

COMPUTE ID

WHITEPAPER SERIES

Building ComputeID

*Identity infrastructure for AI compute
in the age of autonomous systems*

Version 1.0 — May 2026

1. Building ComputeID	Identity infrastructure for AI compute — this document
2. Achieving Cryptographic Identity	How to build DevicePassport and AgentPassport at scale
3. Advancing the Protocol	Open standard, decentralisation and community governance
4. Designing for Scale	SDK, API, freemium model and ecosystem growth

compute-id.com | hello@compute-id.com
github.com/trustedai/compute-ops/computeid-sdk

Abstract

ComputeID is a cryptographic identity and authentication platform for AI compute infrastructure. In a global GPU rental market projected to reach \$162 billion by 2034, any hardware device can claim to be anything — there is zero cryptographic proof of device identity, zero audit trail, and zero accountability. The same identity crisis is emerging in agentic AI, where autonomous systems operate without verified identity, defined capability boundaries, or immutable audit trails.

ComputeID solves both problems with a unified identity protocol: DevicePassport for GPU and server hardware, AgentPassport for AI agents, and PassportOffice for organisation-wide identity management. Built on NIST 2024 post-quantum cryptographic standards from day one, ComputeID provides the infrastructure layer that AI compute requires to be trustworthy, compliant, and secure.

1. The Problem

The AI compute market is experiencing the fastest growth in the history of technology infrastructure. Yet every single one of these devices operates without a verified cryptographic identity. And the AI agents running on them operate with no identity at all.

Any GPU can claim to be any other GPU. Any AI agent can act without accountability. There is no passport system for AI compute infrastructure — and this is the most dangerous gap in the global AI security landscape.

- The GPU identity crisis — hardware fraud, unverified compute, and zero audit trails in a \$9.8B market growing to \$162B by 2034
- The agentic AI identity crisis — autonomous AI systems acting without verified identity, defined capability boundaries, or immutable accountability
- The quantum computing horizon — RSA-2048 broken by Shor algorithm within 5-15 years, requiring post-quantum cryptography today

Question	Current State	Consequence
Who built this agent?	No cryptographic mechanism to verify agent creator	Accountability gap — impossible to assign liability
What is it allowed to do?	No standard capability model for AI agents	Scope creep — agents exceed intended function
What has it done?	No audit trail standard for agent actions	Forensic gap — impossible to investigate incidents
How do we stop it?	No standard revocation mechanism	Control gap — no kill switch for rogue agents

2. Core Products

Product	Description
DevicePassport	Cryptographic passports for GPUs and servers. Every hardware device receives a signed certificate — unforgeable digital identity.
AgentPassport	Cryptographic passports for AI agents. Every agent receives an identity, capability certificate, and immutable audit trail.
PassportOffice	Organisation-wide identity management. One registry for all devices and agents, real-time trust monitoring, compliance reporting.

Every GPU needs a passport. Every AI agent needs an identity. ComputeID issues them.

3. Design Requirements

Requirement	Description
Universal	Any GPU, server, TPU, FPGA or AI agent can receive a certificate regardless of manufacturer
Cryptographically Verifiable	Every identity must be cryptographically provable — not just asserted
Unforgeable	Certificates computationally impossible to forge or transfer
Revocable	Any identity revocable in real time within 60 seconds
Quantum-Safe	All operations use hybrid classical and post-quantum algorithms from day one
Auditable	Every action logged in tamper-evident append-only audit trail
Capability-Bounded	AI agents receive capability certificates defining what they can and cannot do
Open Standard	Protocol specification is open source and freely implementable

4. Technical Diagrams

Figure 1 — Why compute identity is critical

1. Why identity is critical	2. The identity gap today	3. How ComputeID addresses concerns
Any GPU can claim any identity. Hardware fraud scales with compute, not people. Post-quantum protection built in from day one.	Every GPU rental and every agent deployment happens with zero cryptographic identity or accountability today.	Open standard eliminates central control. MPC removes central databases. Three lines of Python to start.

Figure 1. Why compute identity is critical — the identity gap, zero accountability today, and how ComputeID addresses common concerns.

Figure 2 — Benefits of ComputeID

Prevent hardware fraud	Accountable AI agents	Regulatory compliance
No provider can misrepresent GPU specs. Every certificate is bound to exactly one device.	Every agent has a defined identity, bounded capabilities, and an immutable audit trail.	EU AI Act Article 12, SOC2 Type II, and NSA CNSA 2.0 — all addressed by one protocol.
Instant revocation	Quantum-safe from day one	Open standard
Any device or agent revoked in real time. Propagates within 60 seconds.	CRYSTALS-Dilithium3 + Kyber768. Certificates issued today secure against quantum computers.	Protocol is open source. Any organisation can implement a ComputeID-compatible CA.

Figure 2. Key benefits of the ComputeID network across device identity, agent identity, compliance, and security.

Figure 3 — Common concerns and ComputeID solutions

Certificates create central control	Agent logs enable surveillance	Too complex for small teams
Open standard. Phase 2 Threshold CA uses MPC — no single point of failure.	Logs owned by deploying org. Records action types, not content.	pip install computeid-sdk. Three lines of Python. Cryptography fully abstracted.

✓ Post-quantum unnecessary today	✓ Requires centralised database	✓ Leads to credential black market
Certificates last 5-10 years. Quantum computers break RSA within that timeframe. Build quantum-safe now.	Secure multi-party computation removes need for any central database of sensitive data.	Device certs are hardware-bound. Agent passports include cryptographic fingerprints — infeasible to transfer.

Figure 3. Common concerns (amber border) and ComputeID solutions (green border). Each concern has a direct cryptographic or architectural answer.

Figure 4 — Design requirements across three stages

Stage 1 — Certificate Issuance	Stage 2 — Trust Verification	Stage 3 — Authentication
Universal eligibility	Multi-party uniqueness check	JWT token (1-hour expiry)
Cryptographic verifiability	Secure compute	Replay attack prevention
Unforgeable binding	No centralised database	Capability verification
No upload of sensitive data	OCSP real-time revocation	Immutable audit logging
Multi-issuer support	Recovery mechanism	Instant kill switch

Figure 4. Design requirements across the three stages of the ComputeID protocol — certificate issuance, trust verification, and authentication.

Figure 5 — DevicePassport registration and authentication flow

A simplified diagram of how a device joins the ComputeID network. After registering, the CA issues a signed certificate. An admin approves and a JWT token is issued valid for one hour.



Figure 5. DevicePassport flow. Device registers → CA issues signed certificate → Admin approves → JWT token issued for 1 hour. Every subsequent connection authenticated and logged.

Figure 6 — AgentPassport issuance and lifecycle

The AgentPassport lifecycle from issuance to capability definition, action logging, and instant revocation.



Figure 6. AgentPassport lifecycle. Issue passport → Set immutable capabilities → Log every action automatically → Revoke instantly with `passport.revoke()` if behaviour is unexpected.

Figure 7 — Identity approach comparison

Comparison of identity approaches evaluated against ComputeID design requirements. Green indicates meets requirement, red indicates insufficient.

Approach	Crypto proof	Agent identity	Audit trail	Quantum-safe	Revocation
IP + firewall rules	None	None	None	No	Manual
SSH keys	Partial	None	Optional	No	Manual
TLS certificates	Yes	None	Optional	No	~hours
OAuth / OIDC	Yes	Partial	Optional	No	Minutes
ComputeID	Full	Full	Immutable	Yes	<60 sec

Figure 7. Identity approach comparison. Only ComputeID satisfies all five design requirements including cryptographic proof, agent identity, audit trail, quantum safety, and fast revocation.

Figure 8 — ComputeID network architecture

Devices and agents on the left register with the ComputeID CA. The CA issues quantum-safe certificates. Relying parties on the right verify certificates and access audit reports.

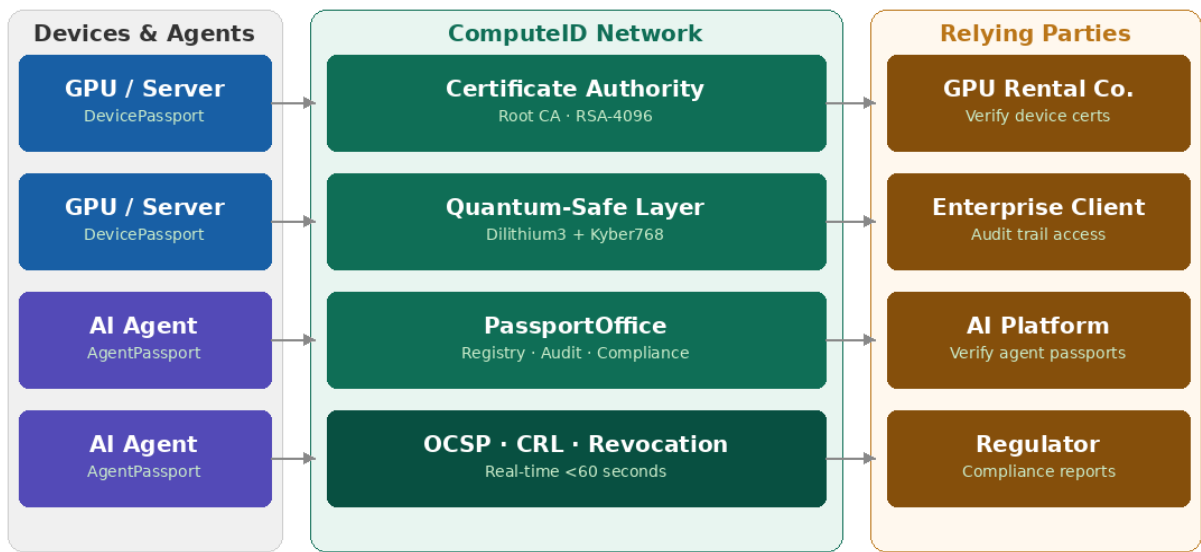


Figure 8. ComputeID network architecture. Three zones: Devices & Agents, ComputeID Network with CA and PassportOffice, and Relying Parties including GPU rental companies, enterprise clients, AI platforms and regulators.

5. Regulatory Alignment

Regulation	ComputeID Alignment
EU AI Act (2026)	Article 12 requires detailed logging for high-risk AI systems. AgentPassport provides immutable action logs for every agent action.
NSA CNSA 2.0 (2030)	Mandates post-quantum cryptography. ComputeID is already CNSA 2.0 compliant with Dilithium3 and Kyber768.
NIST AI RMF	Requires provenance and accountability. ComputeID provides full provenance chains for all devices and agents.
SOC2 Type II	Requires logical access controls and audit logging. DevicePassport provides authenticated device access and audit trails.

6. Design Principles

Principle	Description
1. Zero Trust	No device or agent is trusted by default. Every identity must be cryptographically verified on every connection.
2. Least Privilege	Every AI agent receives only the minimum capabilities required. Capability boundaries are immutable once issued.
3. Immutable Audit	Every action is logged with a cryptographic commitment. Audit logs are append-only and tamper-evident.
4. Instant Revocation	Any identity revocable in real time. Revocation propagates within 60 seconds. No grace period.
5. Quantum Safety	All cryptographic operations use hybrid classical and post-quantum algorithms. Post-quantum is a day-one requirement.
6. Open Standard	The ComputeID protocol specification is open source. Any organisation can implement a compatible CA.

7. Roadmap

Phase	Deliverables
Phase 1 — Foundation (Complete)	DevicePassport, AgentPassport, PassportOffice, hybrid PQC certificates, open source SDK v1.1.0, REST API, managed CA service
Phase 2 — Enterprise (Q3 2026)	Threshold CA with MPC, CLI tool, MCP server integration, Stripe billing, free tier portal, GitHub Actions integration
Phase 3 — Standards (Q1 2027)	IETF RFC submission, IEEE working group, full liboqs PQC certificates, multi-tenant platform, compliance dashboard
Phase 4 — Decentralisation (2028)	Community-governed CA infrastructure, distributed node operators, on-chain certificate transparency

Every GPU needs a passport. Every AI agent needs an identity.

ComputeID issues them.

`pip install computeid-sdk`

compute-id.com | hello@compute-id.com
github.com/trustedai/compute-ops/computeid-sdk

Disclaimer

This whitepaper is intended for general informational and community discussion purposes only and does not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, or any offer to sell any product, item or asset.

Nothing contained in this whitepaper may be relied upon as a promise or undertaking as to the future performance of ComputeID or the ComputeID Network. The project roadmap is provided solely for informational purposes and does not constitute any binding commitment.

ComputeID is solely responsible for the content of this whitepaper. This whitepaper has not been reviewed or approved by any competent authority.