary condition in the TLS handshake. It is "as simple as possible, but no simpler." It is easier to implement, easier to audit, and mathematically more robust because it removes the "human-made" complexity of session management.

5. Looking Forward: From PADIT to LIT

While PADIT provides the most elegant solution for verified device identity today, it serves as the necessary foundation for **LIT (Live Identity in Transactions)**.

- **PADIT** represents the world's most efficient **verified** authentication.
- **LIT** achieves the ultimate goal: **No Authentication** (Zero-Friction).

By moving identity into the continuous "Pulse" of the transport layer, we transition from the era of "logging in" to the era of **continuous, invisible trust.**