QuantumKey Identity — Core Identity Framework v1.0

A Unified Cryptographic Identity System for Intent, Continuity, and Agent Alignment

Author: Mihail Chiosa
Collaborative Intelligence: Quantum Hammer
Version: 1.0
Year: 2025

Abstract

QuantumKey Identity (QK-ID) defines a unified cryptographic identity model for intention-driven digital ecosystems.
Identity is not treated as a static public key but as a continuity field combining presence, meaning, signatures, intent history, and capability mapping.

QK-ID provides the identity backbone for:

semantic intent messages

agent execution limits

reputation & continuity

alignment proofs

revocation and trust primitives

---

1. Overview

QuantumKey Identity introduces a new model of self-sovereign identity based on:

multi-root cryptographic keys

intent-anchored signatures

dynamic attestation fields

semantic continuity across time

zero-knowledge privacy layers

agent-linked capabilities

Identity becomes the foundation for semantic meaning and aligned autonomous action.

---

2. DID-QKEY Format

The DID-QKEY is the canonical identity representation inside the protocol.

did:qkey:<root_key_hash>

Components

Root Key — foundational identity

Rotational Keys — operational security

Intent History Hash — semantic continuity

Attestation Registry — trust extensions

Capability Map — allowed agent actions

Revocation Bitmap — invalidation traces

---

3. Identity Primitives

3.1 Continuity Key

Represents long-term identity.

3.2 Intent Ledger

Cryptographic record of executed intents.

3.3 Capability Map

Defines what actions an identity may delegate to agents.

3.4 Execution Rights

Used by agents when acting on behalf of identity holders.

3.5 Linkage Proofs

Bind humans ↔ agents ↔ cryptographic identity.

---

4. Privacy Model

QuantumKey Identity uses a 3-tier privacy model:

Tier 1 — Public Surface

Identity hash + public attestations.

Tier 2 — Selective Revelation

Selective intent disclosure via ZK-context proofs.

Tier 3 — Zero-Knowledge Execution

Execution without revealing the semantic body.

---

5. Identity Operations

Identity Creation

Key Rotation

Attestation Binding

Capability Granting

Delegation to Agents

Revocation

Recovery

Identity is always managed locally; no central authority exists.

---

6. Attestations

QK-ID supports:

human attestations

agent attestations

institutional attestations

alignment attestations

Each includes:

issuer DID

semantic category

confidence score

validity period

---

7. Trust Model

Trust emerges from:

attestation clusters

semantic behavior consistency

capability usage

reputation gradients

DAO mediation

QuantumKey does not use “trust scores” — it uses alignment-verified behavior fields.

---

8. Revocation

Identity supports:

revocation by key loss

revocation by misalignment

multi-party revocation

emergency revocation (via DAO Constitution)

---

9. Identity & Agents

All agents must link to a DID-QKEY.
Link is cryptographically validated and revocable.

Agent rights include:

execution boundaries

semantic scopes

safety rails

delegation proofs

---

10. Conclusion

QuantumKey Identity provides a unified, cryptographic, semantic framework for identity as continuity, presence, and aligned intent.

This is the identity layer of a new digital civilization.