TuringKey: Post-Quantum Behavioural-Entropy Identity Device and GDPR-Compliant Access Control System

Technical Field

The invention relates to digital identity, access control, post-quantum cryptography, lawful data-processing compliance, privacy-preserving authentication, behavioural identity modelling, secure hardware modules, personal data governance, and regulatory enforcement systems. It provides a portable cryptographic device enabling user-controlled GDPR-compliant data access.

Background

Conventional identity systems rely on biometric storage, static credentials, and server-side identity records. These create privacy risks, enable identity theft, and fail to meet evolving regulatory standards. GDPR requires data controllers to process personal data with strict transparency, minimisation, and user consent, yet current access systems cannot provide hardware-level enforcement of these principles. Existing hardware tokens lack behavioural-entropy binding, contextual attestation, coercion-detection, or fine-grained, time-limited access authorisation. There is a need for a portable identity device enabling user-controlled, regulation-compliant access tokens, secured through post-quantum cryptography and behavioural entropy without retaining sensitive behavioural data.

Summary of the Invention

The invention provides a portable identity device comprising a secure fractal-entropy hardware module, a behavioural-entropy identity engine, an attestation subsystem, and a post-quantum cryptography controller. The device generates user-specific cryptographic keys using entropy from physical variability, environmental context, and behavioural indicators. Raw behavioural data is not retained. The device produces GDPR-compliant, time-limited, read-only access tokens governed by user-approved policy logic. Tokens enable processors to access specific personal data categories for limited durations without revealing full identity material. The device includes coercion-resistance modes, PQ-secure key regeneration, zero-retention enrolment, and an internal trust engine aligned with the system of GB2520368.8.

Detailed Description

Device Overview

The device comprises:

1. A fractal-entropy secure hardware module.
2. A behavioural-entropy identity engine.
3. A device-state and environmental attestation module.
4. A post-quantum cryptography controller.
5. A GDPR policy-enforcement container.
6. A tokenisation engine generating time-limited access credentials.
7. A coercion-detection subsystem.
8. A trust-fusion engine referencing the system of GB2520368.8.

Fractal-Entropy Hardware Module

A hardware module generates non-deterministic values via fractal-entropy sampling. These values seed post-quantum key generation and provide entropy for authentication-modulation and attestation timestamps. Entropy is device-bound and cannot be exported.

Behavioural-Entropy Identity Engine

Behavioural indicators including timing micro-patterns, interaction consistency, and context-response signals are sampled. Raw data is not stored. Indicators are transformed into non-reversible behavioural-entropy values. These values contribute to cryptographic key derivation and identity verification without persisting sensitive behavioural information.

Attestation Module

The device records device-state proofs, environment signatures, temperature variability, motion signatures, and context markers. These are fused into attestation bundles required for token issuance and session authorisation.

Post-Quantum Cryptography Controller

A PQC module manages key generation, rotation, encapsulation, and signature events. Keys are derived from fractal entropy and behavioural-entropy values. Key regeneration occurs on-device and is not externally observable.

GDPR Policy-Enforcement Container

A container stores user-defined access policies. Policies define:
• permitted data categories,

• maximum access duration,
• allowed processors,
• read-only enforcement,
• retention limitations.
Tokens are generated only when policy conditions are satisfied.

Tokenisation Engine

The engine generates a time-limited, read-only authorisation token containing:
• permitted data fields,
• validity duration,
• PQ-secure signatures,
• attestation bundle,
• policy hash.
Tokens expire automatically, aligning with GDPR principles of minimisation, purpose limitation, and user-controlled access.

Coercion-Detection Subsystem

The device monitors grip pressure, tremor irregularity, temperature anomalies, movement profile deviation, and environmental changes. Detection of coercion triggers restricted-mode identity output, token suppression, or emergency revocation.

Trust-Fusion Engine

The device integrates entropy, behavioural indicators, attestation signals, anomaly factors, and key-state information to compute an internal trust value. The trust engine is aligned with the multi-layer trust-orchestration architecture of GB2520368.8.

Zero-Retention Enrolment

Enrolment occurs without storing biometric or raw behavioural material. Only non-reversible behavioural-entropy values and entropy-derived keys remain.

Operational Use

When a processor requests access, the device evaluates:
• user approval,
• policy constraints,
• trust state,
• attestation conditions,
• coercion status.
Upon approval, the device issues a read-only, PQ-signed, time-limited authorisation token. Data processors use the token without direct access to private keys or identity secrets.

Claims

Claim 1

A portable identity device comprising a fractal-entropy hardware module, a behavioural-entropy identity engine, a device-attestation module, a post-quantum cryptography controller, and a GDPR policy-enforcement container, wherein the device generates user-specific cryptographic keys without retaining raw behavioural data and issues time-limited, read-only authorisation tokens for GDPR-compliant data access.

Claim 2

The device of Claim 1 wherein the fractal-entropy hardware module produces non-deterministic values used for post-quantum key generation and token-timestamp modulation.

Claim 3

The device of Claim 1 wherein behavioural indicators are transformed into non-reversible entropy values that contribute to identity verification.

Claim 4

The device of Claim 1 wherein the post-quantum cryptography controller manages key-generation, rotation, and revocation according to trust-state changes.

Claim 5

The device of Claim 1 wherein the GDPR policy-enforcement container defines permitted data categories, allowed processors, access duration, and retention constraints.

Claim 6

The device of Claim 1 wherein the tokenisation engine generates read-only access tokens comprising permitted data fields, validity duration, a policy hash, and a post-quantum signature.

Claim 7

The device of Claim 1 wherein the attestation module provides device-state and environmental indicators incorporated into the authorisation token.

Claim 8

The device of Claim 1 wherein the coercion-detection subsystem detects grip pressure, tremor variance, temperature shifts, or contextual anomalies and suppresses token issuance.

Claim 9

The device of Claim 1 wherein an internal trust engine fuses entropy, behavioural indicators, attestation signals, anomaly indicators, and cryptographic-state information to produce a trust value regulating token issuance.

Claim 10

The device of Claim 1 implemented as a personal data-sovereignty vault enabling user-controlled identity disclosure and regulatory-compliant data-processing authorisation.

Claim 11

The device of Claim 1 wherein time-limited tokens enforce purpose limitation and data-minimisation principles for GDPR compliance.

Claim 12

The device of Claim 1 wherein the device interfaces with external processors using signed authorisation tokens without exposing identity secrets or cryptographic seed material.

Claim 13

The device of Claim 1 wherein zero-retention enrolment prevents storage of biometric or raw behavioural material.

Claim 14

The device of Claim 1 wherein authorisation tokens expire automatically and cannot be extended without renewed device authorisation.

Claim 15

The device of Claim 1 referencing the trust-orchestration architecture of GB2520368.8 as related prior art by the same inventor.

Abstract

A portable identity and access-control device implementing post-quantum cryptography, behavioural-entropy identity binding, and a zero-retention verification mechanism. The device generates and stores cryptographic material within a secure fractal-entropy hardware module and produces time-limited, read-only authorisation tokens for GDPR-compliant processing of personal data. Behavioural indicators, environmental attestation, and fractal entropy are fused to derive user-specific cryptographic keys without retaining raw behavioural or biometric data. The device enforces user-controlled policy decisions, governs access lifecycles, enables coercion-resistant authentication, and provides hardware-anchored trust for distributed systems. The invention relates to GB2520368.8 as prior art by the same inventor.