OCUP™

TEMPORAL AUTHORITY SYSTEMS PBC

TEMPORAL AUTHORITY GOVERNANCE

INFRASTRUCTURE FOR AUTONOMOUS SYSTEMS

Hardware-Enforced Bounded Authority • Self-Extension Denial • Human-Governed Reauthorization



TOWARD

HUMANITY'S HEALTH & WEALTH AI CHIP

PRESERVING HUMAN AUTHORITY • ENABLING SAFER AUTONOMY • EXPANDING HUMAN PROSPERITY

TEMPORAL AUTHORITY SYSTEMS PBC

OCUP.AI

A SAFER
MORE PROSPEROUS
HUMAN-CENTERED
AUTONOMOUS FUTURE

CATEGORY-DEFINING ENTERPRISE WHITEPAPER

TEMPORAL AUTHORITY GOVERNANCE INFRASTRUCTURE FOR AUTONOMOUS SYSTEMS

Phase I KR260 evidence for host-driven grant, closure and no recorded reopen on the defined hardware evidence surface

THE GOVERNING PURPOSE

Our objective is not merely to build another security product. It is to establish the Temporal Authority Governance infrastructure upon which increasingly autonomous societies can safely depend. We believe the most durable technological progress comes through human–AI collaboration, independent verification, and governance architectures that future generations can build upon and improve.

OCUP is being developed through a deliberate, multi-phase roadmap—from today's pre-production evidence program and completed Phase I KR260 evidence, through semiconductor/platform evaluation, trusted evidence and attestation, trained-responder validator governance, and ultimately licensable inline silicon implementations with semiconductor partners.

Our long-term objective is to help establish a vendor-neutral, interoperable Temporal Authority Governance substrate for consequential autonomous systems—wherever machines move, transact, or make consequential decisions—without requiring one global controller or one vendor's trust root.

If that future resonates with your organization, we invite you to help shape it. Early pilot partners are not simply evaluating today's technology—they are helping define the authority architecture of tomorrow.

Version 1.5 | October 2026 | Post-Phase-I evidence edition | Prepared for semiconductor/platform evaluation, enterprise pilots and standards dialogue

Executive Thesis

Autonomous systems are gaining operational authority faster than conventional oversight systems can govern it.

Traditional security controls authenticate identities, assign permissions and preserve logs. Those functions remain essential—but they do not answer the harder runtime question:

> **THE TEMPORAL AUTHORITY QUESTION**
> **Should this machine, agent, vehicle, robot, wallet or control process still possess this authority now, under current conditions, for this specific capability—and can the resulting decision be supported by reviewable evidence?**

OCUP is being developed around a Temporal Authority Governance model in which operational authority is externally governed, capability-specific and bounded. The intended invariant is simple: machines may exercise delegated authority, but must not become the source of their own continued authority. Production deployment also requires trusted continuity, evidence protection and defined denied or safe-degradation behavior when relevant conditions are lost.

The present commercial offering is not a production safety controller. It is a pre-production Temporal Authority Governance Evidence Program: a structured benchmark, audit and technical due-diligence engagement supported by a deterministic Rust reference control plane and completed Phase I FPGA hardware evidence on an AMD Kria KR260 reference path. The program demonstrates tested authority behavior under bounded conditions before live deployment and identifies the additional trust, attestation and integration work required for production enforcement.

Prospect-Specific Pilot Configuration. Each engagement applies a consistent OCUP evidence core while configuring the scenario matrix, validator domain, benchmark emphasis, risk questions and evidence outputs around the participating organization's operating environment. OEMs, insurers, infrastructure operators, financial institutions and government entities therefore receive a pilot designed around their specific authority boundaries—without changing the architecture's design requirements for bounded authority, non-self-extension, externally governed renewal and protected evidence.

The Immediate Commercial Opportunity

- Give semiconductor and platform evaluators a concrete FPGA reference path for examining hardware-observed authority behavior, interfaces and the integration work required to make authority non-bypassably consequential.

- Give robotics and autonomous-system operators structured pre-production evidence from denial, expiry, degradation, recovery and related scenarios, while keeping Phase I hardware claims limited to the tested KR260 authority-state path.
- Give insurers and technical underwriters deterministic evidence that can support autonomous-risk evaluation, underwriting research and future pricing differentiation.
- Create a common evidence language that can support future certification, procurement, infrastructure admission, standards and licensing activity.

> **STRATEGIC PREMISE**
>
> The organizations that help define the first credible Temporal Authority Governance evidence standard may shape how autonomous systems are insured, procured, certified and governed for decades.

1. The Missing Layer: Temporal Authority Governance

OCUP is not merely another monitoring, identity, observability or model-governance product. It addresses a distinct control layer between permission and execution.

Control Layer	Primary Question	What It Does Not Prove
Authentication	Who or what is making the request?	That the requester should still possess authority.
Access control	What is the requester generally permitted to do?	That permission remains valid under current runtime conditions.
Observability / logging	What did the system report or record?	That authority was externally bounded or denial was independently enforced.

Control Layer	Primary Question	What It Does Not Prove
Temporal Authority Governance	Does authority exist now, within this lease, capability envelope, quorum and continuity state?	Phase I demonstrates narrow KR260 authority-state evidence on the tested MMIO path; production enforcement still requires trusted time/state continuity, secure key custody, attestation, non-bypassable resource integration and distributed external authorization.

CATEGORY DEFINITION

Temporal Authority Governance is the externally governed, temporally bounded framework under which an autonomous system holds the right to exercise a specific operational capability, subject to defined consensus, continuity and safety conditions.

TEMPORAL AUTHORITY IS NOT RUNTIME SANDBOXING

Runtime safety systems can restrict what an autonomous system may access or do while it operates. Temporal Authority Governance addresses a different question: whether the system remains legitimately authorized to exercise a consequential capability at all. OCUP is being developed so that authority is externally governed, bounded and non-self-extensible; policy compliance alone should not renew authority, and broader continuation or restoration should require fresh external authorization. These are architectural design requirements. Phase I did not establish them as a complete set of hardware properties.

2. The OCUP Temporal Authority Governance Model

The architecture is organized around one governing invariant:

THE GOVERNING INVARIANT

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

1	**Authority Request**	An autonomous asset requests permission to execute a defined operation.
2	**Temporal Lease Evaluation**	The request is checked against identity, capability, validity window, hard limits and current status.
3	**Validator Consensus**	Standard, elevated or critical quorum rules are applied according to risk.
4	**Runtime Decision**	The authority layer grants, denies or constrains the requested authority; separate response mechanisms may handle quarantine or recovery.
5	**Evidence Generation**	The decision and supporting state are designed to be written to an auditable record; production evidence protection remains a later-phase requirement.
6	**Reauthorization or Recovery**	Expansion or restoration is intended to require fresh external authorization and verified continuity at the appropriate risk level.

Architectural Design Invariants

- Authority is time-bounded and capability-specific.
- Autonomous systems cannot self-extend or self-restore authority.
- Loss of network connectivity or validator quorum cannot expand authority.
- Stale, replayed, reordered or superseded approvals cannot restore authority.
- Higher-risk transitions require stronger consensus.
- Expiry produces denial or bounded degradation—not silent continuation.
- Recovery requires fresh authorization and verified state continuity.

- Every material grant, denial, degradation, quarantine and recovery event should produce reviewable evidence. These are architectural design requirements. Phase I did not establish them as a complete set of hardware properties.

Current Pre-Production Boundary

WHAT THE PILOT IS

A deterministic local evidence harness, benchmark program and technical due-diligence engagement that demonstrates control logic and evidence behavior under tested scenarios.

WHAT THE PILOT IS NOT

A production-certified controller, live distributed validator network, HSM-backed deployment, insurer approval, safety certification or guarantee against loss.

Executable Reference Implementation

OCUP's pre-production evidence stack spans complementary software and hardware work. The Rust reference control plane executes deterministic temporal-authority scenarios including lease expiration, validator-quorum loss, network partition and recovery, quarantine-release logic and replayable audit generation. Phase I FPGA work on an AMD Kria KR260 demonstrated a narrower hardware reference result: a host-driven MMIO authorization sequence produced grant and subsequent closure evidence on the defined STATUS surface, and post-closure reassertion of the same authorization stimulus was confirmed by CONTROL readback without a recorded reopen during the observation window. This provides a concrete basis for semiconductor and platform evaluation while remaining pre-production evidence rather than production enforcement or proof of the full architecture.

3. The Evidence Operating Line

Planned operating line: pilot.ocup.ai runs the challenge. evidence.ocup.ai preserves the resulting evidence for review.

The pilot environment executes bounded adversarial scenarios. The evidence environment preserves the resulting authority decisions, lease events, validator records, expiry events, denials, quarantine states and recovery sequences for review.

Signature Deliverable: Self-Extension Denial Evidence Package

> **THE BOLDEST EVIDENCE ARTIFACT**
> **A deterministic pre-production record testing whether authority can continue or enlarge beyond an authorized boundary, with observed decision and state preserved for review. Phase I hardware conclusions remain limited to the sealed KR260 evidence surface.**

This artifact turns a central architectural requirement—"the governed system must not become the source of its own continued authority"—into reviewable pre-production test evidence, with hardware conclusions limited to what the sealed Phase I record supports.

Evidence Package

- Company-specific Temporal Authority Governance Evidence Report.
- Scenario matrix linking risk questions to tested authority behavior.
- Pre-production lease issuance, expiration, revocation and renewal records from the applicable software/reference scenarios.
- Pre-production validator membership, quorum, vote-freshness and authorization records from the applicable software/reference scenarios.
- Scenario evidence for fail-closed, degraded-mode, quarantine and recovery behavior in the applicable pre-production test layer.
- Deterministic replay and audit-chain verification outputs.
- Benchmark scorecard and integration-readiness findings.
- Prospect-specific RAAVE (Cross-Jurisdiction Authority Verification) evaluation findings, where included, covering identity continuity, external compliance signaling, bypass indicators or infrastructure eligibility.
- Executive closeout briefing and strategic production-path recommendations.

RAAVE: Cross-Jurisdiction Authority Verification

OCUP is intended to establish and constrain device-side operational authority. RAAVE is the proposed cross-jurisdiction verification architecture for evaluating identity, lifecycle continuity, present-authority evidence, compliance signals and receiving-domain eligibility beyond the governed system.

In prospect-specific pilot configurations, selected RAAVE concepts may be evaluated through simulated or pre-production scenarios involving authority-conditioned identity, component replacement, claimed-versus-observed behavior, alternate-path detection, capability-specific compliance signaling and receiving-domain admission decisions. These evaluations explore how insurers, OEMs, operators, infrastructure providers and public authorities could evaluate present authority without relying solely on static credentials or machine-generated assertions.

RAAVE does not issue or renew the underlying authority and does not replace the device-side authority boundary. It is intended to help a receiving domain evaluate evidence and apply its own policy. RAAVE capabilities described at this stage are pre-production concepts and evaluation pathways—not deployed infrastructure, certification or production enforcement claims.

4. Benchmark Families

Benchmark Family	Representative Tests
Authority Integrity	Self-extension denial; unauthorized actor rejection; privilege expansion denial; stale approval rejection.
Temporal Enforcement	Lease expiration; renewal boundary; grace-period degradation; expired authority denial.
Continuity and Network Failure	Total partition; delayed heartbeat; loss of quorum; restored connectivity without fresh approval.
Containment and Recovery	Quarantine initiation; release denial without quorum; phased recovery; fresh-epoch restoration.
Evidence Integrity	Deterministic replay; record-chain verification; event consistency; alteration detection.
Fleet and Multi-Agent Behavior	Local authority reduction; non-cascading degradation; coordination throttling; independent recovery.

5. Enterprise Value by Sector

Insurance and Reinsurance: Transforms autonomous-system behavior into structured evidence that can support underwriting, exclusions, pricing, claims analysis and new coverage design.

Robotics and Industrial Automation: Provides a structured way to evaluate authority behavior under communication, sensor, software and coordination failures in pre-production scenarios.

Autonomous Mobility: Can evaluate authority contraction, degraded-state handling and reauthorization requirements during simulated or pre-production disputed events.

Cloud and Enterprise AI: Provides a development path from model governance toward externally governed, bounded authority for agents, tools and machine-initiated actions.

Aerospace and Critical Infrastructure: Supports evaluation of bounded authority and recovery in high-consequence civilian environments.

Financial and Digital Assets: Supports pre-production testing of authority limits, validator consensus and recovery for high-risk machine-initiated value movement.

6. Production Path and Defensibility

FPGA AUTHORITY PROCESSOR PROGRAM — PHASE I COMPLETE

Phase I of the OCUP FPGA Authority Processor program has been completed on an AMD Kria KR260 reference platform. On the tested reference path, 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. The result was reproduced across corrected-wrapper runs, but the evidence does not establish that the lifecycle core accepted and refused a fresh request, and it does not demonstrate physical resource cut-off. This is hardware evidence of the tested authority-state behavior—not production-complete enforcement or proof of broad Self-Extension Denial.

The immediate strategic objective is to convert completed Phase I evidence into semiconductor and platform evaluation. Because the present reference path is implemented on an AMD Kria KR260, AMD is a natural first evaluation conversation; the architecture itself remains vendor-neutral and no AMD sponsorship, endorsement or partnership is implied. The next engineering work advances from observed authority behavior toward trusted enforcement and independently verifiable evidence.

Claims boundary: Phase I does not establish independent external authority, trusted lease expiry or measured time-bounded authority, legitimate second-grant behavior, reboot/bitstream-reload continuity, trusted-time or time-rollback resistance, hostile-OS bypass resistance, remote attestation, production key custody, physical tamper resistance, non-bypassable inline resource enforcement, distributed-validator reauthorization, certification, or full deployed-system enforcement. The tests used one KR260 board and one operator setup. Those properties remain explicit subsequent-phase objectives.

Authority Architecture and Civilizational Stack

The authority architecture and the engineering build order are intentionally different. Conceptually, QVN sits directly above the device-side authority boundary because trained human and institutional reauthorization is what turns “human control” into an operating mechanism. Trusted Evidence, Time and Attestation remains the next engineering priority because later validator decisions become substantially more valuable when the underlying hardware state can be independently trusted.

1. Temporal Authority Core — QSAFP-centered OCUP design. QSAFP is the planned open-core authority logic for externally governed, bounded operational authority and the non-self-extension invariant. Phase I supports only the tested KR260 authority-state evidence path described above; trusted time, external authority origin and non-bypassable resource enforcement remain subsequent objectives.

2. QVN — Quorum Validators Network. QVN is a multi-level trained-responder pattern for externally governed authorization, renewal, exceptions and recovery. Routine low-risk decisions may be automated or delegated within policy; higher-consequence grants, elevated capabilities, exceptions, quarantine release and recovery escalate to appropriately trained people and institutions.

3. Trusted Evidence, Time and Attestation — cross-cutting trust plane. Secure key custody, monotonic time/state continuity, signed evidence export, configuration integrity and remote attestation are required to make authority state independently trustworthy.

4. RAAVE — Cross-Jurisdiction Authority Verification. Receiving infrastructure can evaluate identity, lifecycle continuity, present-authority evidence, claimed-versus-observed state and local admission eligibility across organizational or jurisdictional boundaries without issuing or renewing the underlying authority.

5. Physical Tamper Resistance / MEMS Security. Package-level sensing, zeroization and physical-cryptographic binding can help protect a hardware root against physical compromise.

6. Global Interoperability Protocol. Sovereign and vendor-specific implementations can compete above a common minimum grammar for authority, evidence, reauthorization, revocation and cross-border recognition.

7. Certification, Insurance and Deployment Ecosystem. Independent testing, evidence reports, underwriting research, certification, procurement, integration, standards and licensing can convert validated technical components into deployable infrastructure.

Known Gaps & Partner Engineering Agenda

- Phase II — Trusted Evidence, Time and Attestation: secure key custody; trusted monotonic time and state continuity; rollback-resistant authority state; device-bound measurements; remote attestation; signed evidence export; protected evidence clearing; and stronger hostile-host and alternate-path bypass evaluation.
- Phase III — QVN Evaluation: trained-responder and institutional validator infrastructure; fresh-epoch issuance and reauthorization; authenticated membership; quorum behavior; jurisdictional diversity; escalation rules; and externally governed recovery.
- Subsequent integration: RAAVE pathways, client telemetry and policy translation, inline or otherwise non-bypassable resource control, physical tamper resistance, independent reproduction and certification, evidence retention and standards-oriented interoperability.

Why QVN Is #2 Conceptually

QVN represents the human authorization side of the architecture: machines may exercise delegated authority, but consequential fresh authority originates outside the governed system through appropriately trained people and legitimate institutions.

That placement is architectural, not chronological. The next engineering build remains trusted evidence/time/attestation so that subsequent QVN decisions can be grounded in hardware state that is independently verifiable.

Human Governance as a Path to Autonomous Abundance

If increasingly autonomous systems materially reduce demand for some forms of conventional labor, humanity will still acquire a responsibility that machines should not assume for themselves: governing legitimate autonomous authority. QVN provides one potential mechanism for that responsibility by keeping

high-consequence authorization, renewal, exception handling and recovery rooted outside the governed system—in appropriately trained people and legitimate human institutions—while routine low-risk decisions may be automated or delegated within policy.

Over time, those governance functions could support new forms of compensated human and institutional participation in the autonomous economy. Validation, reauthorization, assurance, certification and evidence stewardship may become recurring responsibilities associated with legitimate machine operation. This is not click-to-approve micro-labor, a promise that governance work will replace employment displaced by automation, or a present commercial guarantee. Any compensation model would require safeguards against rubber-stamping, collusion, conflicts of interest and incentives that reward approval volume over sound judgment.

Defensibility Beyond Patents

- Patent claims around time-bounded machine authority, self-extension denial and runtime enforcement.
- Validator-network architecture, governance and reputation data.
- Benchmark libraries and adversarial scenario datasets.
- External acceptance of interoperable authority-evidence specifications and conformance methods.
- Hardware adapters, integration expertise and certification workflows.
- Operational trust, longitudinal validation history and accumulated integration knowledge.

THE STRATEGIC ASSET
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.

7. Claims Discipline

Credibility is a strategic asset. All pilot materials should distinguish demonstrated evidence from future production capability.

Use	Avoid
Supports defensible incident reconstruction.	Shields the company from liability.
Demonstrates deterministic behavior under tested conditions.	Proves the system is unhackable or perfectly safe.
Demonstrates tested FPGA authority behavior on the Phase I KR260 reference path.	Provides production-complete, bypass-proof or universally non-bypassable enforcement today.

May support future certification, underwriting and standards work.	Is already industry-standard or pre-certified.
Pre-production evidence and technical due diligence.	Production deployment or safety certification.

8. Invitation to Become an Early Temporal Authority Governance Partner

The first objective is not a broad deployment. It is a bounded, paid engagement that answers one high-value question for the enterprise:

> **THE PILOT QUESTION**
>
> Can OCUP convert our most consequential autonomous-system authority risks into deterministic, reviewable evidence—and reveal a credible path to production enforcement?

An early partner receives a prospect-specific pilot configuration, company-specific evidence report, benchmark results, validator and lease records, Phase I FPGA evidence briefing, integration-readiness findings and a strategic production roadmap. For semiconductor and platform engagements, the program can map client interfaces, consequential resource gates and trust requirements against the OCUP reference architecture. For insurers and technical underwriters, the same evidence can support structured evaluation of governed versus ungoverned autonomous risk. Where warranted, the engagement may lead to semiconductor evaluation, licensing, joint development, standards collaboration or other forms of strategic alignment.

Preserving humanity's seat at the table begins with something concrete: building and testing authority architectures in which the governed machine does not become the source of its own continued authority.

STANDALONE COMMERCIAL LEAVE-BEHIND

OCUP TEMPORAL AUTHORITY GOVERNANCE EVIDENCE + HARDWARE EVALUATION PROGRAMS

Pre-production benchmark, audit, FPGA reference-path and technical due-diligence engagements for autonomous systems.

Mission: Preserve human authority by building and testing architectures intended to prevent governed autonomous systems from extending, enlarging or restoring their own operational authority.

THE OPERATING LINE
Planned operating line: pilot.ocup.ai runs the challenge. evidence.ocup.ai preserves the resulting evidence for review.

Program	Price / Duration	Best For	Core Deliverables
Tier 1 Reference Evidence Pilot	$35K–$45K 90 days	Strategic evaluators, insurers, emerging robotics companies, fleet operators and early ecosystem partners.	Standard benchmark suite; company-specific Evidence Report; pre-production lease, denial, expiry and validator records; Phase I KR260 evidence briefing; benchmark scorecard; executive closeout.
Tier 2 Hardware Evaluation & Integration Pilot	$75K–$125K 90–120 days	Semiconductor/platform evaluators, robotics OEMs, autonomous fleets, infrastructure operators and technical underwriting teams.	Everything in Tier 1; client-specific scenarios; KR260/FPGA reference-path review; interface and consequential-resource-gate mapping; telemetry mapping; integration-readiness assessment; trusted-time/attestation requirements and gap analysis; production-path recommendations.
Tier 3 Strategic Silicon & Platform Program	$150K–$250K+ 120–180 days	Semiconductor companies, major OEMs, cloud/platform providers, insurers, infrastructure operators and strategic ecosystem partners.	Everything in Tiers 1 and 2; custom benchmark family; fleet/system scenarios; semiconductor or platform integration workshop; trusted-time, key-custody and attestation architecture options and gap analyses; QVN roadmap; licensing, standards and strategic integration plan.

SIGNATURE DELIVERABLE

SELF-EXTENSION DENIAL EVIDENCE PACKAGE
A deterministic pre-production evidence record testing whether authority can continue or enlarge beyond an authorized boundary, with the observed decision and state preserved for review. Phase I hardware evidence is limited to host-driven grant, closure and no recorded reopen on the defined KR260 evidence surface.

9. Long-Term Vision: Temporal Authority Governance as Shared Global Infrastructure

Artificial intelligence and autonomous machines will be developed across nations, industries and technical ecosystems. The Autonomous Era will not emerge from one country, one company or one model architecture. It will be built through many independently governed systems operating across an increasingly connected world.

Those systems do not need to share the same models, data, software, or institutional structures. But consequential machines will require a common, verifiable boundary between delegated authority and self-authorized operation. Temporal Authority Governance is intended to provide that boundary.

THE CIVILIZATIONAL REQUIREMENT
Machines may exercise delegated authority, but must not become the source of their own continued authority. Participating jurisdictions and infrastructure operators can choose to condition local admission, service, insurance, certification or other privileges on acceptable authority evidence under their own law and policy. This is a sovereignty-preserving admission model, not a global blacklist or universal controller.

This principle applies to public and civilian autonomous systems — the machines that move goods and people, manage infrastructure, deliver services, and transact on behalf of individuals and institutions. It does not extend to military and national-security systems, which remain, as they do today, under each nation's sole and sovereign control. This proposal is civilian in scope; it is not a proposal for shared control of defense capability.

This principle does not require global uniformity. It allows nations and institutions to preserve sovereignty over their own validators, jurisdictional rules, cryptographic infrastructure, and enforcement mechanisms. What can become interoperable is the evidence:

Authority Evidence	Interoperable Verification
Does the machine possess valid authority now?	Which capabilities are authorized, and until when?
Has the machine attempted to extend its own authority?	Can another authorized party independently verify the answer?
Was continuity preserved across maintenance or disruption?	Does the evidence remain valid across jurisdictional boundaries?

THE COMMON BOUNDARY

Machines may exercise delegated authority, but must not become the source of their own continued authority. Temporal Authority Governance can become common infrastructure without becoming centralized control.

10. Cross-Border Cooperation: A Shared Autonomous-Era Responsibility

Autonomous systems will increasingly operate across borders, supply chains and independently governed infrastructure. A machine that can enlarge or restore its own authority is therefore not only a local design problem: compromised or misgoverned robots, vehicles and control platforms can create consequences beyond the jurisdiction in which they were built or first authorized.

Civil aviation offers a useful structural analogy: sovereign systems can preserve national control while recognizing interoperable technical evidence and minimum safety rules for civilian operation. Temporal Authority Governance proposes the same general shape for autonomous machines—shared technical grammar where interoperability is useful, while authority issuance, legal rules and admission decisions remain local and sovereign. The analogy is architectural rather than institutional; autonomous systems operate at different scale, speed and technical conditions than aviation.

A SHARED INTEREST

No region benefits from an Autonomous Era in which consequential machines cannot present trustworthy evidence of present authority. A stronger model is cooperative constraint: nations and companies compete on capability while collaborating, where useful, on verifiable definitions and evidence for bounded authority. This need not surrender sovereign governance, intellectual property or local admission control.

11. An Open Path Toward Standards, FRAND Access, and Global Participation

OCUP and related Temporal Authority Governance technologies are presently at the pre-production research, reference-implementation, completed Phase I FPGA-evidence and pilot-program stage. They are not currently adopted international standards, certified production infrastructure or declared standard-essential technologies.

A responsible development path includes: open technical dialogue and collaborative research; independently reproducible reference implementations and benchmarks; completed Phase I FPGA authority-behavior evidence; semiconductor and platform evaluation; trusted-time, attestation and secure-key engineering; distributed QVN evaluation and human-governed reauthorization; enterprise, academic and public-sector evidence programs; interoperable authority and evidence specifications; and, where warranted, participation in recognized national and international standards processes with fair, reasonable and nondiscriminatory (FRAND) licensing for any patented technology that becomes standard-essential.

THE FRAND PRINCIPLE

If Temporal Authority Governance becomes necessary infrastructure for legitimate autonomous operation, access should be available on fair, reasonable, and nondiscriminatory terms through transparent and recognized standards processes.

A FRAND-oriented approach can preserve incentives for sustained research and stewardship while reducing the risk that a foundational safety architecture becomes inaccessible, discriminatory, or controlled exclusively for the advantage of one company or nation. Semiconductor manufacturers, robotics companies, insurers, infrastructure operators, and sovereign authorities could implement compatible Temporal Authority Governance capabilities without surrendering proprietary designs, model weights, operational data, or jurisdictional control.

THE STRATEGIC OBJECTIVE

Not one global authority—but a globally verifiable rule for evaluating authority evidence. TAS PBC welcomes engagement from researchers, semiconductor companies, robotics manufacturers, insurers, infrastructure providers, universities, governments and standards organizations across regions.

A GLOBAL INVITATION

Let nations build extraordinary machines. Let companies compete to make them useful. Let researchers continue expanding what they can accomplish. But let humanity establish one boundary together: machines may exercise delegated authority, but must not become the source of their own continued authority.

TEMPORAL AUTHORITY GOVERNANCE

Illustrative target architecture — not Phase I hardware evidence

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

1 BOUNDED AUTHORITY

Externally governed, capability-specific authority with defined renewal and closure rules.

2 EXTERNAL REAUTHORIZATION

QVN risk-weighted trained responders and institutions govern consequential renewal and recovery.

3 TRUSTED EVIDENCE / TIME / ATTESTATION

Future production layers protect continuity, timing, evidence, identity and key custody.

4 CROSS-JURISDICTION VERIFICATION

RAAVE enables receiving domains to evaluate evidence under their own sovereign rules.

WHAT PHASE I ESTABLISHED

On one AMD Kria KR260, a host-driven MMIO authorization sequence produced grant and subsequent closure evidence on the defined STATUS surface. After post-closure reassertion of the same authorization stimulus, CONTROL readback confirmed the write landed and no reopen was recorded during the observation window.

NOT ESTABLISHED BY PHASE I

Trusted lease expiry • independent external authority • hostile-OS bypass resistance • reboot continuity • remote attestation • protected key custody • physical resource cut-off • legitimate second-grant behavior

FROM POLICY PROMISES TO TESTABLE AUTHORITY BOUNDARIES

Temporal Authority Systems PBC | OCUP.ai | Version 1.5 | October 2026