Existence Authentication — Inspection Brief

A presence-based authorization model, presented for public and governmental inspection

Version: 1.0
Date:
Prepared for: Government, regulatory, and public-infrastructure review
Contact: https://existenceauthentication.com

This document is not promotional. It is prepared solely to enable inspection.

1. Purpose, Scope, and Limits

This Inspection Brief is provided to enable initial, good-faith review of Existence Authentication, a presence-based authorization model intended for use in public and regulated digital environments. The purpose of this document is to define the problem the model addresses, state its core assertion, describe its enforcement boundaries, and identify the governance constraints under which it operates.

This brief does not seek endorsement, procurement, mandate, or approval. Its sole purpose is to allow reviewers to determine whether deeper inspection is warranted.

2. The Structural Problem

In physical environments such as secure facilities, financial institutions, and healthcare systems, proof of identity or presence is required before access or action is permitted. This requirement is not treated as a feature or an enhancement; it is treated as a prerequisite. Without it, responsibility cannot be assigned, access cannot be justified, and enforcement cannot occur.

Digital systems evolved under different constraints. Early network architectures prioritized connectivity, availability, and fault tolerance in environments where users were few, systems were isolated, and automation was limited. In that context, authentication mechanisms based on credentials and tokens functioned as practical proxies for presence. Possession of a credential was treated as sufficient evidence that a human was requesting an action.

At modern scale, this assumption no longer holds.

Contemporary digital environments operate continuously, globally, and at speeds that exceed human interaction. Credentials, certificates, session tokens, and behavioral indicators can be copied, delegated, replayed, or automated without the presence of the individual to whom they were originally issued. As a result, authentication systems increasingly verify *data artifacts* rather than the existence of the person claiming them.

This is not a failure of implementation, compliance, or policy. It is a category error.

Multi-factor authentication, biometrics, and behavioral analytics attempt to increase confidence that a request originates from the "rightful" user. However, these mechanisms remain probabilistic. They assess likelihood, risk, or similarity rather than establishing a deterministic condition. At the moment a privileged action occurs, execution of a command, approval of a transaction, transfer of data, the system does not know whether a human is present. It knows only that certain data conditions have been satisfied.

Continuous authentication and risk scoring extend this model but do not resolve the underlying issue. They distribute trust across time rather than anchoring it to the moment of action. A request may be allowed because it appears consistent with prior behavior, even if no human is present at the time the action is executed.

This gap enables impersonation, unauthorized delegation, automation abuse, and attribution failure as *structural possibilities*. These outcomes do not require sophisticated attackers or system compromise. They arise naturally from systems that accept requests without requiring proof of presence.

Critically, the absence of a presence requirement undermines accountability. When actions are performed without proof that a human is present, responsibility becomes ambiguous. Systems can log credentials, IP addresses, and timestamps, but they cannot establish whether a person existed at the moment the action occurred. This ambiguity weakens enforcement, auditability, and legal attribution.

The structural problem, therefore, is not that digital systems lack controls. It is that they lack a foundational condition that is assumed in physical security contexts: verification that a human exists at the moment privileged actions are requested.

Existence Authentication is proposed as a response to this specific absence. It does not seek to replace existing authentication mechanisms or to improve risk scoring. It introduces a missing prerequisite that must be satisfied before other controls are evaluated.

3. Core Assertion and Definition of Existence

Existence Authentication is based on a single, narrow assertion:

Privileged digital actions must require proof of human presence at the moment of execution.

This assertion does not claim that presence alone is sufficient for authorization. It claims only that presence is a necessary precondition. Authorization, identity, and entitlement remain governed by existing mechanisms once presence has been established.

To support this assertion, the model introduces a strict and limited definition of *existence*.

Existence is defined as a condition independent of the network and independent of stored data. User data, credentials, certificates, and session artifacts may persist across time and systems. Existence does not. It is evaluated only at the moment it is queried and has no state before or after that moment.

When queried, existence returns a binary outcome:

- **Present**
- **Absent**

There is no intermediate state. There is no confidence score, probability, or risk threshold. Presence is not inferred from past behavior, device characteristics, location, or reputation. It is established or it is not.

This binary constraint is intentional.

Probabilistic systems, such as behavioral analytics, anomaly detection, and continuous authentication, optimize for likelihood. They are designed to reduce false positives or false negatives over time. While useful for detection and monitoring, probabilistic models cannot provide deterministic answers at the moment a privileged action occurs. They may indicate that an action is *likely* legitimate, but they cannot establish that a human is present.

In regulated and legal contexts, this distinction matters. Accountability, liability, and enforcement require clear attribution boundaries. A system that allows an action based on probability cannot later establish with certainty, whether a person existed at the moment that action was taken. Binary presence by contrast, maps cleanly to audit, responsibility, and enforcement.

Existence Authentication deliberately excludes identity attributes from the presence check. The system does not determine *who* the user is, nor does it evaluate personal characteristics, biometrics, or behavior. Identity is evaluated only after presence has been established and only through existing authentication mechanisms chosen by the network.

This separation prevents the presence check from becoming a surveillance mechanism or a proxy identity system. Presence is treated as a condition, not as a judgment about a person.

Absence is treated as a hard stop. If a user is not present at the exact moment a privileged action is requested, the system does not evaluate credentials, risk, or intent. The request is rejected. This constraint is fundamental to the model and is not subject to discretionary override.

By defining existence as a binary, moment-bound condition, Existence Authentication establishes a clear, inspectable boundary between *assumption* and *verification*. It does not attempt to predict legitimacy. It requires proof of presence before legitimacy is evaluated.

4. Enforcement Boundary

Existence Authentication is intentionally constrained by a clearly defined enforcement boundary. This boundary determines where presence verification is mandatory, where it is optional, and where it is explicitly not applied.

The mandatory enforcement point for existence verification is **prior to authentication access**.

If a user cannot prove presence, authentication does not proceed. Credentials, certificates, tokens, and other authentication artifacts are not evaluated. This ordering is deliberate. It ensures that no identity claim is processed unless a human is present at the exact moment the claim is made.

This boundary establishes a necessary condition without altering existing authentication logic. Identity verification, authorization decisions, and entitlement evaluation remain governed by systems already in place. Existence Authentication does not replace or subsume these mechanisms; it precedes them.

The enforcement boundary is intentionally narrow.

Requiring presence verification only before authentication prevents the system from expanding into continuous monitoring or surveillance. Presence is not checked persistently, periodically, or retroactively. It is checked only when a user requests access or initiates a defined action. Once the check is complete, the system does not continue to observe or evaluate the user.

Beyond initial access, networks may choose to extend presence verification to additional actions. These may include, but are not limited to, execution of privileged commands, transfer of sensitive data, configuration changes, or approval of high-impact operations. Such extensions are network-specific decisions, not defaults imposed by the model.

This optional expansion is designed to preserve network sovereignty. Each environment determines which actions are sufficiently sensitive to warrant a presence check. The model does not prescribe a universal policy. It provides a mechanism that can be applied selectively, proportionally, and transparently.

Equally important are the actions to which presence verification is not applied by default. Existence Authentication does not require presence for passive activities such as data storage, background processing, system maintenance, or automated tasks that do not represent user-initiated privilege. This distinction prevents disruption and avoids conflating human presence with system operation.

The enforcement boundary also serves as a safeguard against misuse. By limiting mandatory presence checks to specific, inspectable points, the system prevents the accumulation of presence data and avoids creating a continuous signal that could be repurposed for tracking or profiling. The system answers a single question at a single moment and then stops.

This boundary is auditable. Reviewers can inspect where presence checks occur, where they do not occur, and how those decisions are made. The model's security benefit derives not from breadth of enforcement, but from precision.

By defining and enforcing this boundary, Existence Authentication introduces a presence requirement without expanding its authority beyond what is necessary to achieve its stated purpose.

5. System Behavior

Existence Authentication operates by introducing a presence verification call at defined points of user-initiated action. This call is executed synchronously with the action request and evaluates only whether the requesting user is present at that moment.

The system does not attempt to interpret intent, analyze behavior, or assess risk. It answers a single question and returns a single result.

If presence is confirmed, the request proceeds unchanged to existing authentication and authorization mechanisms. Credentials, certificates, access policies, and role definitions are evaluated exactly as they would be in the absence of Existence Authentication. No modification to entitlement logic is required.

If presence is absent, the request is rejected immediately. No credentials are processed, no identity is evaluated, and no partial authorization occurs. The rejection is deterministic and attributable to a single condition: absence of presence at the moment of request.

The system does not retain presence state. Presence is not cached, replayed, or inferred across actions. Each presence check is independent and moment-bound. The system does not establish sessions, profiles, or continuity of presence beyond the instant of evaluation.

Existence Authentication operates independently of content. It does not inspect payloads, commands, or data values. Its operation is orthogonal to application logic and does not require awareness of what action is being performed beyond whether the action has been designated as requiring presence.

From an audit perspective, the system produces a clear, inspectable outcome: a presence check occurred at a defined enforcement point and returned either present or absent. This outcome can be logged and reviewed without revealing identity attributes, behavior patterns, or content.

The security effect of the system derives from *ordering*, not complexity. By requiring presence before authentication or execution, the system ensures that privileged actions cannot be initiated in the absence of a human, regardless of how credentials or automation are otherwise handled.

6. Explicit Non-Capabilities

Existence Authentication is defined as much by what it does *not* do as by what it does. These non-capabilities are intentional design constraints, not omissions.

The system does *not* track individuals across systems or over time. It does not establish identity continuity, behavioral profiles, or longitudinal records of presence.

The system does *not* score behavior, infer intent, or evaluate legitimacy probabilistically. There are no thresholds, confidence levels, or adaptive models. Presence is not a risk signal and is not combined with other signals.

The system does *not* perform continuous monitoring. It does not observe users between actions, during sessions, or after authentication. There is no background verification, or persistent signal.

The system does *not* monetize, aggregate, or externalize presence information. Presence checks are not exposed as data products and are not repurposed for analytics, marketing, or surveillance.

The system does *not* replace existing authentication standards or identity frameworks. It does not define who a user is, what they are entitled to do, or how identity should be managed. Those responsibilities remain with existing systems chosen by the network.

The system does *not* introduce discretionary or opaque decision processes. There are no human overrides, policy engines, or hidden rules. The outcome of a presence check is inspectable, binary, and attributable.

These non-capabilities exist to prevent mission creep. They ensure that Existence Authentication remains narrowly focused on enforcing a single prerequisite and does not evolve into a general-purpose monitoring or control system.

7. Governance and Economic Alignment

Existence Authentication is accompanied by a governance framework designed to address a known failure-mode in security systems: misaligned incentives over time.

Historically, security mechanisms that concentrate control and economic benefit within a single operating entity tend to expand beyond their original scope. Even systems introduced with narrow technical purposes can evolve into instruments of surveillance, coercion, or extraction when incentives favor expansion rather than restraint.

Existence Authentication explicitly acknowledges this risk.

The technical system is therefore paired with a governance constraint intended to limit extractive outcomes and align long-term incentives with public benefit. This constraint takes the form of an independent, citizen-governed mechanism known as the **Existence Development Fund (EDF)**.

Revenue generated within a jurisdiction may be partially reinvested through the EDF. Allocation authority does not reside with Existence Authentication and is not subject to discretionary control by the system operator. The EDF is governed by a separate constitution that defines eligibility, oversight, and decision-making processes.

This separation is structural, not procedural.

Existence Authentication does not control how funds are allocated, which projects are selected, or how benefits are distributed. Its role is limited to technical enforcement of presence verification. Economic benefit allocation occurs outside the technical system and is governed independently.

The purpose of this separation is preventative. By removing the ability of the system operator to directly extract or concentrate value, the governance model reduces incentives to expand enforcement scope, collect additional data, or repurpose technical signals for secondary use.

Citizen governance is not presented as a political or ideological position. It is a constraint mechanism. By placing allocation authority outside the technical operator, the model limits unilateral decision-making and creates an inspectable boundary between enforcement and benefit.

The governance framework is intentionally inspectable. The EDF Constitution defines constraints, not aspirations. Reviewers are invited to examine whether the structure meaningfully limits extractive behavior and whether it preserves proportionality over time.

Details of governance operation are not embedded in this brief to avoid conflating technical enforcement with economic administration. They are available for inspection upon written request as separate materials.

8. Inspection Pathways and Closing Statement

The following materials are available for further inspection:

- Declaration of Integrity
- Existence Development Fund (EDF) Constitution
- Executive Summary: Presence Problem / Solution
- Board and Regulator Brief

Existence Authentication is presented for inspection, not persuasion. If the model fails integrity, governance, or enforcement review, it should not be adopted.