# CERTEN: The Control Layer of Digital Finance

## Technical Whitepaper

## Contents


**1. Abstract**

**2. Introduction: The Control Problem**

**3. Design Principles**

**4. System Overview**

- 4.1 Authority Layer
- 4.2 CERTEN Core
- 4.3 Authority Vaults

**5. Architecture**

- 5.1 Identity Framework (ADIs and Authority Mapping)
- 5.2 Signature Participation Model
- 5.3 Governance Resolution
- 5.4 Proof Generation
- 5.5 Autonomous Agents as Scoped Principals

**6. Protocol Flow (Transaction Lifecycle)**

**7. Security Model**

**8. Regulatory Alignment**

- 8.1 UCC Article 12: Exclusive Control
- 8.2 MiCA Article 75: Asset Segregation and Safekeeping
- 8.3 Jurisdictional Control and Data Residency
- 8.4 Legal and Interpretive Considerations

**9. Ecosystem and Use Cases**

- 9.1 Secured Lending and Collateral Management
- 9.2 Treasury Management

9.3 Custody Orchestration
9.4 Cross-Institution Workflows
9.5 Proof-Gated Contract Execution
9.6 Emerging Application Classes

**10. Status, Trust Assumptions, and Limitations**

10.1 Forward-Looking Statement
10.2 Implementation Status
10.3 Trust Assumptions
10.4 Liveness and Censorship
10.5 Out of Scope
10.6 Assurance Status

---

**An identity-based control network for institutions and autonomous agents.**

> **Note to the reader.** This document contains forward-looking statements and describes a protocol under active development. Capability descriptions throughout are qualified by Section 10, which states what is built, what the protocol assumes, what it does not do, and its assurance status. Section 10.1 is the full forward-looking statement. No part of this document should be relied on without it.

# 1. Abstract

Digital assets are controlled by keys. Institutions are governed by identity.

This mismatch creates a structural gap between how assets move on blockchains and how decisions are made within organizations. Existing solutions attempt to bridge this gap by embedding governance into custody platforms or smart contracts, forcing institutions to replicate policy logic in new environments that are difficult to audit, costly to maintain, and fragile under change.

CERTEN introduces a governance layer that separates authority from execution.

Institutional decisions are made by designated authorities (systems, roles, and individuals) within existing environments. CERTEN verifies that the correct authorities have participated, resolves governance deterministically, and produces a cryptographic proof of authorization. This proof is designed to be enforced on any blockchain able to verify it, through execution environments that accept only valid governance outcomes.

Built on Accumulate's identity-based architecture, CERTEN provides a chain-agnostic control layer that preserves institutional governance, enables multi-party coordination, and enforces authorization without requiring assets to be moved to new chains or governance logic to be rewritten.

CERTEN extends this model with protocol-native proof generation, enabling institutions to demonstrate cryptographic evidence of governance satisfaction, designed to align with emerging regulatory requirements such as UCC Article 12 "exclusive control" and MiCA asset segregation.

The same authority-before-execution property extends to a new class of actor. Autonomous agents are a new principal type, and the same identity framework governs them: an agent proposes, and the institution's designated authorities resolve the authorization (Section 5.5).

## 2. Introduction: The Control Problem

Institutional adoption of digital assets has introduced a fundamental mismatch between governance and execution.

Within institutions, control is defined by identity. Decisions are made by systems, roles, and individuals operating under established policies, compliance frameworks, and operational procedures. These processes are distributed, auditable, and deeply integrated into existing infrastructure.

On blockchains, control is defined by possession of private keys.

This mismatch forces institutions into a duplicate policy stack. Governance must be recreated inside custody platforms, smart contracts, or application layers, separate from the systems where decisions are actually made. As a result, institutional control becomes fragmented across environments that cannot be easily reconciled.

Enterprise computing solved this class of problem decades ago with LDAP, PKI, and OAuth: standard ways to express who someone is, what they are permitted to do, and how to delegate authority without surrendering credentials. Digital assets have no cross-chain equivalent. There is no LDAP for a treasury, no PKI for a permission, no OAuth for an agent.

**The Current Options and Their Limitations**

Custodial platforms centralize governance in vendor infrastructure. Governance state lives in vendor infrastructure, and assurance is contractual rather than cryptographic.

Smart contract wallets embed governance into execution code. While transparent, they require governance to be rewritten as static logic, so a change in authority structure becomes a contract change.

Neither approach preserves institutional governance as it exists.

**Regulatory Context**

UCC Article 12, enacted in more than thirty U.S. states and the District of Columbia, with effective dates now arriving across jurisdictions (in New York it took effect on June 3, 2026), defines exclusive control of a controllable electronic record, a standard that contemplates technical means of enforcement. MiCA introduces parallel expectations for asset segregation and supervisory auditability. In the United States, the GENIUS Act, signed July 18, 2025, adds a federal

framework for payment stablecoins, with enforcement beginning January 18, 2027, extending the same expectation of demonstrable operational control to stablecoin issuers.

CERTEN establishes control prior to execution and produces verifiable proof of that control.

**The Agentic Dimension**

This mismatch is now being magnified by autonomous software. As institutions begin delegating financial operations to AI agents, authority becomes distributed across humans, systems, and agents that can act continuously and without direct supervision. An agent can hold a key and produce a valid signature, but possession of a key has never been the same as the authority to act. The control problem does not change when the actor is a model rather than a person; it becomes more acute, because the actor is faster, more autonomous, and harder to constrain after the fact. Authorization must be established before the action and remain provable after it. This is the same property CERTEN provides for institutional governance, extended in design to a new principal type.

## 3. Design Principles

Five constraints shape the architecture that follows. Each is a requirement the design must satisfy, not a feature.

**Authority is expressed as identity, not as key possession.** Institutions operate through structured roles, systems, and delegated responsibilities, and those structures, rather than the holding of a private key, are what determines who may act. The architecture maps authority to identities representing roles, systems, and organizational functions, so governance can be expressed in the terms institutions already use.

**Authority resolution is strictly separated from execution.** In existing blockchain systems, execution environments determine whether an action is valid by evaluating embedded logic or verifying signatures tied directly to asset control. This conflates decision-making with execution and forces governance to be reimplemented inside systems that were not designed to express institutional policy. CERTEN inverts the order: authority must be fully resolved before execution, and execution environments verify only the proof of that authorization. Enforcement is therefore consistent across every chain where an Authority Vault is deployed, independently of which of those chains a given asset sits on.

**Institutional policy stays in the systems of record, and participation is the proof.** Compliance evaluations, risk assessments, credit approvals, and operational workflows are not migrated into CERTEN or rewritten in smart contracts. CERTEN verifies that these processes occurred by requiring participation from designated authorities. It does not interpret or evaluate policy logic; it verifies that the correct authorities produced cryptographic attestations of participation.

**Execution environments are minimized.** Removing governance logic from execution reduces attack surface and is designed to enable consistent enforcement across heterogeneous blockchain environments. Execution components are verification gateways that accept or reject transactions on proof validity alone.

**Proof of governance is a first-class, portable artifact.** Governance is not an internal process or a system log. Every authorization produces a cryptographic result that can be validated without reliance on intermediaries, vendor systems, or internal records, and that is designed to be enforced in any execution environment able to verify it. This is what allows institutions to produce evidence of control for auditors, counterparties, and regulators, and to coordinate multi-party workflows across chains without duplicating governance logic. Whether that evidence satisfies a

given legal standard is addressed in Section 8 and remains subject to the considerations in Section 8.4.

# 4. System Overview

CERTEN separates institutional governance into three distinct layers: the Authority Layer, CERTEN Core, and Authority Vaults. This separation creates an architectural boundary between decision-making, governance resolution, and execution enforcement, allowing each function to operate independently while remaining cryptographically linked.

This model can be understood as a structural division between a governance system that resolves authority and an execution system that enforces outcomes. Governance is performed once and enforced everywhere, eliminating the need to replicate policy logic across multiple systems, contracts, or custodial platforms.

Spanning these layers is the CERTEN validator network, which independently re-executes the verification of a resolved authorization and produces the proofs the execution layer consumes. This network is distinct from the consensus validators of the Accumulate blockchain and is described in Section 5.4.

## 4.1 Authority Layer

The Authority Layer consists of the external systems, roles, and individuals responsible for institutional decision-making.

These authorities include compliance systems performing AML and KYC validation, risk engines evaluating exposure and collateralization, treasury systems managing asset movement, operational workflows coordinating approvals, and human participants acting within defined roles. In addition, external authorities such as third-party compliance providers, data oracles, and specialized regulatory services may participate as part of the governance process.

Each authority operates within its existing environment and evaluates policy according to its own logic. CERTEN does not replace, replicate, or reinterpret institutional policy. Decisions such as whether a transaction meets compliance requirements, satisfies risk thresholds, or adheres to internal controls are performed entirely within the systems that already govern those processes.

Authorities participate in governance by producing cryptographic signatures tied to their identities. These signatures do not represent transaction execution, but rather attest to the completion of decision-making within the authority's domain. In this way, CERTEN captures the outcome of institutional processes without requiring those processes to be reimplemented.

CERTEN integrates these authorities by mapping them into its identity framework. Each authority is associated with a corresponding identity, allowing its participation to be verified as part of a governance process. This mapping enables institutions to reflect their organizational structure directly within the governance system, preserving the relationship between roles, responsibilities, and authority.

Institutions retain their existing infrastructure. Policy logic is not duplicated, and no new decision-making component is introduced into the approval path.

### 4.2 CERTEN Core

CERTEN Core resolves governance into a deterministic and verifiable decision.

It aggregates cryptographic participation from authorities mapped within the identity framework and evaluates whether all required identities have participated and whether defined thresholds have been satisfied. This evaluation is performed using Accumulate's identity-based architecture, where identities, signature hierarchies, and authorization structures are explicitly defined.

CERTEN Core does not evaluate institutional policy logic. It does not determine whether a compliance check is correct or whether a risk assessment is valid. Instead, it verifies that the authorities responsible for those decisions have participated according to the defined governance structure. This preserves a clear separation between decision-making and verification.

Governance is expressed through structured identity hierarchies using Key Books and Key Pages, which define required categories of approval and valid methods of satisfying those approvals. These structures enable the expression of complex governance requirements, including role-based approvals, quorum thresholds, hybrid human and system validation, and conditional participation paths.

Once all required participation has been collected, CERTEN Core resolves governance deterministically. The result is a governance decision that is independent of execution environment, asset location, or application interface.

CERTEN Core resolves governance on Accumulate, and the validator network independently re-executes that resolution and generates a cryptographic proof encoding the fact that all required authorities have participated and that all governance requirements have been satisfied. The proof serves as a portable authorization artifact that can be consumed by execution environments on any supported chain.

### 4.3 Authority Vaults

Authority Vaults are the enforcement gateways on destination chains. The execution layer on each destination chain comprises an anchor registry, a proof verifier, and per-institution accounts deployed at deterministic addresses. This document refers to that per-chain enforcement surface collectively as the Authority Vault, and the terms execution environment and execution contract refer to these contracts.

An Authority Vault receives a transaction request accompanied by a governance proof generated by CERTEN Core. The vault verifies the proof and executes the transaction only if the proof is valid. Any transaction that does not include a valid proof, or includes an invalid or incomplete proof, is rejected.

Authority Vaults are required for enforcement. They are the enforcement point for assets held under them: a transaction that does not present a valid governance proof is rejected, whether it originates from a wallet, an application, or an automated system.

Importantly, Authority Vaults do not evaluate policy logic or interpret governance rules. They do not contain embedded approval conditions, compliance checks, or decision-making processes. Their sole function is to verify proofs and enforce execution outcomes. This keeps execution environments simple, auditable, and resistant to complexity-driven vulnerabilities.

Existing wallets and applications integrate with CERTEN by routing transactions through Authority Vaults. In this model, the wallet manages user interaction and key custody, while CERTEN governs authorization. A transaction is initiated through the wallet, submitted for governance resolution, and then executed through the Authority Vault once a valid proof has been obtained.

This creates a clear operational flow: wallets initiate actions, authorities evaluate and approve, CERTEN resolves governance, and Authority Vaults enforce execution.

By separating these functions, CERTEN enables governance to be performed once and enforced on every chain where an Authority Vault is deployed.

# 5. Architecture

CERTEN implements its governance model using an identity-based architecture built on Accumulate, a public blockchain purpose-built around identities rather than accounts. The system maps external authorities into a deterministic identity framework, resolves authorization through structured signature participation, and produces verifiable cryptographic proofs that can be enforced across heterogeneous execution environments.

This architecture separates governance from execution at a protocol level. Governance takes place on the Accumulate blockchain, where identities, proposed actions, and governance state are recorded and where CERTEN Core resolves authorization; the execution layer refers to the minimal verification contracts (Authority Vaults) on destination chains, where proofs are enforced. Governance is performed on Accumulate, which is designed to express institutional authority; execution occurs in the minimal verification environments on destination chains. The linkage between these layers is established through cryptographic proof, which serves as a portable and deterministic representation of authorization.

## 5.1 Identity Framework (ADIs and Authority Mapping)

Accumulate Digital Identifiers (ADIs) are blockchain-anchored identities that are the persistent root of institutional authority, enabling governance decisions to be expressed, verified, and enforced independently of any single system, application, or custody provider.

CERTEN uses these identities to represent institutional entities, governance domains, systems, roles, and individuals within a unified identity framework.

An ADI is the cryptographic root of an institution's governance structure. It defines the hierarchy through which authority is expressed and enforced, including the relationships between roles, required approvals, and participation thresholds. This structure mirrors institutional organization rather than abstract cryptographic ownership, allowing governance to be expressed in terms that align with real-world operational models.

Each authority in the Authority Layer is mapped to an identity within the CERTEN framework. These identities are organized into hierarchical structures that define authorization requirements for specific actions. External systems such as compliance engines, risk services, and operational workflows are integrated as first-class participants through their associated identities, enabling them to contribute directly to governance without modification of their internal logic.

Key Books and Key Pages provide the structural primitives through which governance is expressed. These constructs allow institutions to define both the categories of required approval and the acceptable methods of satisfying those approvals, enabling complex governance structures to be represented deterministically without embedding logic into execution environments.

The same framework accommodates autonomous agents without modification. An AI agent is represented as a principal within an ADI hierarchy, identical in kind to a human role or an external system. The agent occupies a defined position in a Key Page, subject to that page's signing threshold, and is bound by the other authorities that participate in the same structure. Limits and conditions are policy: they are evaluated by the policy engines participating as signers, which sign or withhold accordingly, rather than by Accumulate. In this model an agent is a scoped identity, not a privileged one. Section 5.5 details the agentic configuration.

### 5.1.1 Role-Based Authority Mapping

CERTEN's identity framework is designed to reflect both organizational structure and functional authority.

Authorities are defined as roles rather than as static cryptographic keys. Roles represent functional responsibilities such as compliance approval, risk validation, treasury authorization, or executive oversight. Individuals and systems are assigned to these roles according to institutional policy, and their authority is derived from that assignment rather than from key ownership alone.

Key Books map directly to roles, defining which categories of authority must participate in governance. Key Pages define how participation within a role can be satisfied, including thresholds, alternative participants, and fallback mechanisms.

For example, a compliance role may include both an automated AML system and a designated compliance officer. A risk role may include a quantitative risk engine and a senior risk manager. A treasury role may include a set of executives operating under a quorum requirement.

A transaction requiring compliance and risk approval does not depend on specific individuals or systems. It depends on participation from the required roles. Authority is therefore dynamic and context-dependent, allowing institutions to maintain continuity of governance even as personnel, systems, or organizational structures change.

### 5.1.2 Authorization Structure: Key Books and Key Pages

CERTEN expresses governance requirements through the composition of Key Books and Key Pages, enabling deterministic evaluation of complex authorization structures.

Key Books define the categories of approval required for a given action. Each Key Book represents a distinct role or functional domain, such as compliance, risk, treasury, or executive authorization. All Key Books associated with an action must be satisfied for governance to be complete.

Key Pages define the acceptable methods of satisfying each category of approval. Each Key Page specifies one or more valid participation patterns, including threshold requirements, alternative signers, and fallback paths. A Key Book may contain multiple Key Pages, any of which can satisfy the requirement for that category.

This structure results in conjunctive evaluation across Key Books, disjunctive evaluation across the Key Pages within a Key Book, and threshold evaluation within each Key Page. All required categories must be satisfied, and each category may be satisfied through one of several valid participation patterns.

For example, a transaction may require compliance approval, risk approval, and treasury authorization. Compliance approval may be satisfied by either an automated system or a human officer. Risk approval may require both a system-generated validation and human confirmation. Treasury authorization may require a quorum of senior executives.

This approach enables institutions to express governance requirements that include role-based approvals, quorum thresholds, hybrid human and system validation, conditional participation, and escalation paths. These requirements are expressed declaratively within the identity framework and evaluated deterministically without embedding logic into execution environments.

### 5.1.3 Dynamic Authority Assignment

Because authority is mapped to identities through ADIs, institutions can modify governance structures without requiring changes to execution environments.

Participants can be added or removed from roles, systems can be replaced, and organizational changes can be reflected immediately within the identity framework. These updates do not require smart contract modification, redeployment, or asset migration.

#### 5.1.4 Authority Vault Alignment

Authority Vaults are mapped to governance requirements through the identity framework. Each institution's execution-layer account is bound to its governing ADI. The account stores no role definitions; the authorization structure lives entirely on Accumulate.

Execution is permitted only when all required roles have been satisfied, sufficient participation thresholds have been met, and governance has been resolved by CERTEN Core. This ensures that enforcement reflects institutional intent as defined within the identity framework rather than static configuration embedded within execution environments.

### 5.2 Signature Participation Model

CERTEN resolves governance through structured signature participation rather than through conditional execution logic.

In traditional systems, execution environments evaluate conditions to determine whether an action is valid. In CERTEN, validation is performed through participation. Authorities signal completion of their decision-making processes by producing cryptographic signatures, and governance is resolved by verifying that the required set of signatures has been collected.

#### 5.2.1 Intent as the Unit of Authorization

Governance in CERTEN operates on a defined unit of work referred to as an Intent.

An Intent represents a proposed action requiring authorization. It includes a complete description of the action to be performed, the target assets and execution environments, and the governance requirements that must be satisfied. Intents are written directly to Accumulate, where they become immutable records associated with the governing ADI.

Authorities do not sign transactions directly. They sign the Intent. This ensures that all participants are authorizing the same action and that governance is resolved prior to execution.

Because Intents are recorded on Accumulate, they eliminate the need for off-chain coordination mechanisms such as file exchange, messaging systems, or intermediary services. All participants interact with the same canonical representation of the proposed action, reducing the risk of modification, miscommunication, or interception.

#### 5.2.2 Participation as Proof

Governance is resolved through participation rather than through evaluation of policy logic.

Each Intent defines a required set of participating authorities, expressed through Key Books and Key Pages. Authorities participate by signing the Intent after completing their respective evaluations within their own systems.

CERTEN Core aggregates these signatures and verifies that all required identities have participated and that all thresholds have been satisfied. The system does not evaluate the correctness of the underlying decisions. Participation itself is the proof that policy requirements have been met.

### 5.3 Governance Resolution

Once the required signatures have been collected, CERTEN Core resolves governance deterministically.

The system verifies the authenticity of each participating identity, the validity of each signature, the satisfaction of threshold requirements within each Key Page, and the completion of all required Key Books. This evaluation is performed using the identity structures defined within the ADI, ensuring that governance resolution is consistent, repeatable, and independent of execution environment.

If all requirements are satisfied, CERTEN Core produces a governance decision. This decision represents the completion of institutional authorization and is independent of any specific blockchain, application, or custody system.

The validator network then independently re-executes that resolution and generates a cryptographic proof encoding the outcome of the authorization process. This proof serves as a portable artifact that can be verified by execution environments across any supported network.

### 5.4 Proof Generation

Following governance resolution, CERTEN generates a compact cryptographic proof, the Proof of Intent, representing the authorization outcome.

Proof generation is performed by the CERTEN validator network: an independent set of validators, distinct from the consensus validators of the Accumulate blockchain, that runs its own Byzantine Fault Tolerant consensus, observes Accumulate, and independently re-executes the verification

pipeline described below. References to validators in the remainder of this document mean this network unless Accumulate's consensus is named explicitly.

Validators produce BLS aggregate signatures attesting to the proofs they have verified. A Proof of Intent is valid only if more than two-thirds of validator voting power attests to it. Validator accountability and network participation requirements are described in separate documentation and are not required to understand the operational architecture of the protocol.

The proof includes commitments to identity participation, verification of threshold satisfaction, and a reference to the governance state on Accumulate. It is designed to be portable, efficient to verify, and independent of the complexity of the underlying governance structure.

#### 5.4.1 Proof Pipeline

CERTEN implements a multi-phase proof pipeline that establishes an unbroken chain of trust from the original Intent through governance resolution and execution to verified effect on the destination chain.

The pipeline verifies five properties:

First, that the Intent exists and is included within a confirmed state of the Accumulate blockchain. This ensures that the action being authorized is canonical and immutable.

Second, that the state containing the Intent and associated signatures is valid, having been produced by Accumulate's Byzantine Fault Tolerant validator set with a verifiable chain of trust to genesis. This ensures that governance resolution is based on a valid and consensus-backed state.

Third, that the correct governance authority authorized the Intent. This includes verification that all required Key Books were satisfied, that thresholds within Key Pages were met, and that all participating identities are valid according to the defined governance structure.

Fourth, that a supermajority of validators attested to the correctness of the proof. This attestation is performed using BLS12-381 aggregate signatures, requiring participation from more than two-thirds of the validator set by voting power. Validators attest twice: once before execution, over the operation being authorized, and once after execution, over the verified result.

Fifth, that the authorized action produced its committed effect. After execution, validators wait for a configured confirmation depth on the destination chain and independently verify the outcome: for a contract call, the expected event committed in the Intent must appear in the transaction receipt, and the receipt itself must be proven included in the destination chain's state; where the

Intent specifies one instead, the expected state change must be present. Execution is confirmed by proof of effect, not by the absence of a revert. Each validator that verifies the effect produces a second attestation; when a supermajority is reached, a proof-result record, aggregate-signed by the attesting validators, is written back to Accumulate.

### 5.4.2 Cryptographic Construction

Proofs are constructed using a combination of signature aggregation and zero-knowledge verification.

Validator attestations are aggregated using BLS12-381 signatures, allowing multiple validator signatures to be combined into a single compact representation. This reduces the size of the proof and enables efficient verification on destination chains.

The aggregate signature verification and the associated Accumulate inclusion checks are executed within a Groth16 circuit off-chain. The destination chain verifies only the resulting succinct proof, which attests that those checks passed, without re-executing them. The circuit's public inputs bind the proof to the Accumulate block anchor containing the Intent, the Intent's execution commitment, and a commitment to the attesting validator set. Verification therefore establishes both that the required authorities participated on Accumulate and that a supermajority of validators attested to that fact. Authority derives from the institution's own signed intent, not from validator signatures: by design, compromising the validator set does not by itself permit an unauthorized action.

The resulting proof is constant in size and complexity regardless of the number of participating authorities, the depth of the governance hierarchy, or the number of validators involved.

### 5.4.3 Execution Commitment and Replay Protection

Each proof commits to the exact execution parameters of the authorized operation: the destination chain, the target address, the value, and a hash of the call data. An arbitrary contract call is therefore bound exactly as tightly as a native transfer; a native transfer simply commits an empty call data hash. For governed operations there is no separately trusted execution path; the planned Sovereign Exit described in Section 7 is a distinct, time-locked recovery path that is not reachable during normal operation. Changing the target, the value, or a single byte of call data invalidates the commitment, and the execution environment rejects the operation.

Commitments are single-use. Each anchored authorization is consumed on first execution, and re-submitting an already-used proof is rejected. A valid proof authorizes exactly one execution of

exactly one operation.

Both properties rest on ordering. The commitment is anchored on the destination chain before execution is attempted, and the runtime parameters of the outbound call are checked against it. Neither the exact-call binding nor the single-use property is available to a design that executes first and reconciles afterward.

Verification runs as a pre-condition rather than a post-hoc check. The enforcement logic executes before the outbound operation; if any check fails, nothing executes and no state changes.

### 5.4.4 Batching and Anchoring

Before an authorization can be enforced, its commitment must exist on the destination chain. Anchoring is therefore not only a cost optimization: it is the precondition that makes both the exact-call binding and the single-use property enforceable (Section 5.4.3).

Multiple governance events can be aggregated into a single commitment through the construction of a Merkle tree. The root of this tree is submitted to the destination chain, and individual proofs include inclusion paths linking them to the committed root. This allows many governance events to share a single anchoring transaction, reducing cost while preserving verifiability.

The protocol supports two anchoring modes, each corresponding to a different operational requirement.

**On-cadence anchoring**: governance proofs are aggregated over a configurable batching window (approximately 15 minutes). At the end of each window, the validator network constructs a Merkle tree of all proofs in the batch and anchors the Merkle root to the destination chain. Because the anchor must land before execution, the window is also the earliest point at which an operation in that batch can execute. This mode is intended for routine operations such as scheduled settlements, periodic treasury movements, and batch processing workflows where minutes-scale latency is acceptable.

**On-demand anchoring**: for time-sensitive operations, an immediate anchor request triggers a smaller dedicated batch, submitted within approximately 30 seconds plus destination chain block time. This mode is intended for use cases such as collateral adjustments, margin calls, and time-critical financial operations where immediacy matters more than batching efficiency.

Both modes produce the same on-chain proof format and are verified by the same destination-chain contracts. The mode used for a given operation is configured at request time.

### 5.4.5 Verification Characteristics

Proof verification on destination chains has a predictable and bounded cost.

On EVM-compatible chains, succinct proof verification requires a fixed amount of gas regardless of governance complexity or validator count. The only variable term is the Merkle inclusion path described in Section 5.4.4, which grows logarithmically with batch size and is independent of governance structure. The cost model is therefore independent of the number of signers and of the structure of the authorization hierarchy.

This contrasts with traditional multi-signature approaches, where cost scales with the number of participants and the complexity of the governance logic embedded within execution contracts, particularly on congested networks. Governance resolution occurs entirely on Accumulate and incurs no destination-chain cost. On the destination chain there are three operations: the anchor submission, whose cost is amortized across the proofs in its batch; the fixed-cost verification of the individual proof; and the execution of the authorized operation itself, whose cost is that of the underlying transfer or call. A governance structure involving many participants, multiple roles, and layered approval requirements therefore incurs the same proof verification cost as a simple authorization.

## 5.5 Autonomous Agents as Scoped Principals

Autonomous agents are becoming financial actors: proposing trades, moving treasury, and executing payments without direct human initiation. The agentic capabilities described in this section are an application of CERTEN's existing identity primitives and require no change to the underlying protocol. CERTEN governs an agent as a principal type within the identity framework already described. An agent is modeled as a scoped principal occupying a position in an ADI's authorization structure, not a privileged one.

An agent controls its own segregated on-chain account, but it holds only one position in that account's authorization structure and cannot move assets on its own. The agent proposes an Intent (Section 5.2.1); it cannot resolve governance on its own. A policy engine participates as a signer positioned so that the agent's proposal alone cannot satisfy the requirement: either in a separate Key Book, which must be satisfied conjunctively, or in a Key Page whose threshold cannot be met without it. When the agent proposes an action, the policy engine evaluates it against the account's policy and either signs or withholds. Authorization is therefore the conjunction of the agent's proposal and the participation of the policy engine and any human authorities. The agent's reasoning is non-deterministic; the authority that bounds it is

deterministic, on-chain, and scoped. This is the signature-participation model of Section 5.2, with the agent and the policy engine as two participating authorities. Because the authorization commits to the exact operation (Section 5.4.3), a compromised agent key is designed to be unable to substitute a different target, amount, or call data; the agent's on-chain account rejects anything other than the proven call.

**The user's policy engine is a signer given an identity, which is then assigned authorities within the hierarchy.** An agent may be bounded by the institution's own policy engine or a third-party's, a third-party compliance or risk service, and an external AI specialized in fraud, sanctions, or exposure evaluation. CERTEN provides the segregated accounts and the signer hierarchy; the policy logic lives in the signer. This preserves the protocol's core separation (Section 4.1): CERTEN verifies that the required authorities participated and does not evaluate the policy itself.

**Hierarchical containment.** Because authority is expressed through ADIs and Key Books and Pages, an agent's authority can be scoped, delegated, and revoked structurally:

- An agent can be granted a bounded sub-account under a constrained sub-identity for a specific task, with its own authority structure and its own policy signers. This provides hierarchical containment of a sub-agent.
- An agent can delegate a narrower scope to another agent for a specific action.
- Authority can be revoked from above at any time by the governing ADI, taking effect immediately and without redeploying execution code (Section 5.1.3).

**Accountability.** Every agent action is an Intent recorded on Accumulate and proven by participation. Accountability resolves to the human or organization that delegated the authority, scoped cryptographically by the ADI tree. The record establishes cryptographically under whose authority, and within what scope, an action was permitted. This is evidence of attribution; legal responsibility remains a matter for the relevant contracts and applicable law (Section 8.4).

**Standards interoperability (roadmap).** In February 2026, NIST launched its AI Agent Standards Initiative to define how autonomous agents authenticate, are authorized, and interoperate across enterprise systems, including adapting existing identity and authorization frameworks to agents. The model described in this section, in which each agent is an independent identity-bearing principal with scoped, revocable authority and an auditable action history, follows the same structure that work describes. The protocol is designed to interoperate with the emerging agent standards as the agent-facing surface matures. These interfaces are part of the development roadmap and are not yet implemented. A Model Context Protocol (MCP) interface is designed to expose authorization, scope-checking, delegation, and revocation to agent runtimes as native

tools. The protocol is designed to authorize machine-native payment flows such as x402 (an emerging agent payment standard) by validating the authority chain before settlement. Verifiable agent-identity standards such as ERC-8004 are designed to be consumable as inputs to authorization policy. Today the underlying primitives exist (ADIs, segregated accounts, signature participation, and the authorization proof described in Section 5.4); the runtime integrations that expose them to agent frameworks are forthcoming.

## 6. Protocol Flow (Transaction Lifecycle)

The CERTEN protocol defines a deterministic lifecycle through which institutional governance is translated into enforceable execution across blockchain environments. End to end, that lifecycle is eight steps.

1. **Intent creation.** An application or wallet interface constructs a representation of the proposed action, including the target assets, execution environment, and governance requirements, and writes it to Accumulate under the governing ADI. It becomes an immutable, canonical record, and every authority signs that same record (Section 5.2.1).

1. **Authority evaluation.** Designated authorities evaluate the proposed action within their own systems. Compliance systems perform regulatory checks, risk engines evaluate exposure, and human participants review according to institutional procedures. Each produces a cryptographic signature tied to its identity, attesting to its participation and not to execution (Section 4.1).

1. **Participation accumulation and governance resolution.** Signatures are submitted against the Intent record, where participation accumulates on-chain. CERTEN Core evaluates it against the structure defined by Key Books (required authorities) and Key Pages (valid satisfaction paths), and resolves the Intent when all required authorities have participated and all thresholds are satisfied (Sections 5.1.2, 5.3).

1. **Independent re-execution and proof generation.** The validator network observes the resolved state, independently re-executes the verification, and generates the Proof of Intent. The proof commits to the exact execution parameters: destination chain, target address, value, and call data hash (Sections 5.4, 5.4.3).

1. **Anchoring.** The proof is anchored to the destination chain, either on cadence within a batched Merkle commitment or on demand for time-sensitive operations (Section 5.4.4). **The anchor commitment is recorded on the destination chain before any execution is attempted**, for the reasons given in Section 5.4.3.

1. **Proof verification as a pre-condition.** The transaction is submitted to the execution layer, which is reachable only through an Authority Vault. The Vault verifies the succinct proof against the recorded anchor, and does so before the outbound operation runs. An invalid,

absent, or already-consumed proof is designed to produce no event, no state change, and no partial effect (Sections 4.3, 5.4.3).

1. **Execution.** If verification passes, the execution contract performs the requested action: transferring assets, updating positions, or calling other contracts. A valid proof authorizes exactly one execution of exactly one operation.

1. **Effect verification and write-back.** After the transaction reaches a configured confirmation depth, validators independently re-observe the result, verify that the committed effect occurred, and write a signed proof-result record back to Accumulate. Section 5.4.1 describes the verification and the second attestation in full.

The governing identity therefore holds not only the record that an action was authorized, but a multi-validator attestation that the exact authorized action executed and produced its committed effect. These properties hold under the trust assumptions stated in Section 10.3.

# 7. Security Model

CERTEN's security model is based on separation of concerns, cryptographic verification, deterministic governance resolution, and explicitly defined trust boundaries. Rather than concentrating control within a single system, CERTEN distributes responsibility across distinct layers, each with clearly defined roles and constraints.

CERTEN holds no customer keys and custodies no customer assets. Keys remain with the institution's authorities and their existing systems; assets remain in accounts the institution governs. The protocol verifies authority and produces proof of it.

At the Authority Layer, decision-making remains within institutional systems and processes. Compliance engines, risk systems, and human approvers are responsible for evaluating whether an action should be authorized. CERTEN does not attempt to validate the correctness of these decisions. Instead, it verifies that decisions were made by the correct authorities according to the defined governance structure. This ensures that institutional policy remains the source of truth while enabling cryptographic verification of participation.

Accumulate expresses and constrains governance structure through ADIs, Key Books, and Key Pages; enforcement itself remains with the Authority Vaults. These structures define who must participate and how participation is satisfied. Because governance is expressed declaratively within this framework, authorization requirements are deterministic and cannot be bypassed without modifying the governance configuration on Accumulate. This eliminates ambiguity in how authority is evaluated and ensures that governance outcomes are consistent across all execution environments.

The validator network provides trust-minimized computation and consensus. Operating under a Byzantine Fault Tolerant model, the network ensures that governance resolution and proof generation remain correct in the presence of adversarial behavior, provided that more than two-thirds of validator voting power follows the protocol (Section 10.3). No single validator can produce a valid proof independently. Proof generation requires participation from a supermajority of validators, and incorrect behavior is designed to be detected and addressed through accountability mechanisms within the network.

Cryptographic proofs are the enforcement boundary between governance and execution. A valid proof attests that all required authorities have participated and that governance requirements have been satisfied. Execution environments rely exclusively on proof verification and do not

evaluate governance logic directly. This prevents execution-layer compromise from bypassing governance, as any transaction lacking a valid proof is rejected.

Execution environments are intentionally minimal and do not contain embedded governance logic. Attack surface at the execution layer is limited to proof verification and transaction execution.

These enforcement properties are directly testable. Four failure modes are rejected on-chain. An operation whose target, value, or call data differs from the committed values is refused, because the runtime parameters no longer match the execution commitment. A fabricated or absent proof is refused before anything runs. A proof that has already been consumed is refused on re-submission, preventing double execution. And because the checks run as pre-conditions to the outbound operation, a failing check produces no event, no state change, and no partial effect.

CERTEN eliminates reliance on off-chain coordination mechanisms. Intents are written directly to Accumulate, and all participation occurs through cryptographic signatures associated with those intents. This removes intermediate steps where transactions might otherwise be modified, intercepted, or misrepresented. The canonical representation of an action is immutable and shared across all participants, ensuring consistency throughout the governance process.

The system is resilient to compromised interfaces and wallets. Because authorization depends on satisfying governance requirements rather than on individual keys, a compromised interface cannot unilaterally authorize a transaction. Exposure of a subset of keys is designed not to be sufficient to authorize a transaction: execution still requires participation from the required authorities under the defined governance structure.

If the governance layer itself becomes unavailable, institutions still need a way to recover control. CERTEN specifies a path toward protocol-independent recovery through the Sovereign Exit mechanism, which is planned for release before mainnet and is not yet implemented. As designed, it introduces an alternative high-threshold signing path that would allow institutions to regain direct control over assets in the event of network failure or systemic disruption. A time-locked safeguard is designed to prevent use of this path under normal operating conditions.

Finally, the separation of governance from execution ensures that institutions retain control over their governance structures independent of any specific implementation or service provider. Governance can be reconfigured, migrated, or recovered without dependency on execution environments or third-party systems.

# 8. Regulatory Alignment

CERTEN is designed to align digital asset control with emerging regulatory frameworks by making authority explicit, verifiable, and enforceable at the protocol level. CERTEN produces cryptographic evidence of governance that regulators, auditors, and counterparties can verify independently.

## 8.1 UCC Article 12: Exclusive Control

UCC Article 12 establishes a new legal standard for control of digital assets, defining exclusive control of a controllable electronic record. The standard is generally understood to contemplate technical means of control, characterized by three core elements: the ability to enjoy the benefits of the asset, the ability to prevent others from exercising control, and the ability to transfer the asset.

CERTEN's architecture is designed to map to these requirements.

Exclusive control is designed to be established through the governance structure on Accumulate. The ADI defines the only valid authorization hierarchy capable of producing a governance proof. No other entity, including CERTEN itself, can authorize transactions without satisfying the defined governance requirements.

Prevention of unauthorized access is enforced at the execution layer. Authority Vaults will not execute any transaction unless accompanied by a valid governance proof. Because proof generation requires participation from the defined authorities, a party that cannot satisfy those requirements is designed to be unable to move assets held under an Authority Vault.

Transfer capability is preserved through the ability of the governing ADI to initiate and authorize transactions. Institutions retain full operational control over assets through their governance structures.

CERTEN is also designed to address the "system" requirement under UCC Section 12-105 by providing a protocol-native mechanism for demonstrating control. Governance decisions are recorded, resolved, and proven within a deterministic system, allowing institutions to produce cryptographic evidence of control rather than relying on contractual claims.

In collateralized finance scenarios, CERTEN is designed to enable automated enforcement of control through mechanisms such as programmatic revocation of authority. For example, a

lender's governance structure can remove a borrower's signing rights in response to a trigger event, achieving real-time enforcement of control conditions without manual intervention.

## 8.2 MiCA Article 75: Asset Segregation and Safekeeping

Under MiCA Article 75, crypto-asset service providers that provide custody are generally required to maintain segregated asset safekeeping, provide sufficient records for supervisory enforcement, and ensure that clients retain access to their assets without undue barriers.

CERTEN is designed to address these requirements through its architecture.

Segregation is achieved through distinct execution-layer accounts governed by separate authorities on Accumulate. Each institutional client can be associated with its own governance structure and execution account, which is designed to support the segregation expectations described above rather than an omnibus custody model.

Auditability is provided through Accumulate, where all governance events are recorded immutably. Every authorization decision, participation event, and proof generation step is preserved as part of the system state, enabling complete reconstruction of the authorization history. Because post-execution attestations are written back to Accumulate (Section 5.4.1), the record extends beyond authorization to include multi-validator confirmation that each authorized action executed and produced its committed effect.

Client access is designed to be preserved through the separation of governance from execution and, once implemented, the planned Sovereign Exit mechanism. Because governance structures belong to the institution rather than to a service provider, the architecture is designed to keep access from being restricted by operational dependencies.

## 8.3 Jurisdictional Control and Data Residency

CERTEN enables jurisdictional requirements to be expressed directly within governance structures, allowing regulatory compliance to be enforced as part of authorization rather than as an external or advisory process.

Jurisdiction is treated as an explicit authority within the identity framework. Governance structures can require participation from authorities associated with specific jurisdictions, ensuring that regulatory approval is a prerequisite for execution. For example, a transaction involving assets subject to regional regulation may require authorization from a jurisdiction-specific compliance authority before it can proceed.

Institutions can maintain localized control by assigning jurisdiction-specific roles within their governance structures. At the same time, global workflows can be constructed by requiring coordinated participation across multiple jurisdictions. This allows organizations to enforce regional compliance requirements while maintaining unified operational processes.

CERTEN also supports delegation of jurisdictional authority to specialized providers. External compliance services can be integrated as participating authorities, contributing signatures that attest to regulatory validation without requiring their internal logic to be embedded within execution environments.

Data residency requirements are preserved by limiting the movement of sensitive data. Institutional systems perform evaluations locally, and only cryptographic attestations of participation are transmitted to Accumulate. This design is intended to keep sensitive information within jurisdictional boundaries while still enabling global verification of governance outcomes. Whether a given deployment satisfies applicable data-residency requirements depends on its configuration and is subject to the considerations in Section 8.4.

Jurisdictional requirements are resolved on Accumulate and are part of what the proof attests. An Authority Vault executes only where those requirements were satisfied, because no valid proof exists otherwise. This is designed to make jurisdictional participation a condition of execution rather than an advisory step.

## 8.4 Legal and Interpretive Considerations

While CERTEN is engineered to align with regulatory frameworks such as UCC Article 12 and MiCA, the ultimate determination of compliance remains subject to judicial interpretation and evolving regulatory guidance.

The architecture is designed to provide a technical basis for demonstrating control, segregation, and auditability. However, institutions implementing CERTEN should obtain independent legal advice to ensure that their specific configurations and use cases meet applicable regulatory requirements.

# 9. Ecosystem and Use Cases

CERTEN supports a range of applications by providing a programmable governance layer for digital assets. By separating governance from execution, the protocol allows institutions and applications to integrate complex, institutional-grade control without embedding policy logic into execution environments.

The system is designed to support both existing institutional workflows and new classes of applications that require coordinated control across multiple parties, systems, and jurisdictions.

## 9.1 Secured Lending and Collateral Management

Secured lending represents a primary use case for CERTEN.

In these scenarios, multiple parties must coordinate control over assets, including borrowers, lenders, custodians, and potentially third-party agents. Traditional approaches rely on custodial arrangements or contractual agreements to enforce control, introducing counterparty risk and limiting verifiability.

CERTEN enables deterministic enforcement of collateral control by requiring participation from all relevant authorities before assets can be moved. Governance structures can encode lending agreements, ensuring that collateral cannot be released, transferred, or rehypothecated without satisfying defined conditions.

This allows lenders to achieve verifiable control over collateral while allowing borrowers to retain operational participation within defined constraints.

## 9.2 Treasury Management

Institutional treasury operations require coordinated control across multiple stakeholders, including finance teams, risk management, and executive oversight.

CERTEN enables treasury workflows to be expressed directly within governance structures, allowing institutions to define approval hierarchies, thresholds, and operational controls without embedding logic into execution systems.

Transactions such as fund transfers, liquidity management, and investment allocation can be governed through structured participation, ensuring that all required approvals are obtained prior to execution.

### 9.3 Custody Orchestration

CERTEN enables orchestration across multiple custody systems without requiring assets to be consolidated into a single platform.

Institutions can maintain assets across different custodians, wallets, or blockchain environments while enforcing a unified governance model. Execution remains distributed, but control is centralized at the governance layer.

### 9.4 Cross-Institution Workflows

Many financial operations require coordination between independent institutions, each with its own governance requirements.

CERTEN enables cross-institution workflows by allowing multiple governance structures to participate in the authorization of a single Intent. Each institution's authorities can contribute signatures according to their own policies, and execution occurs only when all required governance conditions across all parties have been satisfied.

This enables complex workflows such as syndicated lending, multi-party asset management, and coordinated settlement without requiring shared custody or centralized control.

Where workflows span independent institutions, an institution can run its own permissioned enforcement network, so governance and transaction activity stay within that network, on validators the institution owns, and cross-institution coordination does not require disclosing activity to the network at large.

### 9.5 Proof-Gated Contract Execution

Because an authorization commits to the exact call rather than to a category of action (Section 5.4.3), a sensitive contract function can be placed behind governance wherever the function's caller can be restricted to an Authority Vault. The application classes this opens include treasury execution, voting tallies, bridge and settlement release, and staged escrow.

In governance and treasury execution, a treasury spend or parameter change executes only if the underlying proposal was authorized, and effect verification requires the corresponding execution event, so a substituted target or amount cannot pass. In voting systems, the tally-execution call fires only against the proven result. In bridge and settlement flows, funds can be released only on proof of the source-chain event, and the single-use commitment is designed to prevent a second

release of the same transfer, while effect verification can additionally require the processed-state change on the destination. At the application level, operations such as minting, withdrawal, contract upgrade, or configuration changes become proof-gated and bound to their exact arguments. Escrow flows extend this to value-bearing sequences: funds can be held and released in stages, with each step individually authorized and verified.

### 9.6 Emerging Application Classes

By providing a programmable governance layer, CERTEN supports application patterns that require authority to be resolved independently of execution.

These include applications requiring coordinated control across multiple chains, compliance-gated execution, real-time governance in financial markets, and programmable institutional workflows that integrate human and system decision-making.

A growing class of these applications is agentic: autonomous agents managing treasuries, executing cross-chain strategies, and transacting with other agents. An agent operator can run many agents, each controlling its own segregated account under a single governance hierarchy, with per-agent policy signers and per-agent revocation. Section 5.5 describes the mechanism.

# 10. Status, Trust Assumptions, and Limitations

The applications described above assume a protocol that is still being completed. This section states what is built, what the protocol assumes, and what it does not do. Statements of capability elsewhere in this document should be read against it.

## 10.1 Forward-Looking Statement

This document describes the design and current testnet implementation of the CERTEN protocol and contains forward-looking statements. Capability descriptions reflect either current testnet state or protocol design intent, as distinguished in Section 10.2. Forward features, release timing and target dates, configuration values, cross-chain coverage statements, and statements about alignment with regulatory frameworks whose interpretation is still developing are subject to change as the protocol matures and as third-party security audits inform design refinement. Actual results may differ from those described. CERTEN undertakes no obligation to update these statements. This document is a technical description and is not an offer to sell or a solicitation of an offer to buy any security.

## 10.2 Implementation Status

The protocol core is complete and running on test networks. Mainnet launch is targeted for Q4 2026, contingent on security audit completion and validator network operational validation.

The Sovereign Exit mechanism (Section 7) is specified and planned for release before mainnet. It is not implemented.

The agent-runtime integrations described in Section 5.5, including a Model Context Protocol interface, x402 payment-flow authorization, and consumption of verifiable agent-identity standards, are on the development roadmap and are not implemented. The primitives they would expose (ADIs, segregated accounts, signature participation, and the authorization proof of Section 5.4) exist today.

Validator accountability mechanisms depend on the staking model, which is not yet operational. Where this document refers to incorrect validator behavior being detected and addressed, that is a design property of the planned model.

Specific configuration values in this document, including validator counts, batching windows, and confirmation depths, are operational parameters subject to change.

Where this document refers to a supported chain or a supported network, it means a chain the protocol is built to enforce on. That is a larger set than the set of chains where the execution layer is currently deployed, and enforcement is available only on the deployed set. Statements about supported chains are therefore statements about protocol capability, not about current coverage.

### 10.3 Trust Assumptions

**Validator supermajority.** Proof generation requires that more than two-thirds of CERTEN validator voting power follows the protocol. If honest voting power falls below that threshold, no quorum is reachable and no proof is issued, which is a liveness failure. If instead two-thirds or more collude, the assumption is violated in the other direction, and the protection that remains is the design property described in Section 5.4.2: authority derives from the institution's own signed intent, and the circuit binds the proof to inclusion and authority on Accumulate, so by design a compromised validator set does not by itself permit an unauthorized action. That property is a design intent that has not been independently verified (Section 10.6), and it should not be relied on as a substitute for the supermajority assumption.

**Accumulate consensus.** Governance state, Intents, and participation records live on Accumulate. The protocol inherits that chain's own Byzantine Fault Tolerant consensus assumption.

**Correct governance configuration.** Governance cannot be bypassed without modifying the governance configuration on Accumulate. That configuration is itself governed by the institution's ADI hierarchy, so an institution that misconfigures its own authority structure, or that permits authority over that structure to be captured, has not been protected against by the protocol. Correct configuration of the governing ADI is an institutional responsibility.

**Key compromise below the satisfying threshold.** The guarantee in Section 7 that exposure of a subset of keys is insufficient to authorize a transaction assumes that the compromised keys do not themselves constitute a satisfying set across the required Key Books and Key Page thresholds. An institution that concentrates a satisfying set in one place has reduced the assumption to a single point of failure.

**Cryptographic and destination-chain assumptions.** Verification rests on the soundness of the Groth16 construction, including its trusted setup, and on the hardness assumptions underlying BLS12-381. Effect verification additionally assumes the destination chain does not reorganize past the configured confirmation depth.

## 10.4 Liveness and Censorship

The protocol is designed for safety before liveness. If the validator network stalls or declines to attest to a validly resolved Intent, no proof is produced, and no execution occurs. Assets are not moved incorrectly; they do not move at all. Governance resolution itself continues on Accumulate, so the record of what was authorized is durable and survives the outage.

Censorship of a specific institution by a colluding sub-supermajority has the same shape: it withholds proof issuance rather than producing an incorrect authorization. The same is true one layer down, where a destination chain that censors the anchor or execution transaction blocks enforcement without compromising it. In every case the failure is to the institution's ability to act, not to the correctness of what it has authorized.

For sustained unavailability, the Sovereign Exit path (Section 7) is the specified recovery mechanism. It is time-locked so that it cannot be used to circumvent governance during normal operation, and, as noted above, it is not yet implemented. Until it ships, institutions should treat prolonged validator-network unavailability as a liveness risk to governed asset movement.

## 10.5 Out of Scope

**Policy correctness.** CERTEN verifies that the required authorities participated. It does not evaluate whether their decisions were correct. A governance structure that authorizes a bad transaction will produce a valid proof of that authorization.

**Financial-crime detection.** The protocol enforces participation by designated compliance authorities. It does not itself perform AML screening, sanctions checks, or transaction monitoring; those remain with the institutional systems mapped as authorities.

**Data residency.** Only cryptographic attestations of participation are transmitted to Accumulate, and institutional systems evaluate locally. Whether a given deployment satisfies applicable residency requirements depends on its configuration (Sections 8.3, 8.4).

**Legal determination.** Alignment with UCC Article 12, MiCA, and other frameworks is an engineering design objective. Compliance determinations are made by courts and regulators. Institutions implementing CERTEN should obtain independent legal counsel (Section 8.4).

### 10.6 Assurance Status

Third-party security audits have not yet been performed, and no enforcement property described in this document has been independently verified by an external reviewer.

This is the boundary the document ends on deliberately. Digital assets are controlled by keys and institutions are governed by identity; the architecture described here closes that gap by resolving authority before execution and proving it afterward. Whether the implementation discharges the design is a question for the audits, and this section will be updated when they are complete.