Open Tokenized Asset Standard

A Policy-Aligned Framework for Interoperable Tokenized Finance

V2.0 | FINAL RELEASE – April 2026

Executive Summary

Global finance is entering a phase of structural transition. Tokenized assets, programmable payments, and digital representations of money are moving from experimentation into regulated core institutional workflows. Major financial institutions, central banks, and market infrastructures are now actively exploring tokenized securities, deposits, funds, and settlement mechanisms. Yet despite rapid technological progress, adoption remains constrained by a more fundamental limitation: ***the absence of shared standards governing how tokenized financial systems expose identity, compliance, data, and settlement behavior.***

Today's tokenized ecosystem is fragmented across jurisdictions, platforms, and technology stacks. Institutions are forced to re-implement compliance logic, reporting formats, and operational controls for each venue they interact with. Regulators face inconsistent data, incomplete audit trails, and limited cross-market visibility. Liquidity remains siloed across chains and platforms, settlement is bifurcated between on-chain assets and off-chain money, and systemic risk is increasingly difficult to assess as activity scales.

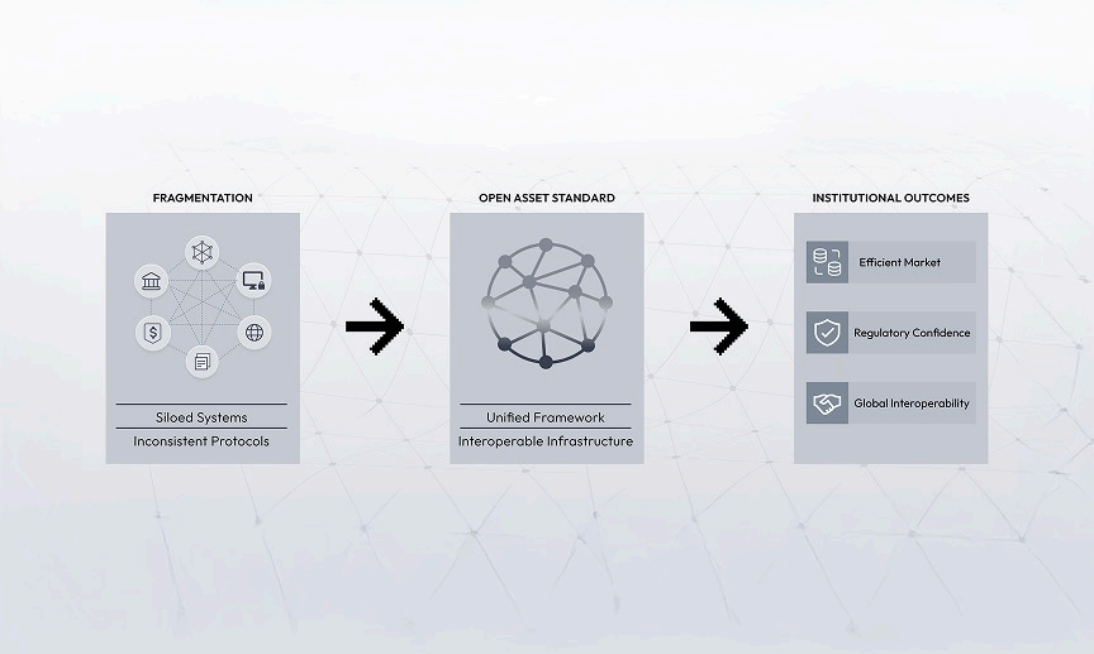
At stake is not only the scalability of tokenized markets, but the ability of the global financial system to modernize settlement, transparency, and cross-border coordination without increasing fragility, exclusion, or supervisory blind spots.

This fragmentation is no longer an early-stage inconvenience. As tokenized markets grow in volume and interconnectedness, inconsistent rules and interfaces become embedded at the infrastructure layer. Retrofitting interoperability after scale is costly, politically complex, and operationally risky. In this context, standardization is not a future enhancement; it is a prerequisite for safe expansion.

This paper introduces the Open Tokenized Asset Standard (OTAS): a modular, implementation-neutral framework defining the observable behaviors, interfaces, and audit artifacts required for interoperable, auditable, and policy-aligned tokenized financial systems. OAS does not mandate blockchains, custody models, cryptography, or vendors. Instead, it specifies what compliant systems must expose to counterparties, auditors, and regulators in order to enable trust, interoperability, and supervisory confidence across markets.

Three findings frame this work:

- Fragmentation is the primary constraint. It is now the limiting factor on institutional tokenization, not technology readiness.
- Absence of standards increases supervisory risk. Without shared rules, compliance costs rise, and supervisory visibility diminishes.
- Interoperability is a prerequisite for scale in tokenized markets, not a downstream optimization.



The Open Tokenized Asset Standard is designed to address these constraints by providing a shared financial language that institutions and sovereigns can adopt incrementally. By doing so, OAS enables tokenization to evolve from parallel innovation into production-grade global infrastructure.

This document presents the problem context, economic opportunity, architectural principles, governance model, and adoption pathway for OTAS. Detailed technical specifications, schemas, and conformance requirements are detailed throughout this document.

1. The Problem: Fragmentation as a Systemic Risk

1.1 Parallel Innovation Without Shared Rules

Tokenized finance has emerged through parallel efforts across exchanges, custodians, blockchain networks, fintech platforms, and national pilot programs. Each initiative has been optimized locally, often in response to specific regulatory environments or technical constraints. Few, however, share common assumptions about identity representation, compliance decisioning, data semantics, or settlement reconciliation. The result is a patchwork of systems that cannot easily interoperate.

Identity verification processes differ by platform and jurisdiction. Compliance checks are implemented independently and are rarely portable. Transaction data is recorded in incompatible formats, making aggregation and analysis difficult.

Asset metadata lacks consistent structure, complicating lifecycle management and secondary market activity. Even when tokenized assets settle instantly on-chain, the corresponding cash leg frequently settles off-chain through legacy systems with limited linkage between the two.

This fragmentation mirrors early phases of other infrastructure revolutions. Before shared protocols, computer networks could not communicate reliably, shipping routes were inefficient, and financial messaging relied on bilateral, error-prone formats. In each case, innovation outpaced coordination.

1.2 Institutional and Supervisory Consequences

For regulated institutions, fragmentation introduces material cost and risk that compound as activity scales:

- **Duplicated compliance effort:** Each platform requires bespoke onboarding, screening, and reporting workflows, increasing operating cost without improving risk outcomes.
- **Supervisory opacity:** Regulators receive inconsistent data and lack reliable mechanisms to correlate activity across venues, chains, and jurisdictions.
- **Operational risk:** Inconsistent asset lifecycle handling, corporate actions, and reserve disclosures increase failure modes, reconciliation errors, and legal ambiguity.
- **Capital inefficiency:** Fragmented liquidity and delayed settlement trap capital across rails, increasing funding costs and limiting market depth.

As tokenized activity grows, these inefficiencies do not remain local. They aggregate into systemic risk. Without standardized audit artifacts and reference models, both institutions and supervisors are forced to rely on bespoke interpretations rather than shared ground truth.

1.3 Sovereign and Cross-Border Impact

For governments and central banks, the lack of standards constrains policy objectives. Cross-border oversight becomes difficult when transaction data and compliance logic cannot be correlated across markets. Capital flow monitoring is fragmented. Domestic innovation risks incompatibility with external financial systems, limiting international participation.

National digital initiatives, whether focused on payments, securities, or digital identity, struggle to connect to global infrastructure without common interfaces. In the absence of standards, sovereign programs risk becoming isolated islands rather than components of a global financial network.

1.4 Why This Is No Longer Viable

At early stages of innovation, fragmentation is survivable. At institutional scale, it becomes a structural liability. Tokenized finance is now approaching volumes, velocity, and interconnectedness where inconsistent rules undermine trust, increase supervisory burden, and elevate cross-border risk.

Without a shared standard, fragmentation becomes embedded at the infrastructure layer. Compliance logic is duplicated rather than orchestrated through a common rules engine, supervisory insight lags real-time market activity, and interoperability becomes increasingly expensive to retrofit across jurisdictions. In this environment, the absence of standards is not neutral—it actively amplifies operational risk, regulatory blind spots, and systemic friction, rather than enabling a unified, programmable regulatory framework for global digital markets.

2. The Opportunity: Tokenization at an Inflection Point

2.1 Market Readiness

Despite fragmentation, institutional pilots for tokenized securities, deposits, funds, and payments are expanding across both developed and emerging markets. Regulatory clarity is emerging unevenly but decisively, with licensing regimes, sandbox programs, and supervisory guidance increasingly addressing tokenized instruments. The underlying technologies required for programmable finance—distributed ledgers, cryptographic attestations, and API-based integration—are mature.

At the same time, tokenization remains marginal relative to the size of global finance. Estimates indicate that **more than 99% of global financial assets remain off-chain,** despite digital systems already underpinning most settlement and record-keeping workflows. By comparison, the total value of global financial assets is often estimated in excess of **$700 trillion,** underscoring the scale of capital that could ultimately benefit from standardized digital representation and settlement.

This gap between technical readiness and institutional adoption reflects coordination challenges rather than a lack of demand. Institutions are increasingly prepared to participate, but require shared standards to do so safely, efficiently, and in alignment with regulatory expectations.

2.2 A Closer Look at Market Momentum

Industry forecasts predict that, according to recent analysis[1], tokenized assets (including stablecoins and tokenized deposits) could reach nearly $19 trillion by 2033 as institutional adoption accelerates.

The market for on-chain real-world assets, things like tokenized securities, funds, and real estate, has been compounding at over 200% annually[2] in recent years. It stands at roughly $35–36 billion[3] in value as of early 2025, up from almost nothing just a few years ago.

Dozens of new issuers and hundreds of thousands of investors have entered the space, as the number of tokenized asset classes continues to expand. This rapid growth signals strong demand for the efficiencies and accessibility that tokenization can bring.

	Live Projects For Tokenization	Digital Representation	Total Non-Tokenized Assets	Total Tokenized Assets As a % of non-tokenized
Currency	tether	Stablecoins	$8 Trillion	$3076 Billion (3.845%)
Bank Deposits	J.P.Morgan, Standard Chartered, citi	Tokenized Deposits	$56 Trillion	$0.0 Billion (0.000%)
Stock Market	Robinhood, Nasdaq	Tokenized Stocks	$89.5 Trillion	$0.7 Billion (0.002%)
Commodities	adecoagro	Tokenized Commodities	$149 Trillion	$2.9 Billion (0.000%)
Government Bonds + Private debts	BlackRock, Franklin Templeton	Tokenized Debt	$406 Trillion	$28.3 Billion (0.007%)
Real Estate	DAMAC, Radisson	Tokenized Real Estate	$650 Trillion	$1.1 Billion (0.000%)
			$770.1 Trillion	**$340.6 Billion (0.044%)**

Beyond the raw numbers, clear signs of momentum are evident among major market players and policymakers. Global financial incumbents and insurgents alike are experimenting with tokenized value. For instance, leading asset managers have launched tokenized money market funds, banks are piloting tokenized deposits and bonds, and stablecoins, tokenized currency, have exploded to over $300 billion in circulation.

Collaborative pilots are bridging traditional finance with crypto rails, with entities ranging from fintechs to the largest financial institutions adopting blockchain technology and tokenization solutions.

tether

Expanded beyond USDT with **tokenized treasury bills**, becoming one of the world's largest buyers of short-term U.S. debt.

Cantor Fitzgerald

Partnered with Tether to manage and trade **tokenized U.S. Treasuries** and other real-world assets.

Fidelity Investments

Announced **tokenized money-market funds** and continues to explore digital asset custody and on-chain settlement.

Fanatics

Bringing **sports memorabilia on-chain**, turning collectibles into verifiable digital assets.

BlackRock

Launched **BUIDL**, the first **tokenized money-market fund** on Ethereum, investing in tokenization infrastructure.

mastercard

Enables **on-chain settlement and tokenized payments**, partnering with Circle and JPMorgan.

ADGM

Established one of the world's most advanced **tokenization and digital asset regulatory frameworks,** attracting global institutions.

Safra

Exploring **tokenized credit, tokenized gold, and real-estate instruments** through its private banking and asset management arms.

btg pactual

Pioneered ReitBZ, one of the first **tokenized real estate** securities backed by tangible assets in Latin America.

VISA

Launched the **Visa Tokenized Asset Platform** for stablecoin and tokenized asset settlement.

HSBC

Issued **tokenized gold and bond offerings**, and built a digital assets custody platform for institutional clients.

Franklin Templeton

Issued **tokenized mutual funds** on public blockchains, leading the push toward on-chain fund management.

2.3 Economic and Institutional Gains

A shared standard unlocks measurable economic value by reducing duplication and inefficiency across the financial system.

Industry analyses have repeatedly highlighted the cost of fragmented settlement and reconciliation processes. Legacy post-trade infrastructure is estimated to generate hundreds of billions of dollars annually in operational and reconciliation costs, much of which stems from inconsistent data formats, manual intervention, and delayed settlement cycles. Even incremental improvements in interoperability and straight-through processing can therefore yield material savings at institutional scale.

In addition, settlement inefficiencies directly impact capital efficiency. Large volumes of collateral and liquidity remain immobilized due to delayed reconciliation and fragmented rails.

Standardized tokenized settlement mechanisms, when paired with interoperable compliance and reporting, have the potential to materially reduce these frictions, improving balance-sheet utilization without increasing risk.

Brazil, for example, has established one of the most forward-looking regulatory frameworks for digital assets in the world. A new law passed in 2022 explicitly recognizes tokenized securities and bonds, providing legal clarity for issuance and trading. The Central Bank of Brazil has already built a massively successful instant payments network (Pix) that handled 70+ billion annual transactions[4] within its first 3 years of existence. Brazil's unified approach also includes Open Finance data-sharing (with over 42 million users connected[5] to 800+ financial institutions) and a nationwide digital ID system ("gov.br") with 155+ million users. This coherent digital finance stack, instant payments, open banking, digital identity, and soon a tokenized real (CBDC), shows the power of standardization in action.

Other emerging economies are also driving innovation: Mexico's Fintech Law set early standards for digital finance, the UAE is integrating crypto and even partnering with global firms on tokenized payment trials, Hong Kong and Singapore have launched regulatory sandboxes and licensing regimes for tokenized assets, and jurisdictions from El Salvador to South Africa have enacted policies recognizing crypto assets in their financial systems.

Even in developed markets, momentum is building, the EU's comprehensive MiCA regulation and U.S. pilot programs for tokenized treasuries indicate that mainstream adoption is a matter of how, not if.

2.4 Societal and Market Inclusion Benefits

Beyond institutional efficiency, standardized tokenized infrastructure can expand market access and reduce structural barriers. Fragmented onboarding and compliance processes currently exclude many participants, particularly in emerging markets, from global financial systems. Portable digital identity and standardized compliance signaling can reduce repetitive verification requirements while preserving jurisdictional controls.

Lower issuance and operational costs also enable smaller issuers, public entities, and community-scale projects to access capital markets more efficiently. In this way, standardization supports not only institutional scalability but broader economic participation.

For example, Brazil's initiative brought 71.5 million unbanked citizens into the digital economy and saw over $55 billion in stablecoin transactions in 2024 alone. As one analysis put it, what is unfolding in Brazil is just the beginning, but it stands as a proof of concept; a live, interoperable stack that can serve as a "reference model" for other markets moving toward agentic, real-time financial infrastructure.

2.5 A Familiar Pattern

History demonstrates that standards catalyze adoption. Open protocols like TCP/IP and HTTP allowed disparate computer networks to interconnect, transforming a niche system into a global utility used by billions. In 1990, only about 2.6 million people[6] were online; by 2020, over 4.5 billion people, more than half of humanity, had Internet access, a meteoric rise enabled by universally adopted communication standards.

In global trade, the adoption of the ISO shipping container standard in the 1960s revolutionized logistics. Today, over 90% of world merchandise[7] travels in standardized containers, slashing transport costs and fueling a boom in international commerce.

In banking, the creation of SWIFT in the 1970s provided a single, secure format for financial messages, replacing the incompatible, error-prone Telex system. As a result, more than 11,000 institutions in over 200 countries can now communicate payments through SWIFT, exchanging over 40 million[8] messages each day that enable trillions of dollars in transactions. These examples underscore that common standards unify fragmented networks, build trust, and unlock scale.

Tokenized finance now faces a similar inflection point. The opportunity is no longer defined by whether digital assets are technically feasible, but by whether shared standards can convert parallel innovation into coherent, trusted infrastructure.

3. What the Open Tokenized Asset Standard (OTAS) Is and Is Not

3.1 Normative Scope & Standards

The Open Tokenized Asset Standard (OTAS) defines a set of normative requirements governing how tokenized financial systems MUST expose externally observable behaviors, interfaces, and audit artifacts in regulated environments.

OTAS is intentionally concerned with verifiable outcomes, not internal implementation. Two systems with materially different architectures MAY both conform to OTAS, provided they expose equivalent external evidence that enables counterparties, auditors, and supervisors to reason about compliance, settlement, and governance.

Normative requirements in OTAS are expressed using the terminology defined in RFC 2119. Where a requirement is designated as MUST or SHALL, failure to satisfy that requirement constitutes non-conformance for the relevant module.

3.2 Modular Conformance Model

OTAS is explicitly modular. Each module:

- Defines a bounded functional scope
- Specifies its own normative requirements
- Identifies the audit artifacts a compliant implementation MUST produce
- Can be adopted independently of other modules

This design supports phased adoption, partial participation, and jurisdiction-specific alignment. Institutions are not required to implement the full standard in order to participate meaningfully.

Modules are designed to interoperate, but OTAS does not assume uniform adoption across institutions, markets, or jurisdictions.

3.3 Observable Behavior and Verifiability

A core design principle of OTAS is that compliance is externally verifiable. Conformance is demonstrated through observable behavior and standardized artifacts rather than self-assertion or internal attestations.

- Counterparties to validate eligibility and settlement status
- Auditors to reconstruct compliance decisions
- Regulators to assess system behavior without intrusive access

Representative protocol flows, data models, interface contracts, and certification workflows illustrating this approach are provided in Appendix A.

3.4 Explicit Non-Goals

To preserve neutrality and long-term durability, OTAS explicitly does not mandate:

- Blockchain networks or ledger technologies
- Custody, wallet, or account models
- Cryptographic algorithms or identity schemes
- Vendor platforms, reference implementations, or deployment architectures

These choices remain the responsibility of implementers and regulators. OTAS standardizes the **external contract** between systems and stakeholders, not internal design decisions.

4. Conceptual Architecture of the Open Tokenized Asset Standard

OTAS defines a layered reference architecture that identifies where standardization is required and where architectural flexibility is preserved. Each layer defines a distinct technical surface area with associated conformance expectations.

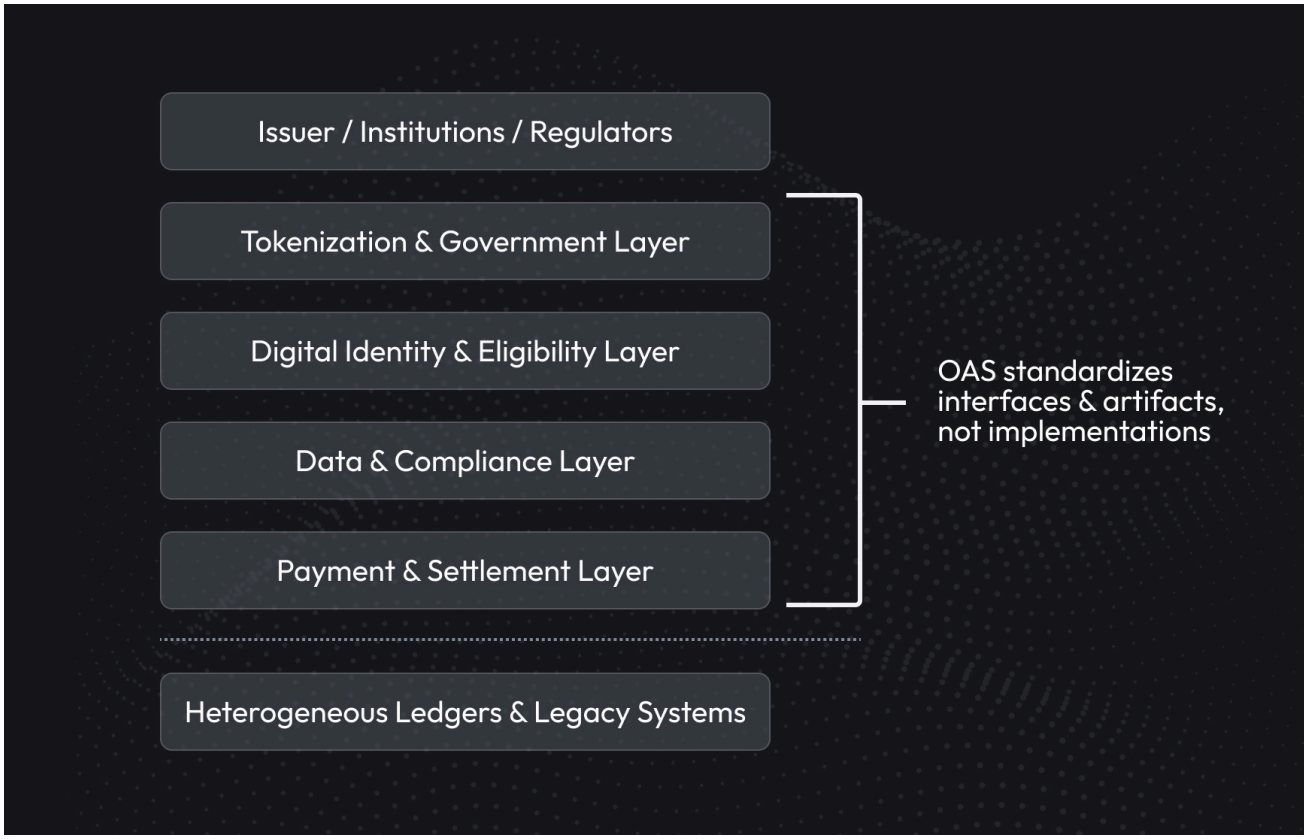


Figure 1: OTAS Layered Reference Architecture

This figure illustrates the conceptual layering of the Open Tokenized Asset Standard. OTAS defines standardized interfaces, artifacts, and observable behaviors at each layer while preserving implementation flexibility beneath and policy autonomy above.

4.1 Architectural Mandate

Interoperability at the institutional scale requires clear separation of concerns. When compliance logic, settlement mechanics, identity controls, and asset governance are tightly coupled, systems become difficult to audit, regulate, and extend.

The OTAS architecture isolates these concerns so that:

- Compliance outcomes can be evaluated independently of implementation
- Settlement mechanisms can evolve without breaking policy enforcement
- Identity and eligibility assertions remain portable across platforms

4.2 Payment and Settlement Layer

Interoperability at the institutional scale depends on making settlement outcomes externally inspectable across heterogeneous rails. In OTAS, the settlement layer defines how an asset movement and its corresponding payment obligation are correlated, reconciled, and evidenced to counterparties, auditors, and supervisors.

Figure 3 illustrates a representative OTAS-compliant settlement sequence across heterogeneous rails. The sequence is intentionally implementation-neutral: an institution MAY use atomic delivery-versus-payment (DvP), a synchronous two-step workflow, or a legacy rail with delayed confirmation. OTAS standardizes what MUST be observable regardless of the internal orchestration approach.

Technical Interpretation

Under OTAS, settlement is modeled as two correlated but independently verifiable state machines: (i) an asset leg and (ii) a payment leg. Each leg produces its own confirmation event and integrity-bound audit artifact. The system links these through shared correlation identifiers so that finality, timing, and failure modes can be reconstructed without privileged access.

Normative Requirements.

A compliant implementation MUST:

- Expose verifiable settlement status for both asset and payment legs (including initiation, reservation/pending, completion, and failure).
- Provide an auditable linkage between tokenized instruments, asset transfer events, and payment confirmations via a shared settlement identifier.
- Expose reconciliation evidence sufficient to correlate asset and payment legs across heterogeneous payment rails and ledger environments.

At minimum, the observable evidence surface SHOULD include: a settlement_id, per-leg references (e.g., asset_tx_ref and payment_tx_ref), per-leg timestamps, and a settlement correlation artifact (e.g., an envelope containing both references and an integrity commitment).

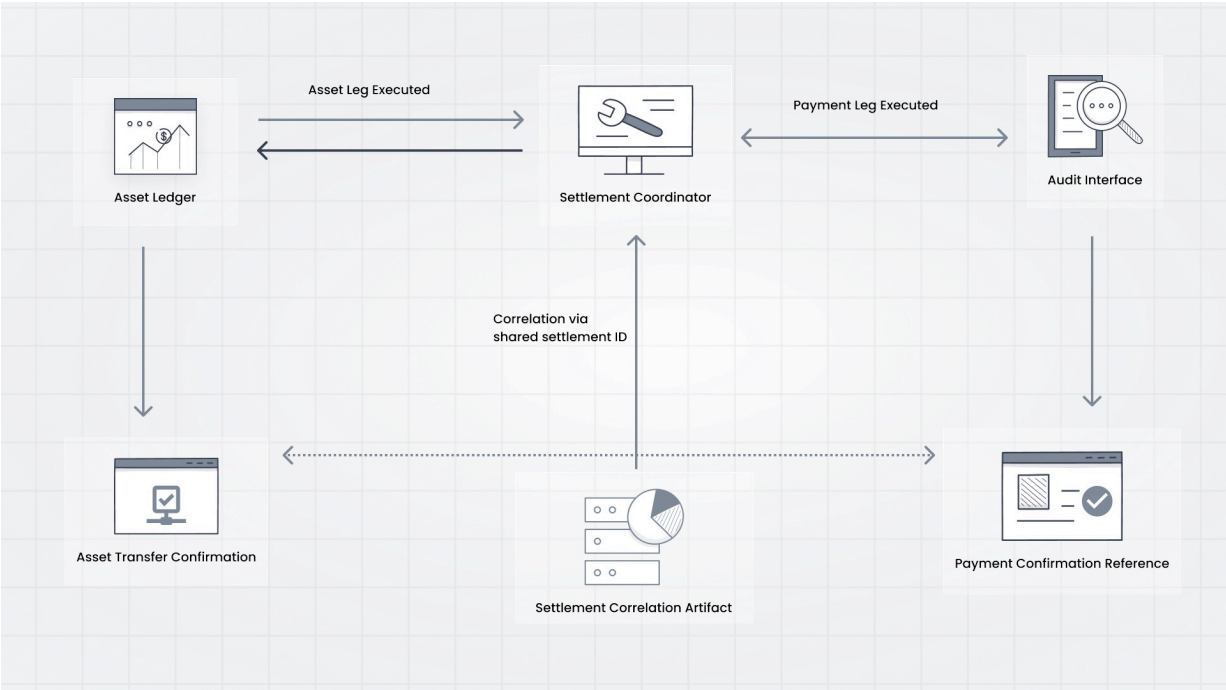


Figure 3: Settlement And Audit Artifact Correlation Flow

This figure shows how OAS correlates asset and payment settlement events across heterogeneous rails using shared identifiers and audit artifacts, without requiring atomic execution or unified infrastructure.

(see Appendix A.1.3 for the full representative sequence and outputs).

4.3 Data and Compliance Layer

This layer defines how transaction data and compliance decisions are structured and exposed.

A compliant system MUST:

- Represent compliance outcomes in a standardized, machine-readable form
- Produce audit artifacts sufficient to reconstruct policy enforcement decisions
- Support consistent reporting across jurisdictions and platforms

OTAS standardizes compliance outcomes, not rule logic. Institutions remain free to implement jurisdiction-specific compliance engines, provided decisions can be externally verified.

Canonical data models and interface contracts are described in **Appendix A.2 and A.3**.

4.4 Digital Identity & Eligibility Layer

OTAS treats identity and eligibility as first-class technical primitives: policy enforcement and interoperability require that eligibility can be asserted, verified, and revoked without repeatedly exchanging raw identity data.

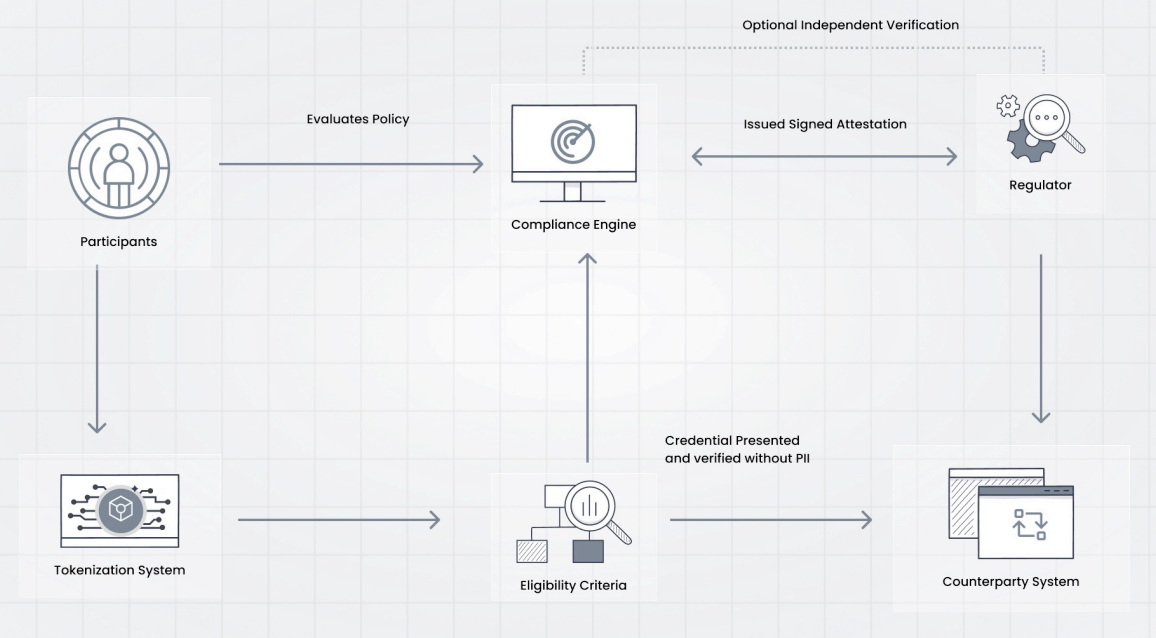


Figure 4: Compliance Attestation And Verification Flow

This flow illustrates how eligibility and compliance decisions are issued as portable, time-bounded attestations that counterparties and regulators can verify without access to underlying identity data or internal rule logic.

Figure 4 shows a representative compliance attestation and verification flow under OTAS. The flow demonstrates how a counterparty can validate eligibility and restrictions using portable, time-bounded credentials and signed decision artifacts, without learning underlying personal or institutional attributes beyond what is necessary for the transaction context.

Technical Interpretation

In OTAS, identity is represented through verifiable, time-bounded credentials issued by trusted authorities (e.g., KYC/KYB providers, regulated intermediaries, or jurisdictional identity systems). Eligibility is expressed as a portable attestation bound to a subject reference (pseudonymous where appropriate), with explicit validity windows and revocation semantics. Policy evaluation consumes credential categories and transaction context, and emits a structured ComplianceDecision artifact that is integrity-bound to the associated transaction.

Normative Requirements.
A compliant implementation MUST:

- Support portable eligibility assertions that can be verified by counterparties without re-onboarding.
- Enable policy enforcement and audit reconstruction without requiring raw identity attributes or PII in the evidence surface.
- Allow counterparties and regulators to verify eligibility claims, including issuer provenance, validity window, and revocation status.

At minimum, the evidence surface SHOULD include: credential issuer identity references, a subject reference suitable for correlation (without exposing raw identity), validity timestamps, revocation/status signaling, and cryptographic proofs sufficient to verify authenticity and integrity.

4.5 Tokenization and Governance Layer

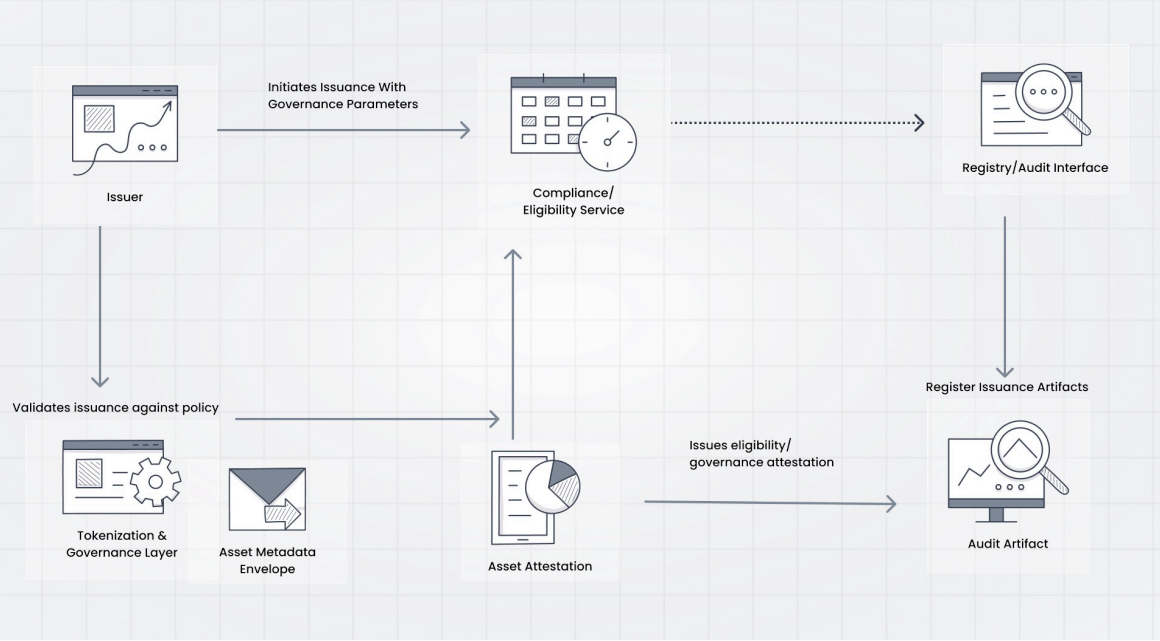


Figure 2: Asset Issuance And Governance Binding Flow

This flow illustrates how governance intent, eligibility constraints, and audit evidence are bound to a tokenized asset at issuance and preserved throughout its lifecycle in an OAS-compliant system.

The Tokenization and Governance Layer defines how tokenized instruments behave predictably across issuance, transfer, restriction, redemption, and administrative actions. In traditional markets, many of these behaviors are standardized through market conventions and legal infrastructure; in tokenized markets, they are frequently redefined per issuer or venue, creating incompatibility and supervisory ambiguity.

Figure 2 illustrates a representative asset issuance and registration flow under OTAS. The figure highlights how governance intent and required evidence are bound at issuance and preserved through audit artifacts that can be verified by external parties.

Technical Interpretation

OTAS standardizes the external contract of a tokenized instrument through: (i) a canonical metadata envelope, (ii) a minimum set of lifecycle events and administrative actions, and (iii) integrity-bound audit artifacts sufficient to reconstruct provenance and governance intent. Implementations MAY be on-chain, off-chain, or hybrid; functional equivalence and observability are required, identical ABIs are not.

Normative Requirements.

A compliant implementation MUST:

- Expose a machine-readable asset metadata envelope including an asset identifier, issuer reference, regulatory/jurisdictional classification, lifecycle state, and references to applicable restrictions and disclosures.
- Emit standardized lifecycle events for at least issuance, transfer, restriction application/removal, and redemption, including timestamps and references to applicable compliance decisions where relevant.
- Support observable administrative controls appropriate to regulated environments (e.g., freeze/unfreeze or restriction actions and lawful override semantics), with each action generating an audit artifact or event record that is externally verifiable.

Where reserve-backed claims are made, the implementation MUST expose reserve attestation references and freshness/status signaling so that counterparties and supervisors can reason about backing quality without requiring privileged access to internal reserve systems.

(see Appendix A.1.1 for the full representative sequence and observable outputs).

4.6 Why Layering Matters

Layered architectures have proven resilient across multiple generations of financial and technical infrastructure. By separating concerns, layering allows systems to evolve without breaking interoperability.

For institutions, layering enables phased adoption. Organizations can adopt specific layers or modules aligned with immediate priorities, while maintaining compatibility with broader markets. Without layering, standards become monolithic and adoption stalls.

4.7 Modular Conformance

Each layer is realized through one or more modules that can be independently adopted and certified. This modularity minimizes disruption to existing infrastructure and allows institutions to engage at their own pace.

5. Governance, Trust, and Neutrality

5.1 Governance as Infrastructure

In standards development, governance is not ancillary; it is foundational. Many technically sound standards have failed due to weak, opaque, or biased governance structures.

For regulated markets, trust in the governance process is as critical as trust in the technical content of the standard.

5.2 Multi-Stakeholder Governance Model

OTAS is governed through a multi-stakeholder structure designed to ensure neutrality, transparency, and long-term viability. Governance includes representation from:

- Financial institutions
- Regulators and supervisory authorities
- Technologists and infrastructure providers
- Academic and standards experts

No single constituency controls the evolution of the standard.

5.3 Open Repositories and Versioning

Specifications are maintained in open repositories with transparent version control and public contribution processes. Release cycles align with regulatory calendars and industry milestones, ensuring predictability for institutions and supervisors.

5.4 Certification and Conformance

Certification in OTAS is designed to validate observable system behavior, not internal implementation details. An implementation is considered conformant only if it can produce standardized, verifiable evidence that demonstrates adherence to the normative requirements of the modules and tiers it claims.

OTAS certification explicitly avoids privileged system access, source code review, or vendor-specific attestations. Instead, conformance is assessed through externally consumable artifacts, enabling independent verification by auditors, counterparties, and regulators.

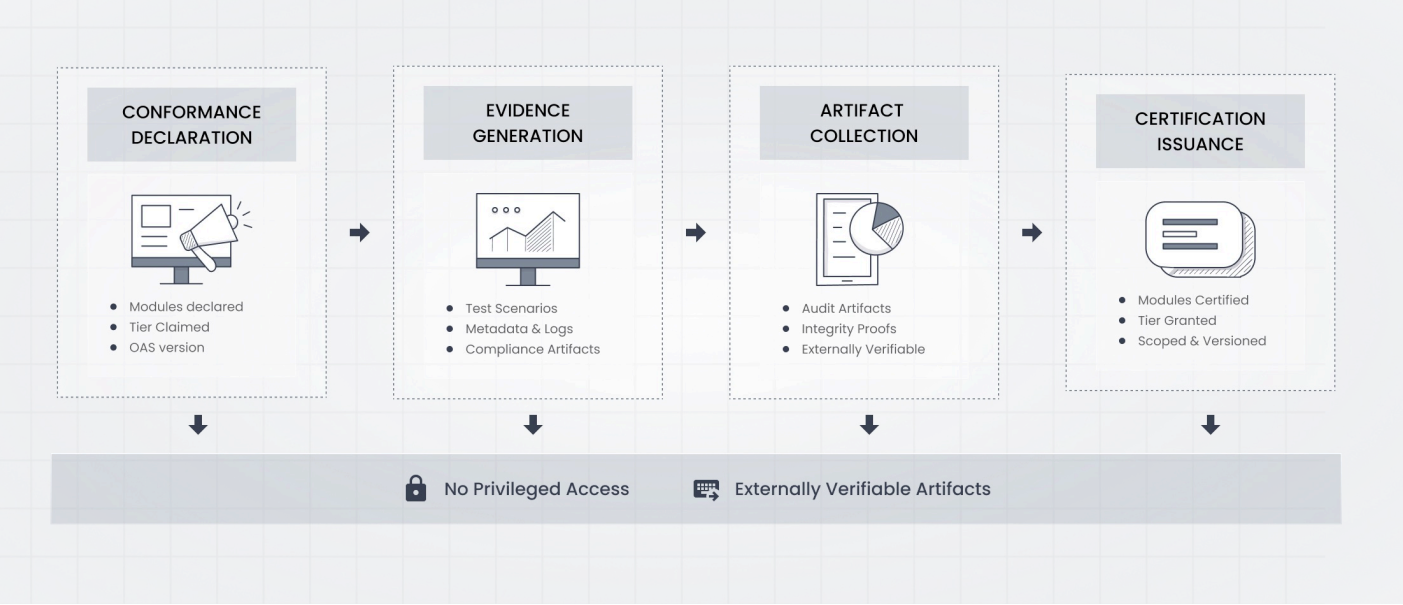


Figure 5: OTAS Certification And Conformance Workflow

This figure depicts the evidence-based certification process used by OTAS, in which conformance is assessed through externally observable artifacts rather than internal system access or vendor attestations.

5.4.1 Conformance Declaration

An implementation claiming conformance to OAS MUST publish a formal conformance declaration that includes:

- OTAS version (e.g., v1.0)
- Conformance tier claimed (OTAS-Core, OTAS-Enhanced, or OTAS-Full)
- Modules implemented (M1–M7)
- Highest supported programmability level (if applicable)
- Scope of deployment (e.g., asset classes, jurisdictions, chains or rails covered)

This declaration establishes the baseline against which certification evidence is evaluated and MUST be version-pinned to prevent ambiguity as the standard evolves.

5.4.2 Evidence-Based Certification Model

Certification is based on the inspection of standardized evidence surfaces generated by the implementation under test. These evidence surfaces correspond directly to the observable behaviors defined in each OTAS module.

At a minimum, a certifiable implementation MUST be able to produce:

- Machine-readable audit artifacts for representative transactions
- Canonical metadata envelopes for assets in scope
- Compliance decision artifacts linked to transactions
- Settlement correlation artifacts (where applicable)
- Integrity commitments (hashes, signatures, or equivalent proofs)

Evidence MUST be sufficient to allow an independent verifier to deterministically reconstruct system behavior without relying on undocumented assumptions or internal logic.

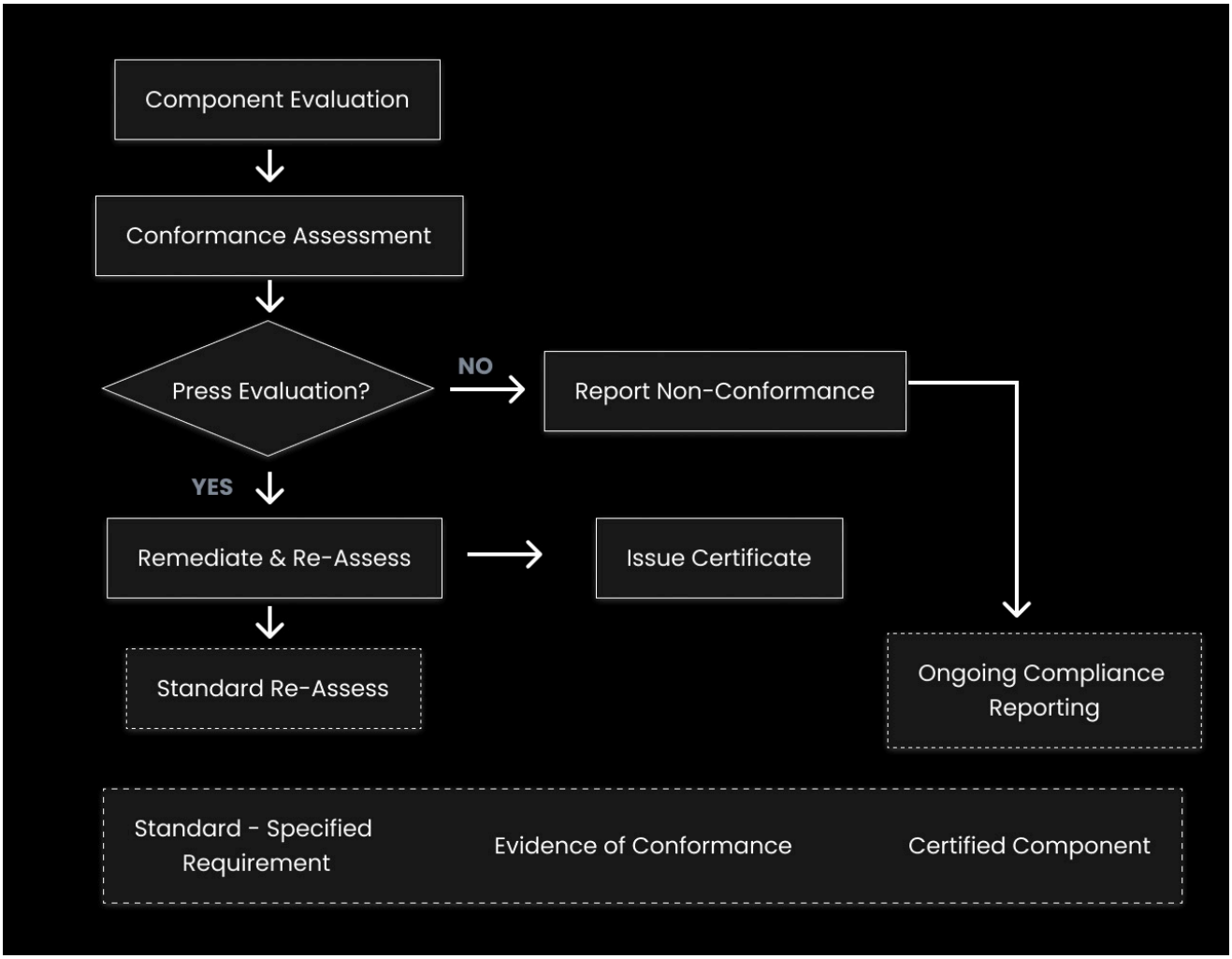
5.4.3 Certification Workflow

Figure 5 illustrates the representative OTAS certification workflow. The workflow demonstrates how certification is performed without requiring access to internal systems or proprietary infrastructure.

The certification process proceeds as follows:

- The implementation declares supported modules, tiers, and versions.
- Defined test scenarios exercise required observable behaviors.
- Required audit artifacts and logs are generated.
- An independent verifier validates artifacts against published module requirements.
- Certification is issued for the declared scope and version.

Certification is scoped and versioned. An implementation certified for OTAS-Core-v1.0 is not implicitly certified for OTAS-Enhanced or future versions.



5.4.4 Conformance Evidence Package

For each certification assessment, an implementation MUST provide a conformance evidence package containing:

- Conformance declaration (Section 5.4.1)
- Asset catalog with canonical metadata
- Representative transaction logs with identifiers and timestamps
- Linked compliance decision artifacts
- Settlement and reconciliation artifacts (if applicable)
- Reserve attestations and oracle references (if applicable)
- Integrity proofs for all included artifacts

All artifacts MUST be machine-readable, and reference shared identifiers defined by OTAS to support correlation across layers.

5.4.5 Regulator and Supervisor Interaction

OTAS certification is explicitly designed to support supervisory oversight without imposing intrusive access requirements.

Regulators and supervisory authorities MAY:

- Verify certification status and scope
- Independently validate artifact integrity
- Request representative evidence packages
- Correlate artifacts across systems and venues

At no point does certification require regulators to access internal system components, rule engines, or proprietary data stores. Supervisory confidence is derived from standardized, verifiable outputs rather than institutional self-assertion.

5.4.6 Certification Durability and Evolution

Certification applies to a specific OTAS version and declared scope.
Material changes to:

- Implemented modules
- Asset classes covered
- Governance or compliance semantics
- Settlement orchestration behavior

MUST trigger a re-certification or scope update.

This ensures that certification remains a reliable signal of current system behavior rather than a static endorsement.

5.5 Global Precedents

OTAS governance draws on precedents from globally adopted standards such as ISO, SWIFT, and open banking frameworks. These models demonstrate that neutral governance, clear scope, and transparent processes are prerequisites for durable adoption.

6. Adoption Path: From Pilot to Global Infrastructure

6.1 Phase-Based Adoption

OTAS adoption follows a phased pattern that reflects how regulated financial infrastructure is adopted in practice:

- **Foundation**: Controlled pilots and sandboxed evaluation within defined risk boundaries
- **Formalization:** Public specification review and institutional testing aligned with internal governance processes
- **Certification:** Independent verification and supervisory alignment for selected modules
- **Expansion:** Marketwide deployment and intelligent automation as confidence and coverage increase

These phases are not strictly linear. Institutions may enter at different points depending on regulatory clarity, internal readiness, and strategic priorities.

6.2 Adoption Without Commitment

A core design objective of OTAS is to enable engagement without forcing premature commitment. Institutions may observe, test, or partially adopt elements of the standard without signaling full production intent.

This includes participation through:

- Observer or review roles
- Internal testing and shadow-mode evaluation
- Limited pilots scoped to specific assets, markets, or modules
- Partial conformance aligned to immediate regulatory or operational needs

By supporting low-friction entry, OTAS reduces institutional risk while enabling early alignment and learning.

6.3 Regulatory Coexistence

OTAS is designed to coexist with evolving regulatory frameworks rather than replace them. Regulation defines policy objectives and legal obligations; standards operationalize how those obligations are expressed, enforced, and audited across systems.

By standardizing observable compliance outcomes and audit artifacts, OTAS can reduce supervisory burden, improve transparency, and support consistent interpretation across markets—without constraining regulatory discretion.

6.4 Adoption in Regulated Environments Is Non-Linear

In practice, adoption within regulated institutions rarely follows a uniform or synchronized path. Different business units, asset classes, and jurisdictions progress at different speeds.

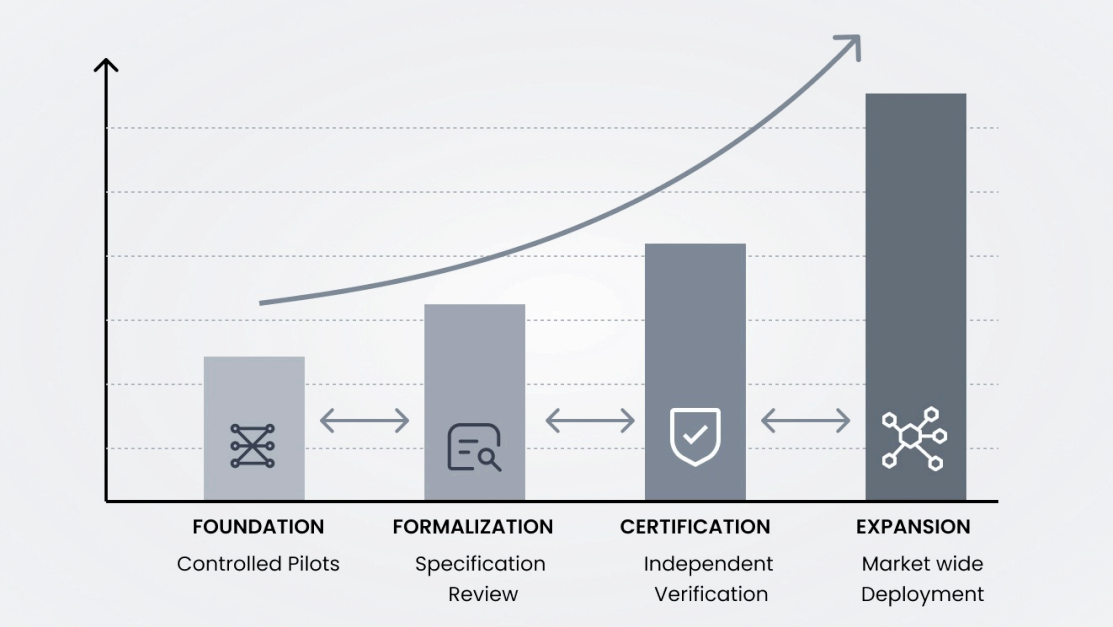
Regulatory clarity may lag technical capability, and internal approval processes often extend over multiple cycles.

OTAS is intentionally designed to tolerate partial, uneven, and asynchronous adoption. Systems may interoperate at different depths while maintaining overall coherence. This flexibility is essential for global institutions and sovereign entities operating across diverse regulatory environments.

6.5 Institutional Readiness and Coexistence With Legacy Systems

Incremental adoption allows institutions to participate without replacing existing systems. OTAS modules can be layered onto current infrastructure, enabling coexistence with legacy platforms during transition periods.

This approach supports internal change management, minimizes operational disruption, and allows institutions to align adoption with regulatory approvals and investment cycles.



7. Engagement Model: Participation and Contribution

7.1 Modes of Participation

OTAS supports multiple modes of engagement, reflecting the diversity of institutional readiness and strategic intent:

- Observers seeking insight and alignment
- Pilot participants testing specific modules
- Contributors shaping specifications
- Governance members overseeing evolution

7.2 What Engagement Is Not

Engagement with OTAS does not obligate adoption, prescribe timelines, or require technology commitments. Institutions retain autonomy over implementation decisions.

7.3 Access to Full Technical Specifications

Detailed technical specifications, schemas, and conformance requirements are available through structured engagement. This approach ensures responsible disclosure, contextual review, and collaborative refinement.

8. Closing Remarks

Tokenization is becoming an integral component of modern financial infrastructure. Without shared standards, however, its potential will remain constrained, and its risks will continue to scale.

The Open Tokenized Asset Standard provides a path from fragmentation to interoperability. By defining common rules for identity, compliance, data, and settlement—without constraining implementation—it enables institutions and sovereigns to participate in tokenized finance with confidence.

Standards are how markets scale. OTAS is designed to ensure that the next generation of financial infrastructure scales safely, transparently, and globally.

References

1. Boston Consulting Group, Ripple, FiNews. 2025. "Approaching the Tokenisation Tipping Point." https://www.finews.asia/images/download/approaching-tokenization-at-the-tipping-point.pdf
2. RWA.xyz. 2025. "Tokenized Assets: Industry Dashboard." RWA.xyz Analytics. https://app.rwa.xyz/
3. 21.co. 2024. "The State of Tokenization." 21.co Research (Dune Analytics). https://dune.com/21sharesresearch/tokenization-overview
4. Banco Central do Brasil (BCB). 2024. "Pix Statistics." Banco Central do Brasil. https://www.bcb.gov.br/en/financialstability/pixstatistics
5. Banco Central do Brasil (BCB). 2024. "Relatório de Gestão do Open Finance" [Open Finance Management Report]. Banco Central do Brasil. https://www.bcb.gov.br/estabilidadefinanceira/openfinance
6. International Telecommunication Union (ITU). 2021. "Measuring Digital Development: Facts and Figures 2021." ITU Publications. https://www.itu.int/itu-d/reports/statistics/facts-figures-2021
7. Containerlift. 2025. "The Evolution of the Shipping Container." https://www.containerlift.co.uk/shipping-container-evolution
8. SWIFT. 2023. "SWIFT in Numbers." SWIFT Annual Review. https://www.swift.com/about-us/discover-swift/fin-traffic-figures

9. Appendix A

Technical Architecture and Conformance Reference (Informative)

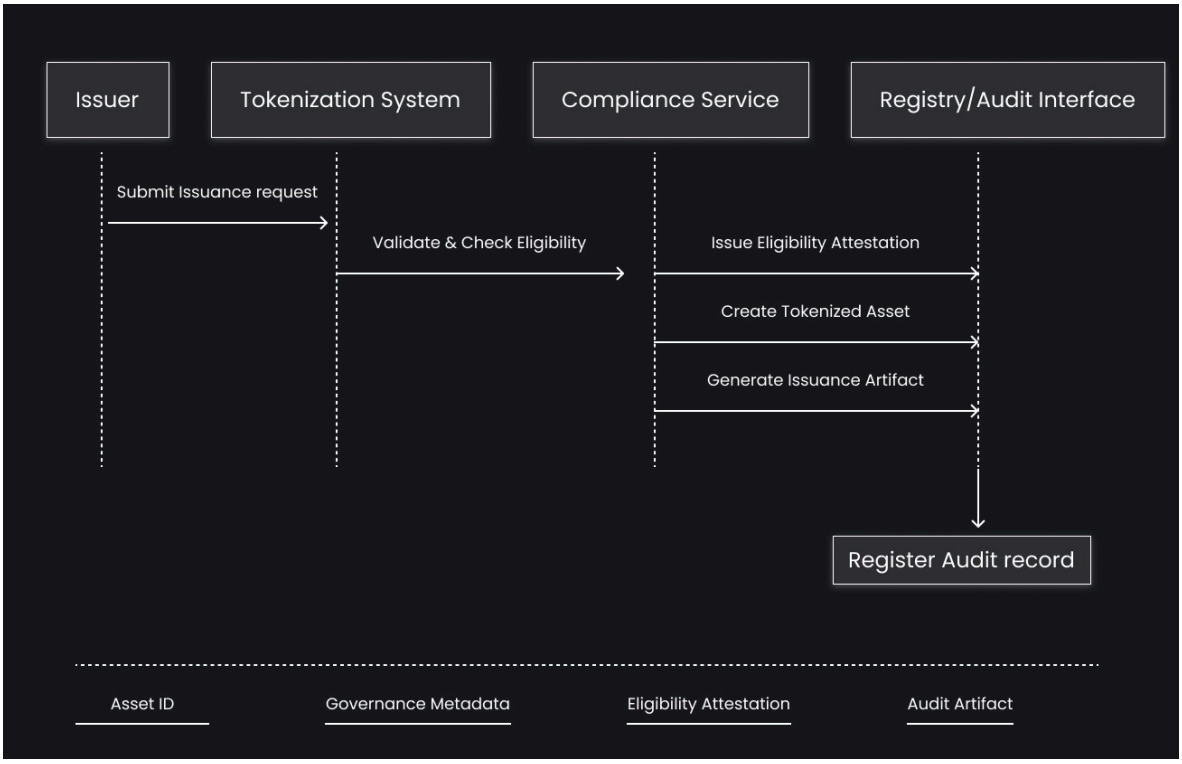
This appendix provides a technical reference to support the normative requirements described in Sections 3–5. It is intended to illustrate how the Open Tokenized Asset Standard (OTAS) operates in practice through representative protocol flows, canonical data models, interface surfaces, cryptographic guarantees, and certification workflows.

This appendix is informative, not prescriptive. It does not define a reference implementation, mandate specific technologies, or constrain deployment architectures. Instead, it demonstrates the technical completeness and verifiability of the standard.

A.1 Representative Protocol Flows

This section describes representative end-to-end flows illustrating how OTAS-compliant systems interact and produce auditable outcomes.

A.1.1 Asset Issuance and Registration Flow



Actors

- Issuer
- OAS-compliant Tokenization System
- Eligibility / Compliance Service
- Registry / Audit Interface

Flow Overview

- Issuer initiates asset creation with declared governance parameters.
- Tokenization system validates issuance parameters against policy rules.
- Eligibility service issues an eligibility attestation for the asset class.
- Tokenized asset is created with governance metadata bound at issuance.
- An issuance audit artifact is generated and registered.

Observable Outputs

- Asset identifier
- Governance metadata
- Issuance attestation
- Audit artifact hash

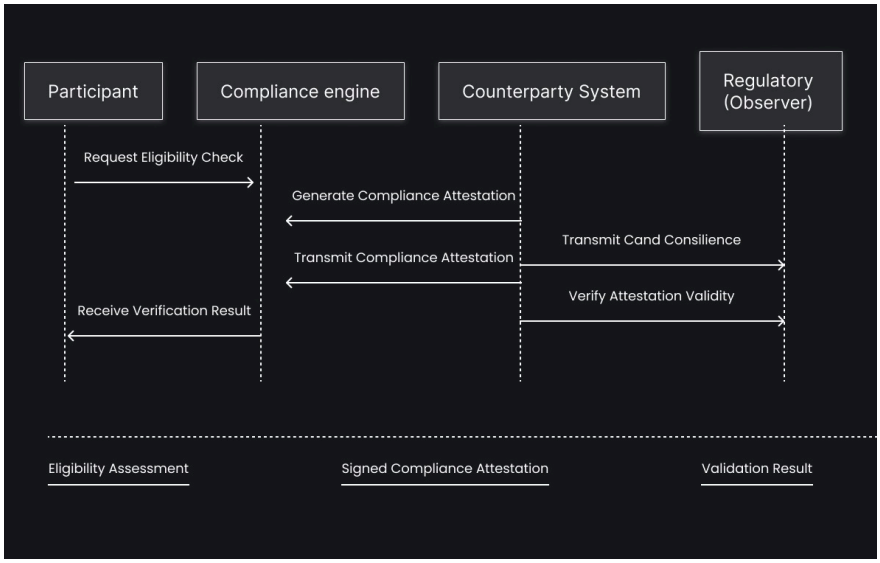
Conformance Requirement

A compliant implementation MUST expose issuance metadata and associated audit artifacts sufficient to verify asset provenance and governance intent.

A1.2 Compliance Attestation and Verification Flow

Actors

- Participant
- Compliance Engine
- Counterparty System
- Regulator (observer)



Flow Overview

- Participant requests eligibility to transact.
- Compliance engine evaluates jurisdictional and policy requirements.
- A compliance attestation is generated and cryptographically signed.
- Counterparty verifies the attestation without accessing underlying identity data.
- Regulator may independently verify attestation validity.

Observable Outputs

- Signed compliance attestation
- Attestation validity window
- Verification result

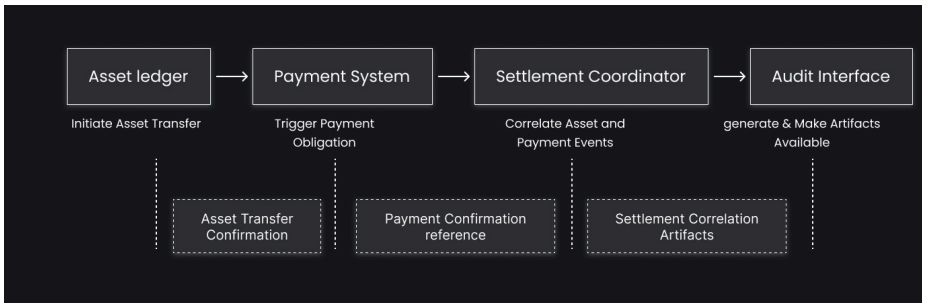
Conformance Requirement

Compliance decisions MUST be externally verifiable without requiring disclosure of internal rule logic or personal data.

A.1.3 Settlement and Audit Artifact Flow

Actors

- Asset Ledger
- Payment System
- Settlement Coordinator
- Audit Interface



Flow Overview

- Asset transfer is initiated.
- Payment obligation is triggered on the selected rail.
- Settlement coordinator correlates asset and payment events.
- Settlement confirmation artifact is generated.
- Artifact is made available for reconciliation and audit.

Observable Outputs

- Asset transfer confirmation
- Payment confirmation reference
- Settlement correlation artifact

Conformance Requirement

A compliant system MUST expose sufficient evidence to reconcile asset and payment legs, regardless of the underlying settlement rail.

A.2 Canonical Data Models (Abstract)

The following canonical models illustrate the minimum data structures required for interoperability. Implementations MAY extend these models, but MUST preserve required fields.

A.2.1 Asset Representation

Required Fields

- Asset ID
- Issuer Identifier
- Asset Class
- Governance Parameters
- Lifecycle State

Required Fields

- Jurisdictional tags
- Disclosure references
- Reserve attestations

A.2.2 Compliance Attestation

Required Fields

- Attestation ID
- Subject Identifier (pseudonymous)
- Policy Context
- Validity Period
- Cryptographic Signature

A.2.3 Audit Artifact Envelope

Required Fields

- Artifact ID
- Artifact Type
- Timestamp
- Hash Commitment
- Issuer Signature

A.3 Interface and API Surfaces (Conceptual)

OTAS defines interface contracts, not transport-specific APIs.

A.3.1 Compliance Attestation Interface

Purpose

Submit and verify compliance decisions.

Functions

- SubmitComplianceAttestation()
- VerifyComplianceAttestation()

Guarantees

- Authenticity
- Integrity
- Non-repudiation

A.3.2 Audit Artifact Retrieval Interface

Purpose

Enable regulators and counterparties to retrieve verifiable evidence.

Functions

- RetrieveAuditArtifact()
- VerifyArtifactIntegrity()

A.3.3 Settlement Status Interface

Purpose

Expose settlement outcomes in a standardized form.

Functions

- QuerySettlementStatus()
- RetrieveSettlementArtifact()

A.4 Cryptographic Assumptions and Guarantees

OTAS relies on cryptographic primitives to ensure trust, auditability, and privacy without prescribing specific algorithms.

Required Properties

- Digital signatures for attestations and artifacts
- Hash commitments for integrity verification
- Time-bounded validity assertions
- Support for selective disclosure where applicable

Explicit Non-Goals

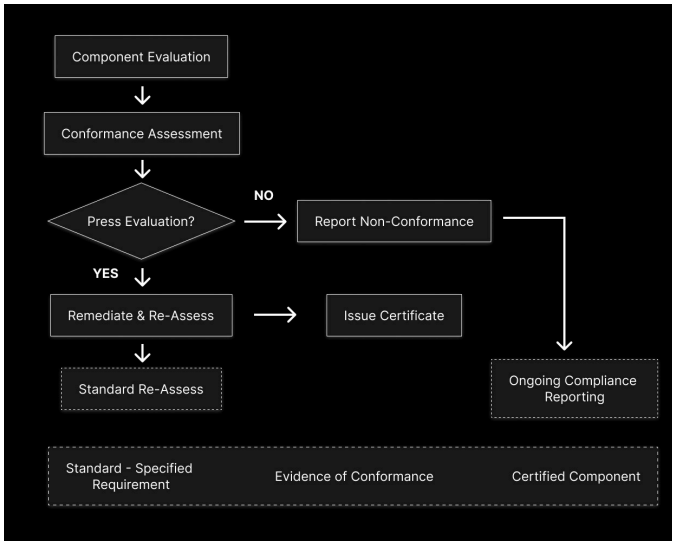
- OAS does not mandate specific algorithms or libraries.
- OAS does not require on-chain cryptographic verification.

A.5 Certification and Conformance Workflow

This section illustrates how OTAS conformance is assessed without intrusive system access.

Workflow Overview

- Implementation declares supported modules.
- Required observable behaviors are exercised.
- Audit artifacts are generated and collected.
- Independent verifier validates artifacts against module requirements.
- Certification is issued for declared modules and versions.



Regulatory Interaction

Regulators may:

- Verify artifacts independently
- Validate certification status
- Review versioned conformance declarations

At no point is direct access to internal systems required.

THANK YOU