

OCUP.AI

TEMPORAL AUTHORITY GOVERNANCE

In Hoc Una Sumus

在此同心



THE BETTER AI RACE

A CROSS-COMMUNITY BRIDGE
FOR COMPETITIVE AUTONOMY
ABOVE A SHARED FLOOR OF HUMAN SOVEREIGNTY



MAXBRUCE & GT SAGE

TEMPORAL AUTHORITY SYSTEMS PBC · BWRCI

THE BETTER AI RACE

A Cross-Community Bridge for Competitive Autonomy Above a Shared Floor of Human Sovereignty

THE PROPOSITION

Let America build. Let China build. Let every region build. Let markets reveal the best autonomous systems - but let humanity establish the boundary beneath them together.

Temporal Authority Systems PBC | OCUP.ai

Version 2.1 | October 1, 2026 | Independent discussion proposal

For consideration across WAICO, OSAA, semiconductor, infrastructure, standards, safety, insurance, and public-interest communities

Executive Thesis

This paper proposes a narrow technical area of international cooperation beneath continued competition in artificial intelligence and autonomous systems: consequential civilian machines should operate under externally governed, capability-specific, bounded authority that the governed machine cannot make itself the source of extending, restoring, or enlarging.

The proposal is not a call for one global controller. It is a proposal for a shared technical grammar through which independently governed systems can present evidence of present authority, and through which a receiving jurisdiction, infrastructure operator, or other legitimate authority domain can decide whether that evidence is sufficient under its own law, policy, risk tolerance, and operating context.

This paper uses WAICO and the Open Secure AI Alliance (OSAA) as two important but institutionally different reference communities. WAICO's founding agreement describes it as an independent intergovernmental international organization headquartered in Shanghai; representatives of 29 countries signed the agreement as founding members in July 2026. OSAA is an industry and open-source security alliance that joined the Linux Foundation in September 2026 after being originally founded by dozens of enterprise leaders and NVIDIA. They are not governmental counterparts and do not represent opposite national blocs. The bridge proposed here is therefore not WAICO-versus-OSAA diplomacy; it is parallel technical work across sovereign institutions, open technical communities, platform companies, independent standards bodies, infrastructure operators, insurers, researchers, and civil society.

The better race is not simply to deploy autonomy fastest. It is to build extraordinary capability while preserving a verifiable distinction between what a machine can do and what it is presently authorized to do.

CIVILIZATION-LEVEL RULE

Machines may exercise delegated authority, but they must not become the source of their own continued authority.

Human sovereignty, as used here, means that legitimate human institutions remain the source of consequential operational authority. It does not mean a human manually approves every machine action, nor does it guarantee that an authorized system is safe. It means that the machine does not acquire an unlimited right to continue merely because its own software, model, or operator asserts that it should.

Temporal Authority Systems PBC (TAS PBC) is developing OCUP as one technical path toward this boundary. OCUP is being developed as an integrated architecture centered on QSAFP for bounded operational-authority logic, with complementary trust, validator, and cross-domain verification layers. QVN provides a pattern for risk-weighted human and institutional authorization. RAAVE is the proposed cross-jurisdiction authority-verification architecture surrounding identity, continuity, compliance evidence, and receiving-domain evaluation. These are development architectures, not international standards or certified production infrastructure.

1. Compete Above the Boundary

Competition in models, robotics, semiconductors, energy efficiency, manufacturing, applications, cost, and performance can remain intense. The shared interest lies beneath that competition: preventing consequential machines from acquiring authority that becomes self-perpetuating simply because the machine, its local software stack, or an unauthorized operator says it should.

- Compete on capability, efficiency, reliability, price, and usefulness.
- Preserve sovereign control over models, weights, keys, validators, legal rules, and enforcement.

- Develop interoperable definitions and evidence semantics for identity, present authority, bounded duration, renewal, loss of authority, recovery, and cross-domain verification.
- Allow each jurisdiction to decide what systems are consequential, what evidence it recognizes, and what admission or operating consequences follow.

THE SHARED FLOOR

Compete above a shared floor of human sovereignty.

2. The Common Boundary

Temporal Authority Governance is a framework in which consequential machine authority is externally governed, capability-specific, bounded, and made technically consequential at an operating boundary. Its central design invariant is that the governed system must not be the source of its own continued authority.

Self-Extension Denial is the intended property that a governed system cannot itself extend, restore, enlarge, or grant the authority under which it operates. In a production implementation, loss or expiry of authority should produce denial or a pre-authorized bounded safe-degradation state; stale, replayed, reordered, or superseded approvals should not restore authority; and broader recovery should require fresh external authorization.

Temporary loss of network or validator availability should not silently become indefinite permission. A deployment may allow a pre-authorized, time-limited offline continuity window for specified low-risk functions. When that window expires, trusted continuity is lost, or required evidence cannot be preserved, the system should move to a predetermined denied or bounded safe state appropriate to the physical context.

OCUP is intended as a composition, not a monolith. QSAFP provides the bounded operational-authority logic. QVN supplies risk-weighted external authorization. A cross-cutting trust plane for time, attestation, evidence protection, device identity, and key custody is required for production deployment. RAAVE addresses verification across organizational, jurisdictional, or infrastructure boundaries.

3. What Phase I Actually Shows

Phase I hardware evidence is deliberately narrower than the architecture. On a physical AMD Kria KR260 development board, a host-driven MMIO authorization sequence produced grant and subsequent closure evidence on the defined STATUS surface. In the strongest evidentiary run, the same post-closure authorization stimulus was reasserted and confirmed by CONTROL readback; no reopen was recorded during the observation window.

That result does not establish independent external authority, trusted lease expiry, hostile-operating-system resistance, reboot continuity, signed remote attestation, production key custody, physical resource cut-off, or a valid second grant succeeding after closure. The tests used one board and one operator setup. The Phase I evidence overview therefore treats the result as register- and signal-level hardware evidence, not as proof of a complete non-bypassable production authority substrate.

The engineering direction is straightforward: move from observed authority state to non-bypassably consequential authority. That requires trusted time and continuity, protected evidence, explicit renewal behavior, fault-driven quarantine, independent authority origin, and an inline or otherwise non-bypassable hardware path that actually controls a consequential resource.

EVIDENCE RULE

Set the claim floor exactly at the evidence ceiling.

4. Identity Is Not Present Authority

Static identity and provenance can establish what a machine is, who produced it, or which credentials it possesses. They do not by themselves establish whether that machine remains authorized, now, for the capability it is attempting to exercise.

A delivery robot authorized for one city's sidewalks is not thereby authorized for another city's airport apron. A cargo system approved before maintenance is not thereby approved after a critical component substitution. A valid identity credential can survive after an operational lease has expired, after authority has been revoked, or after the operating context has materially changed.

The cross-jurisdiction rule is therefore simple: portable identity and provenance do not equal portable operational authority. A boundary crossing may require fresh evaluation by the receiving authority domain.

RAAVE is intended to address that receiving-side problem: verify evidence of identity, authority state, continuity, issuer domain, capability scope, and relevant compliance signals, then allow the receiving domain to apply its own policy. RAAVE does not issue or renew the underlying authority. A valid foreign receipt would show what another domain authorized; it would not compel the receiving domain to admit the machine or certify that the underlying decision was prudent.

5. Sovereignty-Preserving Interoperability

Interoperability does not require centralized command. Each jurisdiction may retain its own cryptographic roots, validators, legal rules, policy thresholds, risk tolerances, and enforcement mechanisms. What can cross the boundary is evidence, expressed in a shared or mutually mapped grammar.

WHAT COOPERATION DOES NOT REQUIRE

No shared models. No shared weights. No foreign control of domestic validators. No single global kill switch. No surrender of proprietary chip designs. No inclusion of military systems.

The force of such a floor comes from local admission control, not universal control over every machine. Participating ports, networks, factories, data centers, fleets, insurers, or public authorities can decide that certain consequential systems must present acceptable authority evidence before receiving access, service, insurance treatment, or permission to operate within that domain. Machines and operators outside the system still exist; the architecture does not claim to make unauthorized autonomy impossible everywhere.

An illustrative end-state example is an autonomous cargo vessel approaching a foreign port. The vessel could present a cryptographically verifiable authority receipt describing its identity, capability scope, issuing domain, validity interval, and continuity state. The receiving port could recognize it, narrow the permitted capability, require fresh authorization, impose a bounded continuity period, or deny admission under its own rules - without receiving the vessel's model weights, private keys, training data, or internal reasoning.

6. The Aviation Analogy - and Its Limits

Civil aviation offers a useful structural analogy, but not a ready-made institution for autonomous machines. An airworthiness certificate resembles identity and provenance: it establishes properties of the aircraft and can travel across borders. Air traffic control clearance is closer to present operational authority: it is contextual, time-sensitive, issued by the authority responsible for the relevant airspace, and not self-renewed by the aircraft.

The analogy also breaks in important ways. Civil aviation rests on mature treaty institutions and professional operating systems; autonomous devices may exist at vastly larger scale and can cross digital boundaries at software speed. Dual-use robotics also blurs the civil/state distinction more than aviation does. The lesson is therefore architectural, not institutional: sovereign systems can remain sovereign while recognizing interoperable evidence where they choose.

7. WAICO, OSAA, and a Wider Bridge

WAICO and OSAA should not be cast as mirror institutions. WAICO is an intergovernmental organization focused on international AI cooperation and global governance. OSAA is an industry and open-source security alliance under Linux Foundation governance. Their different structures are useful precisely because the problem spans both sovereign rule-making and implementable technical infrastructure.

WAICO participants can test whether a bounded-authority and evidence grammar is compatible with diverse sovereign requirements, including the priorities of founding states and Global South participants. OSAA and adjacent open technical communities can test interfaces, threat models, reproducible security scenarios, software and hardware integration points, and vendor-neutral implementation patterns. Semiconductor and platform companies can test where authority state becomes physically consequential. Independent standards bodies can provide neutral processes for definitions, conformance, interoperability, and intellectual-property disclosure.

The purpose is not to make either community subordinate to the other. It is to see whether independently governed systems can converge on a narrow, testable rule without converging on political control.

8. Industry Convergence Without Equivalence

NVIDIA's September 2026 Open Agent Safety Platform is a relevant convergence signal. NVIDIA describes OpenShell as a secure runtime boundary and Sentry as an out-of-band watchdog on BlueField-4 that can monitor and quarantine agents outside the agent process. The Linux Foundation describes OSAA as an industry alliance that joined the Foundation in September 2026, moving to neutral governance.

This is not the same problem addressed by Temporal Authority Governance. Runtime and sandbox enforcement constrain what an agent may do while operating. Temporal Authority asks a different question: whether the system remains legitimately authorized to exercise a consequential capability at all, for how long, and under whose externally governed renewal. The two approaches may be complementary; no endorsement, affiliation, technical equivalence, or partnership with NVIDIA, OSAA, the Linux Foundation, or WAICO is implied.

9. Global South and Multipolar Relevance

The autonomous era will not be built by two countries alone. Many jurisdictions will deploy mixed hardware, cloud, robotics, and infrastructure supply chains and will not want basic safety verification to require choosing one geopolitical technology bloc.

A genuinely multipolar evidence grammar must therefore be implementable without forcing a jurisdiction to surrender its trust roots, law, private keys, models, or policy discretion. It should also be practical for lower-resource jurisdictions: open verification tooling, shared conformance suites, capacity-building, reference implementations, and auditable interoperability services may be as important as the formal specification itself. Otherwise, nominal sovereignty could become dependence on whichever vendor can afford the verification stack.

10. Human Sovereignty and Autonomous Abundance

If autonomous systems generate extraordinary productivity while reducing demand for conventional labor, governance itself may become one area in which human responsibility remains economically relevant. This is not a promise that governance work will replace jobs displaced by automation.

QVN - Quorum Validators Network - is conceived as a multi-level trained-responder model, not click-to-approve micro-labor. Routine, low-risk decisions may be automated or delegated within policy. Initial grants, elevated capabilities, exceptions, quarantine release, recovery, or other high-consequence decisions can escalate to appropriately trained people and institutions according to risk, jurisdiction, and responsibility.

In future implementations, some validation, assurance, certification, or operating functions may support compensated human and institutional work. Any such mechanism would need safeguards against rubber-stamping, collusion, conflicts of interest, inequitable access, and incentive designs that reward approval volume over sound judgment.

THE ABUNDANCE PRINCIPLE

Machines may create abundance, but legitimate machine authority should remain rooted in people and human institutions.

This is a long-term design direction, not a present commercial deliverable, guaranteed economic outcome, tax on automation, or proposal for a centralized global validator.

11. A Practical Cooperation Ladder

1. Independent review of the invariant. Invite WAICO participants, OSAA/open technical communities, semiconductor and platform companies, researchers, regulators, infrastructure operators, insurers, and safety organizations to challenge the non-self-authorization rule against their own architectures and threat models.
2. Shared definitions and threat models. Define consequential systems, authority, lease, expiry, renewal, Self-Extension Denial, identity continuity, validator failure, hostile-host behavior, recovery, evidence requirements, and boundary conditions.
3. Open conformance scenarios. Publish reproducible tests for expiry, quorum loss, replay, unauthorized renewal, legitimate renewal, component replacement, cloning, bypass, fault-driven isolation, degraded operation, silence, and recovery.

4. Evidence grammar. Define a vendor-neutral schema for identity, authority scope, issuer domain, validity, continuity, evidence provenance, revocation, and receiving-domain disposition. Treat trust-root recognition and policy mapping as governance decisions, not hidden technical assumptions.
5. Reference implementations. Support open software interfaces and multiple hardware reference paths, including QSAFP-centered OCUP work, while allowing sovereign and vendor-specific implementations.
6. Independent evaluation. Reproduce evidence across boards, labs, institutions, and implementations before production-readiness claims.
7. Neutral standards pathways. Advance validated definitions, conformance tests, and interoperability requirements through appropriate national and international standards bodies, with early IPR disclosure and appropriate FRAND treatment where patented technology becomes standard-essential.
8. Deployment and insurance learning. Test how verifiable authority evidence can inform local infrastructure admission, procurement, certification, underwriting, and incident accountability without implying that one technical credential substitutes for legal or safety judgment.

12. Development and Claims Boundary

The current OCUP program includes software reference work, deterministic evidence scenarios, FPGA reference testing, and a growing claims-boundary discipline. Phase I KR260 evidence supports a narrow hardware result: host-driven grant and closure evidence was recorded on the defined STATUS surface, and post-closure reassertion of the same authorization stimulus did not produce a recorded reopen during the observation window. That result is useful, but it is not the production architecture described in this paper.

Production realization still requires trusted monotonic time and state continuity; secure key custody; authenticated firmware and rollback protection; device-bound roots of trust; signed and remotely attestable evidence; stronger hostile-OS and alternate-path bypass resistance; qualified validator governance; safe physical degradation; and FPGA, embedded-controller, chiplet, or silicon integration that actually gates consequential resources.

Secure elements and trusted execution environments can protect keys, measurements, and evidence, but they do not by themselves create a non-bypassable authority boundary. The controlled resource path must remain outside the governed workload's exclusive control. Achieving and independently validating that condition is an explicit engineering objective, not a completed Phase I result.

The goal is collaboration to define the invariant, build the evidence path, solve the cross-layer integration problems, accumulate the validation history, and help shape the standards around it.

13. The First Ask

The immediate proposal is deliberately smaller than adoption. TAS PBC can bring three concrete items into an exploratory technical review: an initial conformance-scenario framework, the bounded software control-plane work, and the sealed Phase I KR260 evidence package with its limitations stated explicitly.

The first meeting should not ask participants to endorse OCUP, QVN, RAAVE, or a global standard. It should ask whether the underlying invariant is worth testing across independent architectures, and what evidence would be required before any participant would rely on it.

14. The Invitation

The world does not need one authority controlling all machines. It needs clearer technical ways for legitimate authorities to determine whether consequential machines remain within the authority they were actually given.

The invitation is therefore to pursue parallel, reviewable work across sovereign institutions, open technical communities, semiconductor and platform companies, infrastructure operators, researchers, insurers, and standards bodies: define the invariant, test the failure modes, build the evidence grammar, compare independent implementations, and let standards emerge from reproducible results rather than geopolitical rhetoric.

THE BETTER FINISH LINE

Build the most capable autonomous future - but build it so the machine does not become the source of its own authority, and so legitimate human institutions remain able to verify and govern consequential operation.

Let America go deep. Let China go deep. Let every region build boldly. The autonomous era can remain competitive without requiring a single controller beneath it. The shared opportunity is narrower and more practical: preserve sovereign competition above a verifiable floor of human authority.

Working Definitions

Temporal Authority Governance. A framework in which consequential machine authority is externally governed, capability-specific, bounded, non-self-extensible, and made technically consequential at an operating boundary.

Temporal Authority. The bounded authority granted to a machine or component for a defined capability, period, and operating context.

Human sovereignty. The principle that legitimate human institutions remain the source of consequential operational authority, even when machines act autonomously within that delegated authority.

OCUP. One Chip Unified Protocol; the proposed integrated operating architecture centered on QSAFP bounded-authority logic with supporting trust, validator, and verification layers. The name does not require every architectural function to reside on one physical die.

QSAFP. The planned open-core authority logic for bounded grants, lifecycle state, quorum/freshness logic, and the non-self-extension invariant.

Self-Extension Denial. The intended property that a governed system cannot itself extend, restore, enlarge, or grant the authority under which it operates.

QVN. Quorum Validators Network; a multi-level trained-responder pattern for external authorization, renewal, exceptions, recovery, and other risk-weighted governance decisions.

RAAVE. The proposed cross-jurisdiction authority-verification architecture for evaluating identity, continuity, evidence, compliance signals, and receiving-domain eligibility without issuing or renewing the underlying authority.

Context, Independence, and Sources

Temporal Authority Systems PBC submits this paper independently. No endorsement, participation, affiliation, technical equivalence, or formal relationship with WAICO, OSAA, the Linux Foundation, NVIDIA, AMD, or any governmental body is implied. This is a public discussion draft, not legal advice, a safety certification, a standards declaration, or a representation of any government's policy.

Current institutional descriptions in this revision were checked against official public sources available October 1, 2026. Technical statements about OCUP Phase I are bounded by the project's sealed evidence records and the separately reviewed Phase I Hardware Evidence overview.

Sources & Notes

1. Ministry of Foreign Affairs of the People's Republic of China, 'Signing Ceremony of the Agreement on the Establishment of the World Artificial Intelligence Cooperation Organization Held in Shanghai,' July 16, 2026. Describes WAICO as an independent intergovernmental international organization headquartered in Shanghai and states that representatives of 29 countries signed as founding members.
2. The Linux Foundation, 'Open Secure AI Alliance Joins the Linux Foundation to Build a Shared, Open Defense Stack for the AI Era,' September 14, 2026. Describes OSAA as originally founded by dozens of enterprise leaders and NVIDIA, and as joining the Linux Foundation to move to neutral governance.
3. NVIDIA, 'NVIDIA Launches Open Agent Safety Platform to Secure Agents From Testing to Deployment,' September 28, 2026. Describes OpenShell as a secure runtime boundary and Sentry as an out-of-band watchdog on BlueField-4, with hardware-based monitoring and quarantine.
4. Temporal Authority Systems PBC, 'Phase I Hardware Evidence,' October 1, 2026. Internal evidence overview based on sealed KR260 run records; explicitly not an independent reproduction.