Provable Compliance

A Protocol for Runtime Compliance Evidence and Transaction-Specific Decisioning

CHAINIT®

Executive White Paper

ChainIT Compliance Protocol — CIT-PC-WP-4.0

Architecture and Source Basis

September 2026

Companion document: ChainIT Provable Authority (CIT-PA-WP-7.0).

Authors

Jeremy Blackburn, Chief Executive Officer
Tim Hines, Chief Product Officer
Matthew Koepp, Chief Technology Officer
Russell Lessard, Chief Compliance Officer
Jason Patrick, Chief Commercial Officer

This paper describes the ChainIT Provable Compliance architecture. It does not constitute legal, regulatory, banking, accounting, security-certification, or patentability advice, and it does not replace a regulated institution's own AML/CFT or sanctions program. Deployment configurations, provider coverage, and service levels vary by implementation.

© 2026, Scientia Potentia Est. II, LLC. All rights reserved.

This white paper and the information contained herein are the exclusive property of Scientia Potentia Est. II, LLC and are protected by United States and international copyright laws.

Permission is granted to recipients to access, view, download, print, and retain copies of this white paper solely for their personal, informational, or internal business purposes. Recipients may share an unmodified copy of this white paper in its entirety, provided all copyright and proprietary notices are retained, and no fee is charged for such distribution.

Except as expressly permitted herein, no part of this publication may be reproduced, distributed, transmitted, displayed, published, modified, translated, reverse engineered, incorporated into other works, or used for commercial purposes in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of Scientia Potentia Est. II, LLC.

No license, whether express, implied, by estoppel, or otherwise, is granted to any intellectual property rights, including patents, patent applications, copyrights, trademarks, trade secrets, or other proprietary rights of Scientia Potentia Est. II, LLC, except for the limited right to access and use this white paper as expressly provided above.

Unauthorized copying, modification, disclosure, distribution, publication, or commercial exploitation of this document, or the information contained herein is strictly prohibited.

Contents

Definitions and Document Precedence 3
Executive Summary 7
1. The Problem: Compliance Evidence Ages and Context Changes 8
2. The ChainIT Model: Evidence, Policy, Authority, and Decision 10
2.1 Subject neutrality and verified identity foundation 10
2.2 ARP, Delegated Authority, and Agent Authority 10
2.3 Evidence Assertion VDTs 10
2.4 Compliance Policy Profile 11
2.5 BRE, Workflow Engine, and Compliance Decision VDT 11
2.6 Compliance as an input to the final Authority Protocol 12
2.7 Session eligibility flow 14
2.8 Transaction policy and commit-time flow 14
2.9 Agent Subject Profile boundary 16
2.10 Pactvera, lifecycle VDTs, Valitorum, and later exceptions 17
3. Runtime Re-Verification at the Point of Reliance 17
4. Evidence Domains 19
5. Regulatory Landscape and Current Status 21
6. Risk Tier, Decision States, and Enforcement 23
7. Design Principles, Evidence and Decision Lifetimes, and Residual Risk 23
8. Illustrative Scenarios 25
9. Privacy, Disclosure, and Evidentiary Controls 27
10. Business Value and Measurable Outcomes 28
11. Implementation Priorities and Controlled Deployment 29
12. Conclusion 30
References and Source Basis 31

Definitions and Document Precedence

Authority definitions control

For all terms, artifacts, subject classifications, and process steps defined in ChainIT Provable Authority, CIT-PA-WP-7.0 controls. This paper adopts those definitions and flows by reference and defines only the compliance-side evidence, policy, and decision architecture. Any abbreviated description in this paper is explanatory and does not modify the Authority Protocol. [23]

The shared Authority Protocol terms below are reproduced or closely restated from CIT-PA-WP-7.0 so that the two papers can be read together without creating a second or conflicting authority model. Compliance-specific terms are then defined for this paper. Definitions are provided for reader clarity and do not themselves constitute legal, regulatory, product, or security specifications.

Term	Definition
Agent Authority VDT	The append-only record of a grant of delegated authority from an authorized human or organizational principal to a registered agent, and the agent-specialized form of the Delegated Authority VDT. Each entry immutably records the granting principal, the governing ARP and its version, the registered agent, permitted purpose, counterparties, transaction classes, rails, per-transaction and aggregate value limits, effective period, step-up thresholds, redelegation rule, and revocation conditions. An agent holds no authority of its own. Present validity is resolved at the reliance event against current ARP status and the applicable freshness bound. It is not a bearer credential.
Agent Registration VDT	A versioned record identifying an autonomous workload's organization, responsible party or role, tenant, deployment, software or workload identity, permitted tools and APIs, risk class, attestation method, registered public key, status reference, and version history. It establishes what the workload is, not what it may do.
Agent Subject Profile	The identity and containment controls that exist because the acting subject is an autonomous workload rather than a person: the Agent Registration VDT, the attested workload key and ephemeral session-key hierarchy, and the sovereignty boundary. The profile adds no authority concept of its own; an agent exercises delegated authority under the ARP in the same way a human delegate does, evidenced by an Agent Authority VDT.
Authority Policy Profile (APP)	The versioned rule set selected for a given reliance event, which may vary by organization, product, role, subject class, counterparty, transaction type, value, payment rail, jurisdiction, risk tier, and intended purpose. It is the authority-side counterpart to the Compliance Policy Profile and is versioned so that a later reviewer can determine exactly which rule set produced an authority decision.
Authority Protocol	The general ChainIT protocol for resolving whether an identified subject may perform a specific proposed action at the moment of reliance. It is subject-neutral and rail-neutral: the same identity, authority, evidence, policy, digest, reservation, execution, and outcome-evidence controls govern individual-, group-, organization-, and agent-initiated actions, including organization-controlled scheduled-workflow initiations.
Authority Resolution Pactvera (ARP)	The canonical, versioned organizational authority record: who may act, in what role, for what purpose, within what limits, during what effective period, under what quorum or separation-of-duties requirements, and subject to what amendment or revocation.
Business Rules Engine (BRE)	The deterministic predicate-evaluation engine. It evaluates configured conditions against subject identity and assurance, ARP authority, registration and attestation where the subject is a workload, evidence, status freshness, jurisdiction, scope, session risk, and—for a transaction—the exact transaction, current capacity, required approvals, and rail-specific constraints. It returns explicit, reason-coded true/false predicate results. The BRE does not itself perform risk scoring or assign a disposition; it runs within the ChainIT Workflow Engine.

Term	Definition
Canonical transaction digest	A deterministic hash of a canonical transaction object—including payer, source, payee, destination, amount, currency or asset, rail, fees, nonce, validity window, and rail-specific parameters—computed under a fixed encoding rule so that any material change produces a different digest.
ChainIT ID	The verified identity anchor for an individual, established through authoritative-source verification, biometric and liveness controls, and privacy-preserving, portable identity storage.
ChainIT Org ID	The legal-entity identity anchor for an organization, which may reference entity registration, ownership, officers, governance, and authorized representatives.
ChainIT Pay	The ChainIT payment-execution platform intended to serve as the EAC enforcement boundary where the applicable Authority Protocol profile is deployed; a compatible partner rail adapter may serve this function in another implementation.
Compliance Decision Permits	The compliance-side predicate consumed by the Authority Protocol. It is true only when the applicable Compliance Decision VDT has a final Allow disposition for the stated reliance event after every required compliance control has been completed and the decision has been re-evaluated. It does not establish authority, session eligibility, transaction authority, capacity, or payment authority.
Compliance Decision VDT	The signed, time-bounded, purpose-specific record produced by an organization's configuration of the ChainIT Workflow Engine, recording whether present evidence and policy permit a proposed exercise of authority. It gates present exercise; it does not amend, suspend, or erase the governing ARP. An Allow disposition means compliance-side continuation only and never independently authorizes payment.
Compliance Policy Profile (CPP)	The versioned rule set selecting the compliance evidence, freshness bounds, predicates, review conditions, disclosure rules, and other compliance-side requirements applicable to a reliance event. It may vary by institution, regulated entity, product, role, subject, counterparty, transaction type, value, rail, payer and payee jurisdiction, customer category, risk tier, and intended purpose.
Delegated Authority VDT	A portable artifact that references the governing ARP and exposes only the scope of authority needed by a given delegate, agent, or relying party without replacing or superseding the ARP itself. Its agent-specialized form is the Agent Authority VDT.
Disposition	The explicit outcome produced by an organization's configuration of the ChainIT Workflow Engine from BRE predicate results: Allow, Allow with Controls, Step-Up, Review, Hold, Reject, Prohibit, or Stale/Unknown. The organization configures the disposition set to match its own policies and regulatory obligations. Disposition and risk tier are evaluated independently.
Evidence Assertion VDT	A record of a single sourced fact or institution-generated state, including its subject, source class, source, source version, retrieval and effective time, expiration or review time, jurisdiction, match or confidence state, permitted purpose, and privacy classification. Evidence Assertion VDTs are never aggregated into a universal "compliant" status.
Execution Authorization Credential (EAC)	A single-use, short-lived credential authorizing one exact transaction for one audience, bound to the acting session or approved subject, transaction digest, reservation, status epoch, and expiration, and consumed atomically at commit.
Execution Authorization Lifecycle VDT	A permanent, append-only evidence record of EAC issuance and terminal handling—consumed, expired, canceled, or rejected. The EAC itself is not stored as a reusable ledger object, and earlier lifecycle events are never modified or overwritten.
Pactvera	The ChainIT transaction-logic and append-only evidence framework linking Validated Data Tokens across a transaction's lifecycle.
Provable Compliance	The property of a system in which compliance-relevant evidence, rule selection, predicate evaluation, resulting disposition, freshness, and disclosure treatment are attributable, time-bounded, purpose-specific, and independently verifiable. Provable Compliance supplies the compliance-side decision consumed by the Authority Protocol; it does not itself confer authority.
Reliance event	The moment at which a relying party depends on identity, authority, evidence, or policy state—session issuance or renewal, a transaction proposal or payment initiation, a human step-up approval, a scheduled review, or a source-change or material-risk event. Freshness and policy are evaluated at the reliance event rather than inherited from onboarding.

Term	Definition
Reservation	The atomic hold of transaction capacity against a budget or limit, performed before EAC issuance so concurrent requests cannot commit against the same capacity twice.
Risk tier	A classification—Tier 1–Low, Tier 2–Standard, or Tier 3–High—assigned to a transaction based on factors such as payee history, value, reversibility, and behavioral or device anomalies. It determines minimum verification rigor. The tier is assigned by the organization's configuration of the ChainIT Workflow Engine, not by the BRE, and it does not itself determine the disposition.
Session Authorization Credential (SAC)	A short-lived, sender-constrained credential that permits proposal activity, evidence retrieval, and defined API activity, but which rail adapters must reject as payment authority. A session credential is never payment authority, whether the session belongs to a workload or a signed-in person.
Session Eligibility Decision VDT	A session-context decision recording whether the authenticated subject may open or continue a session that enables consequential action, referencing identity assurance, the ARP, evidence, status, jurisdiction, scope, and policy version. Where the subject is a workload, it additionally references the Agent Registration VDT, Agent Authority VDT, attested deployment, and applicable tool scope. It is not transaction-specific and cannot authorize payment.
Sovereignty boundary	The architectural line beyond which an AI model or autonomous agent may reason, gather evidence, and propose an action, but cannot obtain unrestricted access to payment-account credentials, custody keys, or final execution authority; that authority remains with the deterministic control plane.
Status epoch / status freshness	The signed timestamp or snapshot boundary used to determine whether cached non-revocation or evidence status is still acceptable for a given risk tier versus requiring a live status or source interaction.
Subject of authority	The party whose authority is being resolved: a verified individual, a group acting under a quorum or separation-of-duties rule, an organization acting through an authorized representative, or a permitted software agent. A scheduled workflow is not a fifth subject class; it is an organization-controlled initiation mechanism acting for an identified organization under the governing ARP.
Supplemental Valitorum	A permanent sealed evidence package for a later post-terminal exception—such as a return, reversal, recall, chargeback, or dispute—that references the original Valitorum without altering it.
Transaction Policy Decision VDT	A decision bound to one canonical transaction digest, recording risk tier, disposition, policy version, evidence references, ARP and subject references, required approvals or controls, expiration, and reason codes. It is newly derived per transaction and is not reusable as a standing status.
Validated Data Token (VDT)	A cryptographically verifiable digital record representing validated data concerning a person, organization, asset, service, event, decision, or transaction. A change is represented by a new linked VDT rather than alteration of a prior immutable record.
Valitorum	The final sealed evidence record generated for a completed or otherwise terminal transaction lifecycle under a defined completeness rule. A sealed Valitorum is never altered; later exceptions are captured in a linked Supplemental Valitorum.
Valitorum Service	The ChainIT service that creates, verifies, retrieves, or presents a Valitorum and, where applicable, a Supplemental Valitorum.
Workflow Engine	The organization-configurable orchestration layer in which BRE predicate results, risk-tier assignment, required approvals, review states, and other configured conditions are composed into a disposition and downstream action. The organization is responsible for the policy logic it configures and for its use of the resulting disposition, subject to applicable law and contractual allocation among ChainIT, the organization, payment providers, evidence providers, and other participating parties.

Executive Summary

Provable Authority asks whether an identified individual, group, organization, or permitted software agent is authorized to perform a particular action. Provable Compliance addresses a different question: whether the evidence and policy conditions required for the present action are sufficiently current, complete, and favorable for that authority to be exercised now. The final definitions and execution flows for the shared Authority Protocol are those in CIT-PA-WP-7.0; this paper supplies the compliance-side evidence and decision architecture consumed by those flows. [23]

The distinction matters because compliance is neither a permanent badge nor a universal statement that a person or organization is "in good standing to do anything at all." AML monitoring, sanctions, politically exposed person status, criminal-history information, government-credential state, licensing, KYC/KYB, and payment-transparency obligations operate differently. Some are authoritative facts, some are qualified third-party indicators, and some are institution-generated judgments. Their consequences depend on the institution, product, role, subject class, transaction, counterparty, jurisdiction, risk tier, and intended purpose.

The ChainIT model therefore uses modular Evidence Assertion VDTs and a reliance-event-specific Compliance Decision VDT. ChainIT ID and ChainIT Org ID establish verified subjects. The ARP remains the canonical organizational authority record, and a Delegated Authority VDT—or its agent-specialized Agent Authority VDT—exposes a bounded grant without replacing the ARP. Current Evidence Assertion VDTs preserve source, provenance, retrieval and effective time, confidence, permitted purpose, and privacy classification. A versioned CPP selects the applicable conditions. The BRE returns explicit, deterministic, reason-coded true/false predicate results. The organization's configuration of the ChainIT Workflow Engine composes those results into a signed, time-bounded Compliance Decision VDT.

A favorable Compliance Decision VDT does not establish session eligibility or authorize a transaction. It contributes the Compliance Decision Permits predicate to the final Authority Protocol. For a session, that predicate is evaluated with subject authentication, ARP or delegated authority, the APP, status, scope, and—where applicable—the Agent Subject Profile to produce a Session Eligibility Decision VDT and, only after a final Allow, a SAC. For a transaction, it is evaluated with the canonical transaction digest, authority, APP, risk tier, current capacity, required approvals, and rail constraints to produce the Transaction Policy Decision VDT. Controls and step-up must be completed and the transaction re-evaluated to final Allow before capacity reservation and EAC issuance. [23]

Runtime verification means that ChainIT evaluates evidence freshness and policy at the moment of reliance. It does not mean every external source is queried for every session. Each evidence domain has a source-specific and risk-specific freshness requirement. ChainIT may reuse a signed Evidence Assertion VDT while it remains fresh enough for the present context, perform a live or event-driven refresh when required, and produce Review, Hold, or Stale/Unknown when a source is unavailable, stale, or ambiguous. A change propagates only to the subject, activity, product, rail, counterparty, jurisdiction, or authority relationship that actually depends on it unless law or policy requires broader blocking.

The resulting compliance decision and its evidence references become part of the same append-only lifecycle used by Provable Authority. The operational EAC is not stored as a reusable ledger object; Execution Authorization Lifecycle VDTs record issuance and terminal handling. Each later transaction state is a new event. The Valitorum seals the completed or otherwise terminal evidence graph, and a later return, reversal, recall, chargeback, or dispute may be sealed in a Supplemental Valitorum that references—but never modifies—the original.

Core proposition

Provable Compliance does not ask whether a subject is

universally "compliant." It produces a signed, time-bounded, purpose-specific decision stating whether identified evidence and an identified policy permit compliance-side continuation for one reliance event. The final Authority Protocol still decides whether the subject may open a consequential session or commit an exact transaction.

1. The Problem: Compliance Evidence Ages and Context Changes

The concern ChainIT addresses is not that regulated institutions perform no ongoing monitoring. Banks, payment companies, money-services businesses, and other regulated organizations already maintain onboarding controls, transaction monitoring, sanctions screening, case management, customer-risk profiles, periodic or event-driven reviews, and escalation processes. U.S. customer-due-diligence rules expressly require ongoing monitoring and risk-based updating of customer information; they do not require every data element to be refreshed on one universal schedule. [1]

The operational gap is that relevant facts and judgments remain fragmented. Identity evidence may be in one system, organizational authority in another, sanctions results in a third, AML alerts in a fourth, and payment approval in a bank portal or ERP application. Even where each control is competently operated, a relying party may not be able to obtain compact, cryptographically attributable proof showing which evidence, policy, authority, and transaction context were current at the moment a decision was made.

The gap becomes more consequential as authority is delegated to software agents and scheduled workflows. A human may informally notice an unfamiliar payee, a changed bank account, an expired license, or an unusual pattern. An automated workflow executes the tools, data, and permissions it is given. ChainIT therefore places the same deterministic compliance and authority boundary in front of an agent proposal, a human-initiated wire, a group-approved ACH file, an organization-controlled scheduled payment, and an on-chain transfer. The subject authentication differs; the governing evidence, authority, policy, and execution controls do not.

The objective is not to replace an institution's AML/CFT, sanctions, licensing, privacy, or other compliance program. It is to make the institution's evidence, policy selection, predicate evaluation, disposition, authority context, and reliance event machine-verifiable at the moment of use and auditable after the event.

- Ongoing monitoring is not the same as a permanent status; evidence that was accurate at onboarding does not remain accurate by default.
- A favorable historical screening result does not establish that a subject is currently clear; sanctions, PEP, and entity status can change without notice.
- Compliance evidence gathered for one purpose or product does not automatically justify reliance for a different purpose, counterparty, or jurisdiction.
- A policy exception approved for one reliance event does not carry forward to the next unless the applicable CPP says it does.
- An unavailable or ambiguous evidence source is not the same as a favorable result; it requires a controlled Review, Hold, or Stale/Unknown

disposition.

Capability Status

This paper describes present-tense architecture to keep the control model legible. Not every artifact below is deployed in production in every implementation. Each principal component below is classified on two independent axes: whether it is built and deployed today, and what patent or documentary support currently exists for it. These are different questions — a capability may be deployed while representing potential new patent matter, or described in a filed application without yet being built. The matrix below is the single authoritative classification for this component set; the companion Pilot Measurement & Validation Plan (CIT-PC-PILOT-4.0) uses the identical classification, and the companion Architecture Diagrams & Flows (CIT-PC-DIAGRAMS-4.0) intentionally omits an implementation-status legend to avoid a second, competing classification.

Pending formal sign-off

This matrix reflects the current working classification. Before external distribution, Product, Engineering, and Patent Counsel should formally confirm each row and any change should be reproduced identically across all three companion documents.

Implementation status

Production: deployed and in current use. Development: being built or validated, not yet in general production use. Proposed: architecture is defined but not yet built. External dependency: supplied by a third party outside ChainIT's direct control.

IP / documentary support

Issued patent: covered by an issued ChainIT patent. Filed application: described in a filed, not-yet-issued application. Potential new matter: not yet filed; a candidate for new filing. Counsel review: filing posture not yet determined. Not applicable: a third-party capability outside ChainIT's patent estate.

Component	Implementation status	IP / documentary support
ChainIT ID / ChainIT Org ID / ARP	Production	Issued patent
Pactvera / Valitorum	Production	Issued patent
Business Rules Engine (compliance predicates)	Production	Issued patent
Evidence Assertion VDT	Development	Filed application
Compliance Policy Profile (CPP)	Development	Filed application
Status epoch / freshness model	Development	Filed application
ChainIT Workflow Engine (compliance disposition)	Development	Potential new matter
Compliance Decision VDT (issuer / signature)	Development	Potential new matter
Compliance Decision Permits interface	Proposed	Potential new matter
Disclosure-tier engine	Development	Potential new matter
Manual-review and override architecture	Proposed	Counsel review
Supplemental Valitorum	Development	Filed application

Component	Implementation status	IP / documentary support
Evidence source integrations (sanctions, PEP, registries, bureaus)	External dependency	Not applicable
Partner rail-adapter enforcement	External dependency	Not applicable

2. The ChainIT Model: Evidence, Policy, Authority, and Decision

Provable Compliance is one layer inside the final ChainIT Authority Protocol. It collects or references modular evidence, applies a versioned compliance policy, evaluates deterministic predicates, and records a purpose-specific disposition. The Authority Protocol then consumes that compliance result together with identity, authority, session or transaction context, risk tier, approvals, capacity, and rail controls. Compliance and authority are adjacent but independent: authority can exist while its present exercise is held, and favorable compliance evidence cannot create authority that the ARP does not grant. [23]

2.1 Subject neutrality and verified identity foundation

The Authority Protocol recognizes four subject classes: a verified individual; a group acting under quorum or separation-of-duties rules; an organization acting through an authorized representative; and a permitted software agent. A scheduled workflow is not a fifth subject class. It is an organization-controlled initiation mechanism acting for an identified organization under the governing ARP. [23]

ChainIT ID is the verified identity anchor for an individual. ChainIT Org ID is the legal-entity identity anchor for an organization. The identity materials support authoritative-source identity verification, biometric authentication and liveness, selective disclosure, lifecycle updates, and portable or offline verification without requiring a new government query every time identity is presented. [17] Identity and authority remain distinct: ChainIT Org ID establishes the entity; the ARP establishes who or what may act for it.

2.2 ARP, Delegated Authority, and Agent Authority

The ARP is the canonical, versioned organizational authority record. It identifies who may act, in what role, for what purpose, within what limits, during what effective period, under what quorum or separation-of-duties requirements, and subject to what amendment or revocation. [18][19][23] A Delegated Authority VDT references the ARP and exposes only the bounded scope needed by a delegate or relying party. Where the delegate is a registered agent, the Agent Authority VDT is the agent-specialized form of that portable authority artifact.

An agent has no authority of its own. Its Agent Authority VDT records the granting principal, governing ARP and version, registered agent, purpose, counterparties, transaction classes, rails, value limits, effective period, step-up thresholds, redelegation rule, and revocation conditions. The grant is append-only; current validity is resolved at the reliance event against the ARP and applicable freshness. A compliance disposition may condition or prevent present exercise, but it does not amend, suspend, delete, or retroactively erase the ARP or the grant record.

2.3 Evidence Assertion VDTs

An Evidence Assertion VDT represents one sourced observation or institution-generated state, not the final compliance conclusion. It identifies the subject, source class, source, source version, retrieval time, effective time, expiration or review time, jurisdiction, match or confidence state, permitted purpose, privacy classification, and integrity reference. Separate VDTs preserve the differences among identity-document

status, sanctions data, PEP information, professional licensing, KYB evidence, AML monitoring state, case status, and transaction-specific counterparty facts.

Source class	Examples	Required treatment
Authoritative-source evidence	Government or statutory registries; issuing-jurisdiction identity data; professional-license records; official sanctions lists.	Record the exact source, participating jurisdiction or program, fields returned, version, time, and limits of what the source proves.
Qualified third-party evidence	PEP data; sanctions and ownership enrichment; criminal-history or background reports; adverse-media services; certifications and specialist providers.	Record provider, permissible purpose, methodology or match state, confidence, dispute path, and contractual or legal restrictions.
Institution-generated evidence	Transaction monitoring; customer and relationship risk; source-of-funds analysis; internal alerts; case-management state; analyst findings.	Identify the responsible institution, model or rule version, analyst or case state, confidentiality class, and permitted disclosure.

2.4 Compliance Policy Profile

The CPP selects the compliance-side rules for a reliance event. It may vary by institution, regulated entity, product, role, subject class, counterparty, transaction type, value, payment rail, payer and payee jurisdictions, customer category, risk tier, and intended purpose. It identifies required evidence, acceptable source classes, maximum evidence age, live-query conditions, predicate logic, review requirements, disposition mapping, disclosure tier, retention, and degraded-mode treatment. The profile is versioned so a later reviewer can determine exactly which rule set produced the result. It is the compliance-side counterpart to the APP; neither profile creates the authority grant recorded by the ARP. [23]

2.5 BRE, Workflow Engine, and Compliance Decision VDT

The BRE returns explicit, deterministic, reason-coded true/false predicate results. It does not itself perform risk scoring or assign the disposition. The organization's configuration of the ChainIT Workflow Engine selects the risk tier where applicable, composes the predicate results, applies quorum or review logic, and creates the disposition. The signed, time-bounded result is the Compliance Decision VDT.

The Compliance Decision VDT identifies the subject and reliance event; CPP and version; Evidence Assertion VDT references; evidence ages or status epochs; BRE predicate results; organization-defined disposition; required controls; reason codes; decision time; expiration or reevaluation time; affected scope; review case where applicable; and permitted disclosure level. It contains signed results and controlled references rather than raw source records that a relying party does not need.

Each Compliance Decision VDT identifies the issuing organization or authorized decision service, the applicable tenant and regulated entity, the signature key or verification method, the relying-party or audience restriction, the decision identifier, the reliance-event identifier, the subject and transaction or session reference, the CPP version, evidence epoch, issue time, expiration, status reference, disclosure tier, and reason codes. This is distinct from the Evidence Assertion VDTs it references, which may themselves be a source-signed assertion, a ChainIT-created attestation recording an authenticated source response, or an institution-generated evidence assertion; a source or registry does not itself sign a ChainIT VDT.

Responsibility and allocation

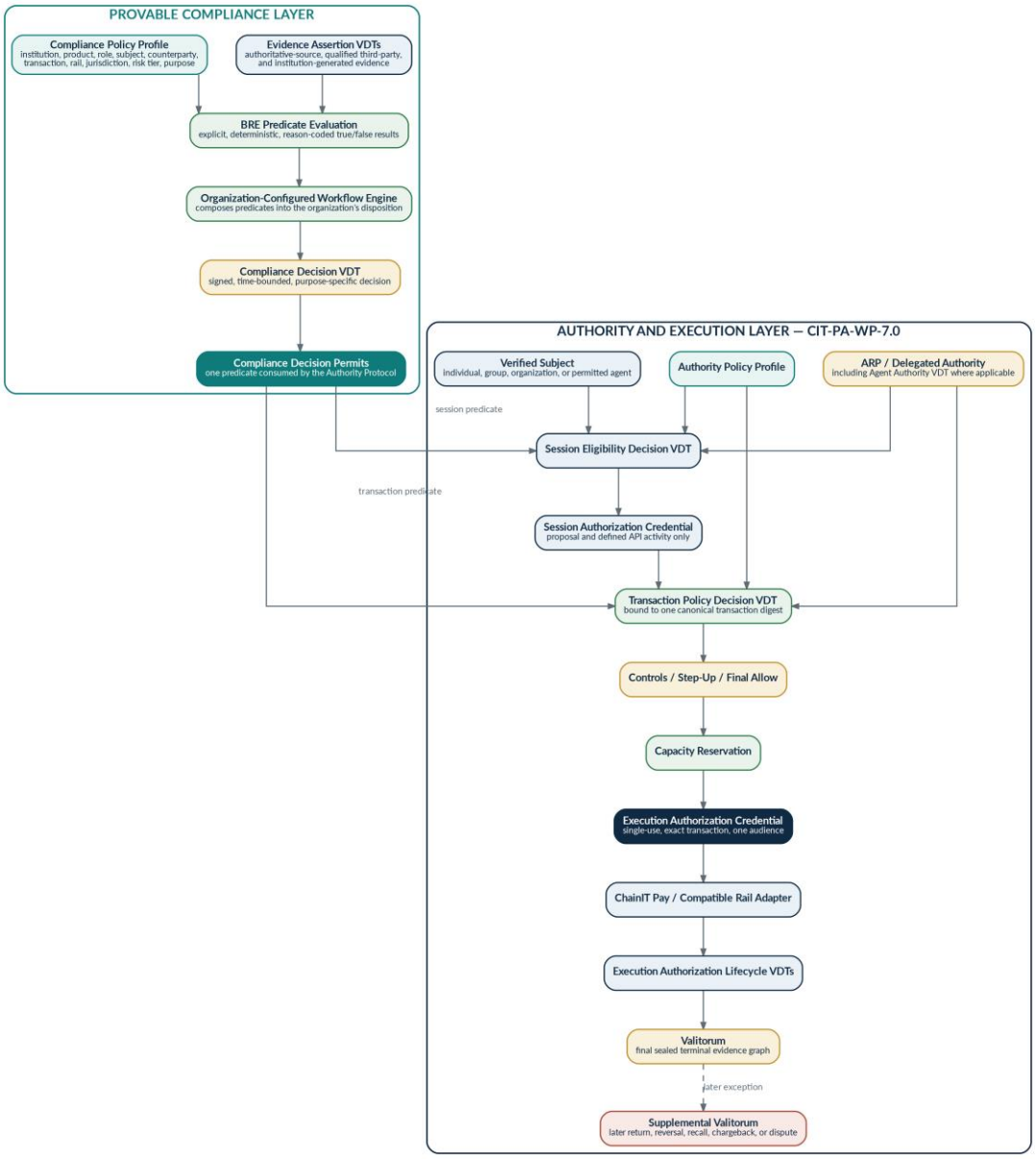
The organization is responsible for the policy logic it configures and for its use of the resulting disposition,

subject to applicable law and contractual allocation among ChainIT, the organization, payment providers, evidence providers, and other participating parties. The white paper does not independently allocate all legal liability.

2.6 Compliance as an input to the final Authority Protocol

The Compliance Decision VDT is not the final session or transaction decision. An Allow disposition means only that the compliance-side predicates permit continuation. A subject may still lack authority, exceed scope, fail authentication, lack required approval or capacity, present a modified transaction digest, or lack a valid EAC. Only the Session Eligibility Decision VDT or Transaction Policy Decision VDT provides the broader Authority Protocol disposition for the applicable reliance event. A Compliance Decision VDT never independently authorizes payment. [23]

Decision artifact	Decision scope	Critical limitation
Compliance Decision VDT	Whether current compliance evidence and the CPP permit, condition, hold, review, reject, or prohibit compliance-side continuation.	Does not establish authority, session eligibility, transaction authority, capacity, or payment authority.
Session Eligibility Decision VDT	Whether the authenticated subject may open or continue a consequential session under current identity, authority, evidence, status, scope, and policy.	Not transaction-specific and cannot authorize value movement.
Transaction Policy Decision VDT	Whether the complete identity, authority, compliance, exact transaction, risk, capacity, approval, and rail conditions support the proposed action.	Only final Allow, after controls and step-up are completed and revalidated, may support reservation and EAC issuance.



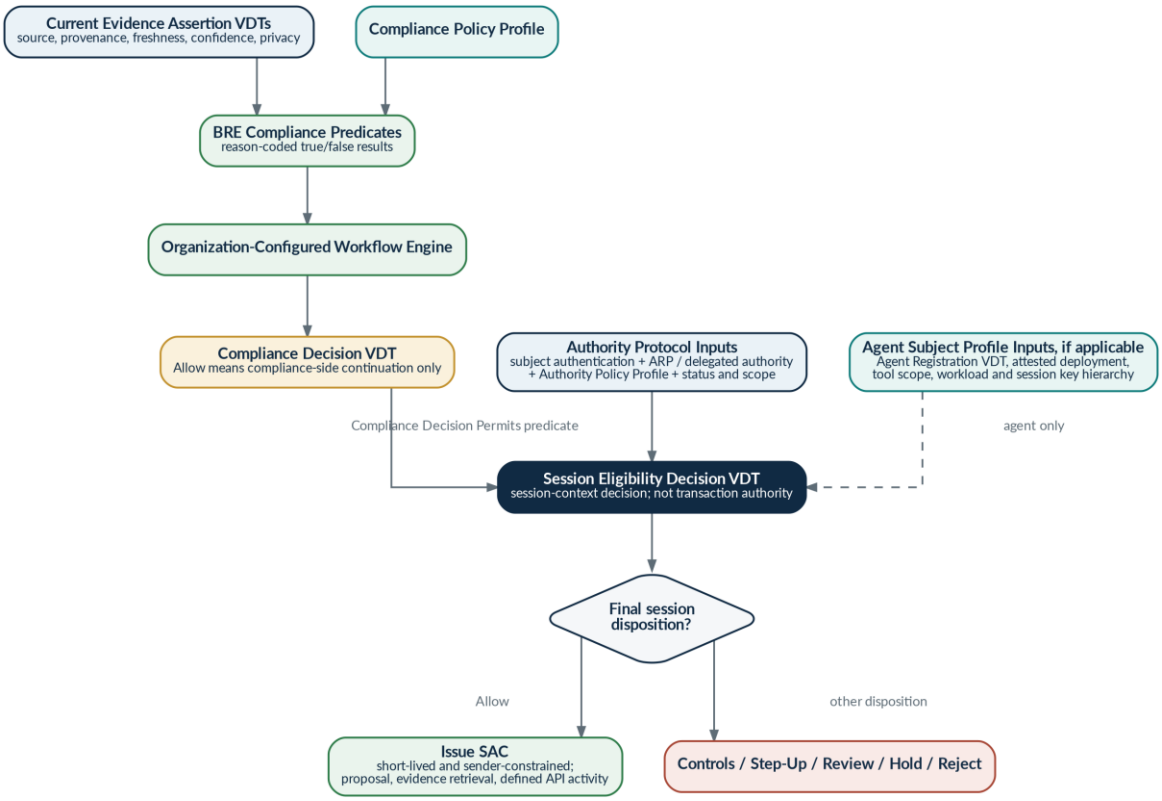
Companion Figure 1. Provable Compliance within the final Authority Protocol.

Compliance supplies a signed predicate; CIT-PA-WP-7.0 controls the session and transaction decision flows.

2.7 Session eligibility flow

For a session that enables consequential activity, the CPP selects current compliance evidence and freshness requirements. The BRE returns reason-coded compliance predicates, and the Workflow Engine creates the Compliance Decision VDT. The Authority Protocol then evaluates Compliance Decision Permits together with subject authentication, the ARP or Delegated Authority VDT, the APP, status, scope, and any subject-specific inputs. Where the subject is an agent, the Session Eligibility Decision VDT additionally references the Agent Registration VDT, Agent Authority VDT, attested deployment, permitted tools, workload key, and ephemeral session-key hierarchy. [23]

Only a final Allow session disposition may support SAC issuance. The SAC is short-lived and sender-constrained. It permits proposal activity, evidence retrieval, and defined API activity. Rail adapters must reject it as payment authority. An Allow with Controls, Step-Up, Review, Hold, Reject, Prohibit, or Stale/Unknown result follows the organization's configured workflow and cannot silently fall through to session issuance.



Companion Figure 2. Compliance input to the Session Eligibility Decision VDT.

A compliance-side Allow permits continuation only; the Authority Protocol still decides session eligibility.

2.8 Transaction policy and commit-time flow

At the transaction reliance event, the Compliance Decision VDT is evaluated with the ARP, Delegated Authority VDT or Agent Authority VDT, APP, verified subject, risk tier, canonical transaction digest, current capacity, required approvals, and rail-specific constraints. The resulting Transaction Policy Decision VDT is bound to one exact digest and one limited evaluation window. It is not reusable as standing status. [23]

General execution predicate

MayExecute = IdentityAssuranceSatisfied AND AuthorityValidUnderARP AND ComplianceDecisionPermits AND TransactionWithinScope AND RequiredApprovalsSatisfied AND BudgetAndRailControlsSatisfied

The payment-boundary predicate is the same test specialized to commit, where the exact instruction, reservation, status, final disposition, and one-time execution credential must also be verified:

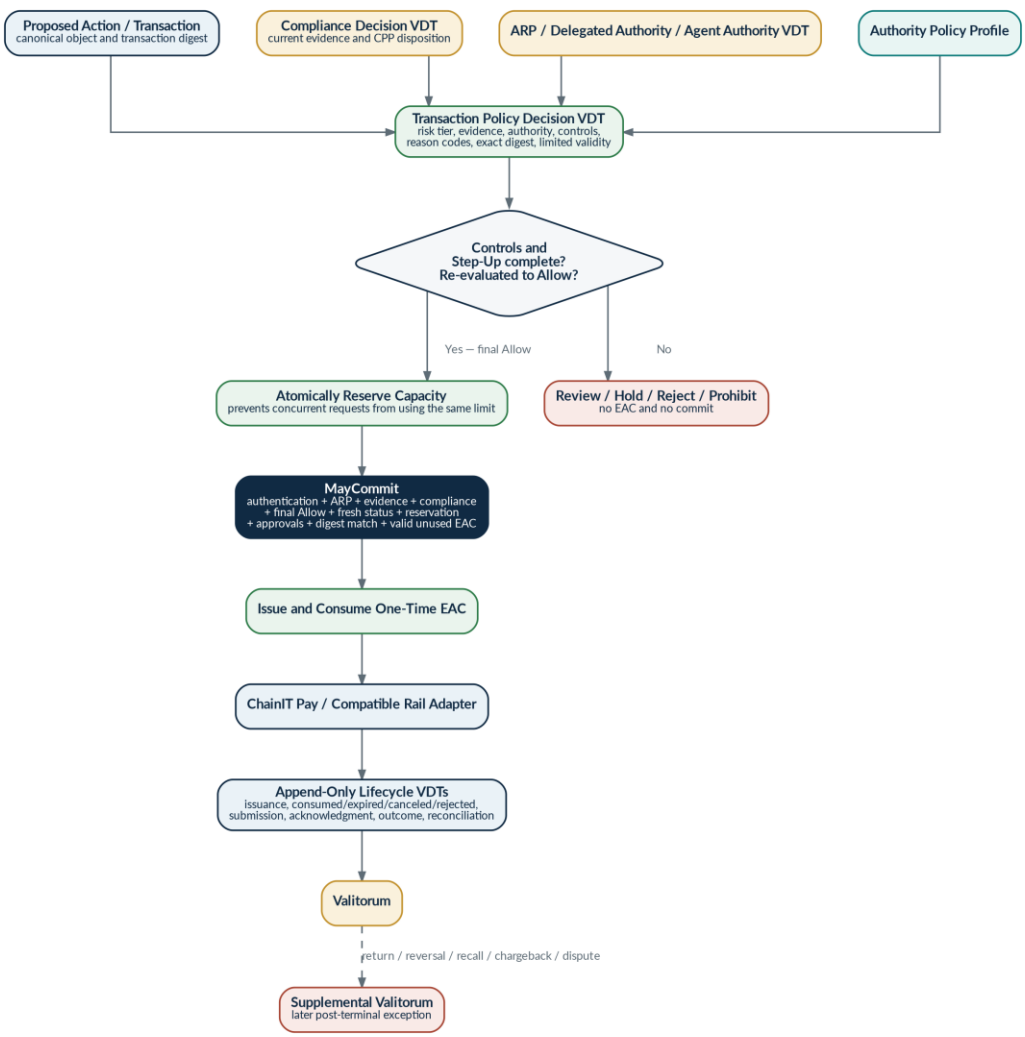
Commit-time execution predicate

MayCommit = SubjectAuthenticated AND AuthorityValidUnderARP AND EvidenceAcceptable AND ComplianceDecisionPermits AND WorkflowDispositionIsAllow AND StatusFresh AND CapacityReserved AND RequiredApprovalsSatisfied AND DigestMatches AND EACValidAndUnused

Every predicate is required. Allow with Controls or Step-Up must be completed and re-evaluated to final Allow before capacity reservation and EAC issuance. The reservation atomically holds capacity so concurrent requests cannot use the same limit twice. The EAC authorizes one exact transaction for one audience and is consumed atomically at the ChainIT Pay or compatible rail-adapter boundary. Failure produces a controlled disposition; there is no silent fallback to the SAC, a stale decision, or a generic bearer credential.

Commit sequence

Gate	Requirement
1. Final decision	The Transaction Policy Decision VDT must resolve to final Allow; a compliance-side Allow alone is insufficient.
2. Controls complete	Any Allow with Controls, Step-Up, Review, or Hold condition must be resolved and the transaction re-evaluated.
3. Capacity reserved	The applicable limit or budget is atomically reserved so concurrent requests cannot commit the same capacity.
4. EAC verified	The one-time EAC must bind the exact digest, audience, reservation, status epoch, subject or session, and expiration, and remain unused.
5. Commit and evidence	The rail boundary consumes the EAC, submits the exact instruction, and creates append-only lifecycle VDTs leading to Valitorum.



Companion Figure 3. Compliance input to the transaction and commit-time flow.

The Compliance Decision VDT contributes one predicate; only final Allow plus reservation and a valid unused EAC can commit value.

2.9 Agent Subject Profile boundary

Only the Agent Registration VDT, the rotatable workload key, the ephemeral session key, and the sovereignty boundary are Agent Subject Profile artifacts. The ARP, Delegated Authority VDT, Agent Authority VDT, Evidence Assertion VDT, Compliance Decision VDT, Session Eligibility Decision VDT, SAC, Transaction Policy Decision VDT, capacity reservation, EAC, Execution Authorization Lifecycle VDTs, Valitorum, and Supplemental Valitorum are protocol-general. Their inputs vary by subject class; their authority and execution meaning does not. [23]

Agent registration, workload attestation, and session-key containment are inputs supplied by the Agent Subject Profile. Provable Compliance may evaluate their current evidence state—for example, whether the registered deployment or key status remains acceptable—but it does not redefine them, and they do not themselves confer authority. An AI model may reason, gather evidence, and propose an action. It does not receive unrestricted payment credentials, custody keys, or final execution authority.

2.10 Pactvera, lifecycle VDTs, Valitorum, and later exceptions

Where a compliance decision governs a Pactvera transaction, the CPP version, Evidence Assertion VDT references, predicate results, Compliance Decision VDT, review or hold case references, disclosure

classification, and material state transitions become part of the same append-only evidence lifecycle used by the Authority Protocol. Pactvera and the Valitorum Service provide the transaction logic and terminal evidence package. [18][19][23]

The operational EAC is short-lived and is not stored as a reusable ledger object. Execution Authorization Lifecycle VDTs record issuance and terminal treatment. Submission, acknowledgment, settlement, rejection, cancellation, return, reversal, recall, chargeback, dispute, and reconciliation are separate linked events; an earlier immutable event is never rewritten. The Valitorum seals the completed or otherwise terminal evidence graph under a defined completeness rule. A later post-terminal exception may be sealed in a Supplemental Valitorum referencing the original.

3. Runtime Re-Verification at the Point of Reliance

The defining commitment of Provable Compliance is point-of-reliance evaluation. ChainIT does not assume that an onboarding result remains valid forever. It also does not impose the technically and economically unrealistic requirement that every source be queried for every event. The system evaluates whether each required item remains fresh enough for the present context and refreshes it when source volatility, transaction risk, policy, or a material event requires a new observation.

3.1 Reliance triggers

1. Session issuance or renewal for an individual, group, organizational representative, or agent where the session enables consequential action.
2. A transaction proposal, payment initiation, smart-contract execution, or other high-impact action.
3. A human step-up approval, particularly for a new payee, changed destination, higher value, irreversible rail, elevated risk, or required quorum.
4. A scheduled review established by source volatility, product risk, jurisdiction, relationship risk, or institutional policy.
5. A source-change notification, sanctions-list update, license change, credential-expiry event, ownership change, AML alert, policy update, ARP or delegated-authority change, key or registration change, or another material-risk event.

3.2 Freshness, not universal live lookup

For each required evidence item, the CPP establishes a maximum acceptable age and any conditions requiring live verification. The BRE evaluates the evidence against the current reliance event:

Freshness rule

$$\text{FreshEnough} = (\text{Current Time} - \text{Evidence Observed Time}) \leq \text{Maximum Age permitted for the source, evidence type, risk tier, product, jurisdiction, and reliance event}$$

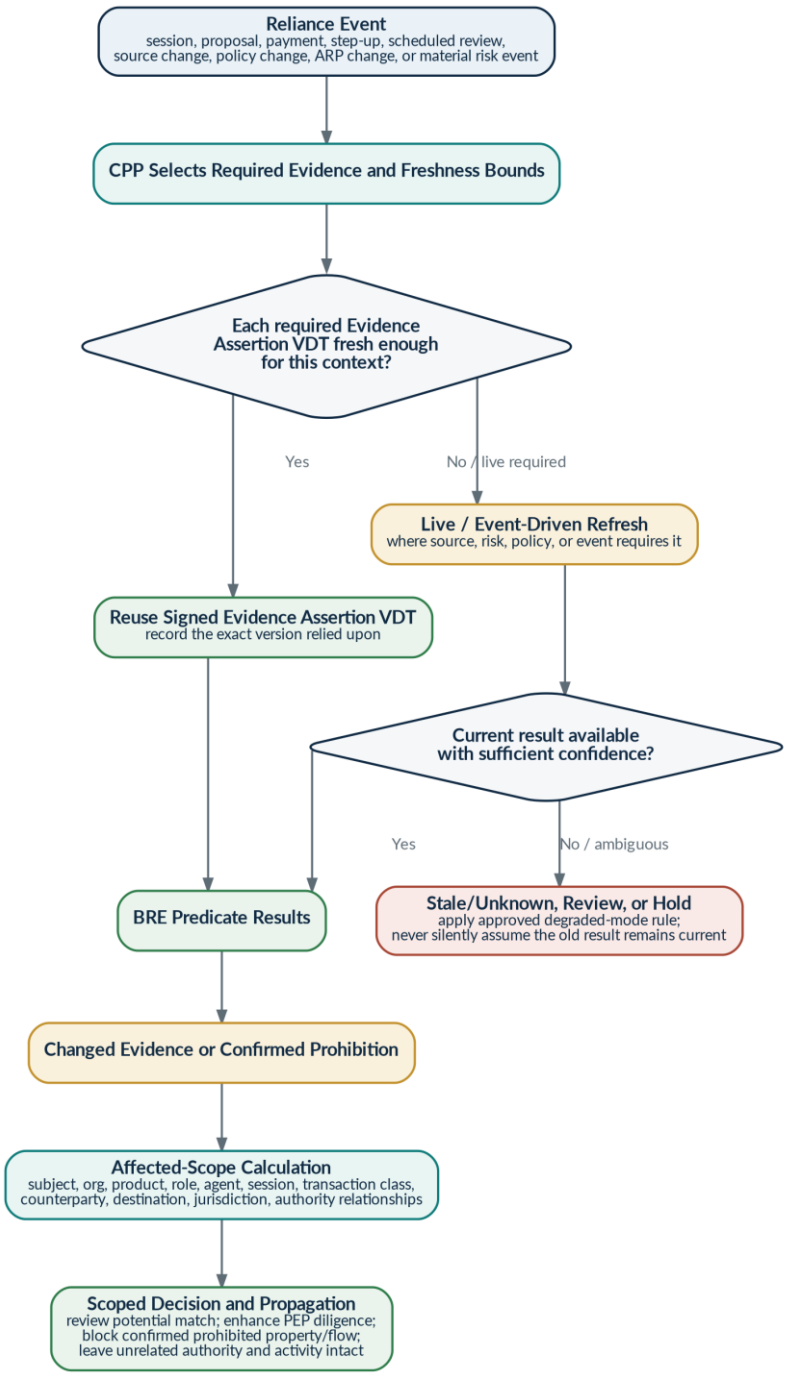
A live source interaction may be required for high-risk or legally sensitive activity. A recently signed Evidence Assertion VDT may be sufficient for a lower-risk action when policy permits. Event-driven invalidation shortens the acceptable interval. If a source is unavailable, the system applies the approved degraded-mode rule—such as stronger verification, Review, Hold, Stale/Unknown, or fail-closed—rather than silently assuming that a prior result remains current. This source-specific model also reflects the risk-based nature of current U.S. CDD guidance. [1]

3.3 Status epoch and verification rigor

The Authority Protocol uses status epochs or status-freshness boundaries to determine whether cached non-revocation and evidence state remain acceptable for a risk tier. Tier 1–Low may permit a signed, recent status snapshot where the APP and CPP allow it. Tier 2–Standard may require a shorter freshness window or targeted live checks. Tier 3–High may require live status introspection or live source verification. The organization's Workflow Engine assigns the risk tier and records the policy version, factors, time, reason codes, and any manual override; the BRE only evaluates the configured predicates. [23]

3.4 Scoped propagation and revocation

A change in evidence propagates to the scope it actually affects. A confirmed sanctions prohibition may require immediate blocking of the affected person, entity, property, wallet, or transaction. A potential name match requires Review or Hold. A PEP designation may trigger enhanced diligence. An expired professional license blocks the licensed activity. A source outage may hold high-risk activity while allowing lower-risk, previously verified activity under an approved policy. The affected-scope calculation identifies the subject, organization, product, role, agent, session, transaction class, counterparty, destination, jurisdiction, and authority relationships that depend on the changed evidence. Broader suspension is used only where law, source state, or configured policy supports it.



Companion Figure 4. Runtime freshness and affected-scope decisioning.

Current evidence is reused only within the applicable freshness bound; changed evidence propagates to the scope it actually affects.

4. Evidence Domains

Evidence Assertion VDTs are not limited to a fixed catalog. Any sourced or institution-generated fact relevant to a compliance decision may be represented under the same architecture. The domains below recur often enough to address in detail, but they are not equivalent Boolean gates and they do not produce one universal compliance badge.

Evidence domain	What it represents	Typical decision effect

Evidence domain	What it represents	Typical decision effect
AML risk and monitoring	Institution-generated customer, relationship, transaction, source-of-funds, alert, case, and monitoring state. There is no universal external "AML-clear" status.	Allow, enhanced monitoring, Step-Up, Review, Hold, Reject, reporting, or another institution-specific disposition.
OFAC and broader sanctions	Official list data plus ownership/control analysis, program restrictions, geography, wallet/address indicators, match confidence, and block-versus-reject rules.	Potential match → Review or Hold. Confirmed applicable prohibition → Prohibit or block, with required reporting and recordkeeping.
PEP and relationship risk	Whether a subject is or is associated with a PEP, together with office, geography, relationship, source-of-wealth/funds, and mitigating evidence.	Enhanced diligence, management approval, monitoring, controls, or risk-based allowance—not automatic universal rejection.
Criminal or background evidence	Purpose-limited reports relevant to a role, license, employment, housing, credit, regulated activity, or another lawful use.	Applied only where lawful and relevant, with required consent, notice, accuracy, dispute, individualized-assessment, and adverse-action processes.
Government identity and assurance	Identity-source match, issuing jurisdiction, credential state where available, ChainIT ID lifecycle, biometric reauthentication, device context, and assurance.	May require identity refresh or stronger authentication. Expiration of one credential does not erase identity or corporate authority.
Jurisdiction, product, licensing, KYC/KYB, and payment transparency	Product- and location-specific obligations, licenses, entity status, customer or beneficial-owner evidence, Travel Rule data, and sector controls.	Selects policy and evidence; limits only the implicated activity, product, role, or geography unless a broader rule applies.

4.1 AML risk and monitoring

AML monitoring is a process performed by the responsible institution, not a government status feed. It evaluates patterns, relationships, expected activity, counterparties, geography, source and destination of funds, products, velocity, structuring indicators, internal alerts, and investigative findings. An Evidence Assertion VDT may represent the institution's current risk and case state, the model or rule version, and the permitted disclosure level. U.S. AML/CFT requirements remain risk-based, and federal agencies continued modernizing that framework through rulemaking in 2026. [1][2]

4.2 OFAC and broader sanctions

Sanctions screening is not limited to checking whether a named person appears on the SDN List. OFAC obligations may extend to entities owned 50 percent or more, directly or indirectly and in the aggregate, by blocked persons; program-specific prohibitions; prohibited trade or investment; digital-currency addresses and other identifiers; and transactions that evade, avoid, cause, or attempt a violation. OFAC states that digital-currency and fiat transactions are subject to the same sanctions obligations. [5][6] The evidence model therefore preserves list version, retrieval time, ownership and control analysis, identifier and wallet results, match confidence, disposition basis, and required reporting or recordkeeping.

4.3 PEP status and enhanced due diligence

PEP status is a risk indicator, not a finding of illegality. U.S. banking agencies state that PEP relationships present varying levels of risk and do not automatically require one unique procedure merely because a customer is considered a PEP. FATF similarly describes PEP controls as preventive rather than criminal. [3][4] The policy response may include source-of-funds or source-of-wealth evidence, senior approval, enhanced monitoring, or other proportionate controls.

4.4 Criminal and background evidence

Criminal-history and broader background information is enabled only where the CPP identifies a lawful, relevant purpose and the required consent, notice, permissible-purpose, accuracy, dispute, nondiscrimination, and adverse-action controls. Where an employer obtains a report from a consumer-reporting company, the FCRA and related employment requirements may apply. [8] Raw records are not placed in a broadly reusable Compliance Decision VDT.

4.5 Government identity and assurance freshness

The identity materials support government-source verification, biometric authentication, selective disclosure, lifecycle updates, and later verification without accessing the government system every time. [17] AAMVA's Driver's License Data Verification service allows approved users to submit driver's-license or identification data and receive match flags against participating issuing-jurisdiction records; it does not establish universal coverage or prove every legal attribute a relying party may require. [7] The decision therefore distinguishes identity, credential state, driving privilege, assurance freshness, and the transaction policy requiring a current credential.

4.6 Jurisdiction-, product-, and industry-specific evidence

Licensing, registration, KYC/KYB, beneficial ownership, age, professional qualification, Travel Rule, gaming, healthcare, employment, environmental, safety, insurance, tax, entity-standing, and other obligations vary materially by activity and jurisdiction. The CPP identifies the applicable regulated entity, product, role, rail, transaction type, and location. Adding a domain does not require a new architecture; it requires an appropriate source class, Evidence Assertion VDT schema, freshness rule, predicate set, workflow configuration, and disclosure policy.

5. Regulatory Landscape and Current Status

Regulatory currency

This section reflects the official sources listed in this edition and is stated as current through August 31, 2026. Rules, effective dates, agency positions, and national implementation continue to change. The section supports architecture and general discussion; it is not product- or jurisdiction-specific legal advice.

5.1 U.S. AML/BSA and customer due diligence

The U.S. CDD framework requires covered financial institutions to understand the nature and purpose of customer relationships, conduct ongoing monitoring to identify and report suspicious transactions, and maintain and update customer information on a risk basis. FinCEN's May 2026 consolidated FAQs emphasize that there is no categorical requirement to update customer information on one continuous or periodic schedule; risk-related information and ordinary monitoring determine when reassessment is required. [1] In February 2026, FinCEN also granted exceptive relief from re-identifying and re-verifying beneficial owners each time a legal-entity customer opens another account, while preserving initial verification, risk-triggered updating, and other ongoing obligations. [1]

5.2 OFAC and sanctions

OFAC expects sanctions controls tailored to the business and its risk. The architecture can preserve screening of relevant individuals, entities, ownership and control, counterparties, wallets or identifiers, geography, and program restrictions; possible-match resolution; block-versus-reject treatment; and the evidence needed for reporting and recordkeeping. Digital-asset transactions do not receive a lower sanctions standard because they use a different rail. [5][6]

5.3 Stablecoin-specific requirements under the GENIUS Act

The GENIUS Act was enacted July 18, 2025 as Public Law 119-27. [10] It establishes a federal and state framework for permitted payment-stablecoin issuers, foreign issuers, custody, reserves, redemption, supervision, and related activities. The Act's effective date is the earlier of eighteen months after enactment or 120 days after the primary federal regulators issue final implementing regulations. The OCC's February 2026 proposal described January 18, 2027 as the expected date absent an earlier trigger. [14]

As of August 31, 2026, implementation remained subject to active rulemaking. FinCEN and the federal banking agencies had proposed customer-identification requirements for permitted payment-stablecoin issuers; FinCEN and OFAC had jointly proposed broader AML/CFT and sanctions-program requirements; and Treasury issued a separate Section 3 proposed rule on August 17, 2026 concerning issuance, offering, and sale of payment stablecoins in the United States. [11][12][13] Provable Compliance can help an issuer, bank, wallet, or service provider evidence screening and policy decisions. It does not itself determine whether ChainIT or another party is an issuer, custodian, money transmitter, digital-asset service provider, or other regulated actor. That perimeter depends on actual issuance, redemption, custody, control, transfer power, conversion, and service functions.

5.4 FATF Travel Rule and cross-border payment transparency

Verified identity records can supply originator and beneficiary data, but storing the data is not the same as satisfying the Travel Rule. Responsible entities must obtain, validate where required, transmit or make available, retain, protect, and screen applicable information under national law and interoperable messaging arrangements. FATF Recommendation 15 and its interpretive materials continue to govern virtual assets and VASPs; FATF's July 2026 update reported increasing implementation together with continuing operational and supervisory gaps. [15] FATF strengthened Recommendation 16 in June 2025 and conducted a public consultation on implementation guidance from June 24 through August 21, 2026, with countries expected to be ready for revised requirements by the end of 2030. [16]

5.5 Identity, background, licensing, and sector rules

Identity, background, licensing, and registration requirements vary by purpose and jurisdiction. AAMVA DLDV is a valuable U.S. source service but depends on approved access and participating jurisdictions. [7] Background reports may implicate FCRA, employment, housing, credit, licensing, consumer-reporting, and local restrictions. [8] Professional licenses and entity registrations require their own official or qualified sources and status semantics. The CPP selects those requirements; no one Evidence Assertion VDT or Compliance Decision VDT is a universal global compliance badge.

6. Risk Tier, Decision States, and Enforcement

Risk tier and disposition are independent. The organization's Workflow Engine assigns Tier 1–Low, Tier 2–Standard, or Tier 3–High based on configured factors and records the policy version, inputs, assignment time, reason codes, and any manual override. The risk tier selects minimum verification rigor. The BRE

returns true/false predicates. The organization's Workflow Engine then combines those predicates into the disposition. A high-risk transaction may resolve to Allow after required controls are satisfied; a low-risk transaction may be rejected because a definitive policy predicate failed. [23]

Disposition	Compliance-side meaning	Typical next action
Allow	All compliance-side predicates are satisfied for the stated scope and time.	Continue to the Session Eligibility or Transaction Policy Decision; do not issue an EAC solely from this result.
Allow with Controls	Continuation is permitted subject to stated restrictions, monitoring, limits, reporting, or safeguards.	Apply controls, record completion, and re-evaluate to final Allow where the Authority Protocol requires it.
Step-Up	A stronger identity event, human approval, second approver, additional source, or enhanced diligence is required.	Pause and initiate the configured step-up workflow.
Review	A potential match, elevated risk, conflicting evidence, or contextual judgment requires an authorized reviewer.	Open or reference a case; preserve confidentiality and reviewer authority.
Hold	Required evidence is unavailable, incomplete, stale, or unresolved.	Do not execute; obtain evidence, restore source access, or apply approved degraded mode.
Reject	The action violates institution policy, risk appetite, or authority conditions but is not necessarily legally prohibited.	Decline with the audience-appropriate response.
Prohibit	A mandatory legal or regulatory prohibition applies.	Block or reject as required, preserve records, and perform required reporting.
Stale/Unknown	The system cannot support a current decision within required freshness and confidence bounds.	Fail controlled; Hold, Review, or deny according to the applicable profile.

The Compliance Decision VDT records the compliance-side disposition. That disposition does not become the final Authority Protocol decision by implication. For sessions, it is consumed by the Session Eligibility Decision VDT. For transactions, it is consumed by the Transaction Policy Decision VDT. Only final Allow after all required controls, approvals, status checks, scope checks, digest checks, capacity reservation, and credential checks can satisfy MayCommit. [23]

7. Design Principles, Evidence and Decision Lifetimes, and Residual Risk

7.1 Zero-Trust Design Principles

- Sourced and attributable. Every evidence item identifies who produced it, which source class applies, what was observed, when it was observed, and what it does and does not prove.
- Contextual rather than universal. The decision is tied to an institution, product, role, subject, counterparty, transaction, rail, jurisdiction, risk tier, and purpose.
- Fresh enough for the present risk. Evidence is not trusted indefinitely, but sources are not queried unnecessarily. Freshness policy is explicit and measurable.
- Authority remains separate. The ARP records organizational power; Delegated Authority and Agent Authority VDTs expose bounded grants; the Compliance Decision VDT gates present exercise without rewriting any grant.
- Compliance is one predicate, not payment authority. A favorable result permits continuation into the final session or transaction decision and cannot issue or replace an EAC.
- Risk tier is not disposition. Verification rigor and decision outcome are separately determined and recorded.
- Uncertainty is a state. Possible matches, source outages, stale evidence, and incomplete data produce Review, Hold, or Stale/Unknown rather than silent allowance or indiscriminate permanent blocking.

- Least disclosure. Subjects and counterparties receive only the minimum outcome; authorized institutional personnel and lawful oversight recipients receive deeper evidence according to role and law.
- Append-only evidence. Refreshes, reviews, approvals, decisions, EAC lifecycle states, outcomes, and later exceptions create new VDTs or Supplemental Valitorums. A sealed record is never edited.
- Human accountability. Overrides, manual findings, approvals, reviews, and release decisions identify the responsible verified person, governing authority, reason, time, and scope.
- Resilience and recovery. Source outages, false positives, key compromise, data corrections, appeals, policy changes, rail ambiguity, and later returns have defined controlled paths.
- Agent containment. Agent registration and keys identify and contain the workload, but authority still comes from the ARP and the agent cannot cross the sovereignty boundary to unrestricted payment credentials or final execution authority.

7.2 Evidence and Decision Lifetimes

Provable Compliance artifacts inherit the platform foundation and Authority Protocol control boundaries described in CIT-PA-WP-7.0. The compliance-specific artifacts below are versioned or reliance-event-specific; none is a permanent status, and a later reviewer can determine exactly which evidence, policy, and decision were current at the time of reliance.

Evidence and Policy Artifacts

Artifact	Layer	Typical lifetime or state	Control boundary
Evidence Assertion VDT	Compliance layer	Source-specific effective and expiration periods; refreshed or re-derived at the reliance event rather than trusted indefinitely.	Evidence service; selective disclosure.
Compliance Policy Profile (CPP)	Compliance layer	Versioned; effective until amended, superseded, or retired.	Institution's compliance policy configuration.
Compliance Decision VDT	Compliance layer	Signed, time-bounded, reliance-event-specific; superseded by a new decision rather than altered.	Organization's configuration of the ChainIT Workflow Engine.
Compliance Decision Permits (predicate)	Compliance layer	Evaluated fresh at each reliance event; not cached or reused as a standing status.	Authority Protocol / BRE.

Decision, Transaction, and Evidence-Graph Artifacts

Artifact	Layer	Typical lifetime or state	Control boundary
Session Eligibility Decision VDT (compliance input)	Authority Protocol	One session context; expires and is re-derived, consuming the current Compliance Decision Permits result.	Authority gateway / BRE.
Transaction Policy Decision VDT (compliance input)	Authority Protocol	One exact transaction and limited evaluation window; not reusable as standing status.	BRE / transaction control plane.
Execution Authorization Lifecycle VDT	Authority Protocol	Permanent immutable evidence events for issuance and terminal handling.	ChainIT evidence ledger.
Valitorum	Platform foundation	Permanent immutable seal over the configured terminal evidence graph, including compliance references.	Valitorum verification package.
Supplemental Valitorum	Authority Protocol	Permanent seal over a later exception graph (return, reversal, recall, chargeback, dispute, or later compliance finding) referencing the original Valitorum.	Post-terminal exception verification package.

7.3 Residual Risk and Non-Goals

Provable Compliance is designed to make evidence, policy selection, predicate evaluation, disposition, and reliance-event context attributable and independently verifiable. It does not eliminate:

- Incorrect, delayed, or incomplete data from a sanctions list, PEP database, credit bureau, government registry, or other third-party evidence source.
- A false negative or false positive produced by a screening, matching, or scoring algorithm operating outside ChainIT's control.
- An institution configuring its own Compliance Policy Profile or disposition set in a way that does not satisfy its actual regulatory obligations.
- Coercion, collusion, or malicious conduct by people who satisfy the formal evidence and policy rules.
- Compromise of ChainIT issuer infrastructure, an evidence provider, or a source system outside ChainIT's control.
- Residual exposure accepted by a verifier that relies on a signed evidence snapshot up to the approved maximum staleness.
- A regulatory change, guidance update, or enforcement action that has not yet been reflected in the applicable CPP.

Claims discipline

Provable Compliance is designed to reduce stale, mismatched, undocumented, and non-attributable compliance decisions. It is not a guarantee of regulatory compliance, a substitute for an institution's AML/CFT or sanctions program, or a certification that a subject is free of risk, and it is not described as such. The residual risks above are stated so that a deploying institution can control for them.

8. Illustrative Scenarios

8.1 Human-initiated wire under the same ARP

Jane, Acme Corp's finance director, authenticates through ChainIT ID and proposes a $60,000 wire under an ARP authorizing treasury activity up to $100,000 per transaction, subject to a second authorized approver above $25,000, within specified counterparties, destinations, and approval rules. The CPP selects sanctions, customer, counterparty, jurisdiction, and other required evidence. The BRE returns deterministic compliance predicates, and the Workflow Engine creates a Compliance Decision VDT. That result becomes the Compliance Decision Permits input to the Transaction Policy Decision VDT. The transaction still must satisfy the ARP, APP, canonical digest, required approvals, capacity, status, and rail conditions before final Allow, reservation, and EAC issuance. A compliance-side Allow alone cannot release the wire.

8.2 Agent-initiated payment within delegated scope

Acme Corp's procurement agent is registered under the Agent Subject Profile. Jane, acting under the ARP, grants a bounded Agent Authority VDT permitting approved cloud-service payments up to $5,000 per transaction and $25,000 per month. The agent authenticates its registered deployment and receives a SAC after the Session Eligibility Decision VDT resolves to final Allow. The SAC permits invoice review and proposal activity but is rejected as payment authority. For a $3,800 payment, the compliance layer returns an Allow, the Transaction Policy Decision VDT confirms the exact digest and scope, capacity is reserved, and a one-time EAC is consumed by ChainIT Pay. The lifecycle events and final outcome are sealed in the Valitorum.

8.3 Quorum and separation-of-duties transaction

An organization-controlled ACH file requires two approvers under the ARP. Each approver is a subject of authority, and each may have a separate Compliance Decision VDT based on identity assurance, role-relevant evidence, and current policy. The group does not become a new identity merely because a quorum is required. The Transaction Policy Decision VDT records the quorum rule and exact digest. Capacity is not committed and no EAC is issued until both approvals refer to the same digest and all compliance and authority predicates are final Allow.

8.4 Confirmed sanctions prohibition affecting a vendor

A vendor becomes subject to an applicable sanctions prohibition. At the next reliance event—or earlier through a source-change feed—the sanctions Evidence Assertion VDT is refreshed. The BRE evaluates the relevant predicates, and Acme's Workflow Engine issues Prohibit for the affected counterparty and flows. Jane's procurement authority, the agent's grant, and unrelated vendors remain intact unless the applicable rule requires broader blocking. The system records the source version, ownership or identifier analysis, decision, affected scope, and reporting treatment without exposing investigation detail to the vendor.

8.5 Newly identified PEP requiring enhanced diligence

Jane is appointed to a public position and is treated as a PEP under the applicable CPP. Her corporate role and ARP do not disappear. The changed Evidence Assertion VDT causes Review or Allow with Controls. Acme may require source-of-funds or source-of-wealth information, senior approval, enhanced monitoring, or a lower autonomous threshold on grants she made. If the controls are completed, a new Compliance Decision VDT may permit continuation and the Authority Protocol re-evaluates the session or transaction. The record preserves the difference between a risk factor and a prohibition.

8.6 Identity credential no longer meeting the assurance profile

Jane's driver's license expires. ChainIT continues to know which verified person the ChainIT ID represents, but the government-credential evidence no longer satisfies Acme's required assurance for a high-value biometric step-up. The compliance result is Step-Up, Hold, or Stale/Unknown according to the CPP; it is not a finding that Jane ceased to exist or lost every corporate role. Jane refreshes ChainIT ID using an accepted current credential or approved alternative process. A new evidence VDT and Compliance Decision VDT are created, and the same ARP and transaction digest are re-evaluated.

8.7 Later return or dispute after terminal settlement

A payment settles and the configured completeness rule is satisfied, so the Valitorum is sealed. A later ACH return, stablecoin reversal mechanism, recall, chargeback, or dispute does not alter the original Valitorum. The rail outcome and any new compliance or review decision are recorded as new linked lifecycle VDTs and may be sealed in a Supplemental Valitorum referencing the original. This preserves both the original terminal record and the later exception history.

9. Privacy, Disclosure, and Evidentiary Controls

A system capable of explaining why a compliance decision changed must also prevent unnecessary or prohibited disclosure. The Compliance Decision VDT separates verifiable outcome data from restricted evidence, case notes, raw source records, and legally protected information. The disclosure tier is selected by policy and audience, and every access or export should itself be attributable and auditable.

Independent verification establishes the issuer, integrity, policy version, evidence references, timestamps, status, and lifecycle of the decision artifact. It does not necessarily permit a third party to re-query a restricted source or independently establish every underlying source fact. For public records or source-signed evidence, a relying party may be able to reproduce or independently validate the underlying fact directly. For restricted government data, commercial screening services, SAR-related information, or institution-generated monitoring, verification is limited to the decision artifact itself rather than the source record it references.



Companion Figure 5. Controlled disclosure of compliance outcomes.

The signed decision remains verifiable while raw evidence, investigation detail, sensitive PII, and SAR-protected information remain behind authorized controls.

Audience	Appropriate disclosure
Subject or counterparty	Minimum disposition: proceed, additional information required, pending review, or unable to proceed. Do not disclose SAR information, confidential investigative logic, or raw restricted records.
Authorized institutional personnel	Source, match, confidence, freshness, case, analyst, review, override, and decision detail according to role, need to know, and applicable restrictions.
Regulator, examiner, auditor, or law enforcement	Authorized evidence package consistent with lawful process, supervisory authority, confidentiality, retention, and privilege requirements.
Payment or technology partner	Only the decision, transaction binding, control completion, status, and proof needed to enforce the relevant session or transaction boundary.

Raw biometric templates, government-identification images, criminal-history records, SARs and SAR indicators, full sanctions-investigation notes, source-of-funds records, beneficial-ownership documents, and similar sensitive material are not placed in broadly portable VDTs. The Compliance Decision VDT contains signed results, evidence references, integrity proofs, reason-code references, and disclosure classification. Underlying evidence remains in restricted stores with access control, retention, correction, redress, and legal-process handling. FinCEN's SAR confidentiality requirements are an explicit design constraint. [9]

10. Business Value and Measurable Outcomes

- Closes the evidence-age gap by evaluating source-specific freshness and context at the moment of reliance rather than treating onboarding as permanent truth.
- Produces a session- or transaction-specific, signed, versioned compliance decision instead of a vague assertion that "compliance was checked."
- Keeps authority, compliance, risk tier, session eligibility, transaction policy, capacity, and payment credentials separate so one favorable result cannot silently substitute for another.
- Creates a common control boundary across individual-, group-, organization-, and agent-initiated actions, including organization-controlled scheduled-workflow initiations.
- Preserves the sovereignty boundary: agents may propose and coordinate, while the deterministic control plane retains final execution authority.

- Reduces reconstruction work by linking identity, ARP, delegated authority, evidence, policy, review, approval, reservation, EAC lifecycle, rail outcome, and Valitorum artifacts.
- Supports selective disclosure by giving each audience only the outcome and evidence detail it is authorized to receive.
- Standardizes evidence collection, freshness evaluation, predicate execution, decision recording, and audit production as transaction and agent volume increase.

Outcome	Measure
Decision completeness	Percentage of decisions containing required subject, CPP, evidence, freshness, predicate, disposition, reason, scope, expiration, and disclosure fields.
Authority-flow consistency	Percentage of compliance decisions correctly referenced by the corresponding Session Eligibility or Transaction Policy Decision VDT.
Freshness compliance	Percentage of reliance events decided within applicable evidence-age or status-epoch bounds; count and cause of Stale/Unknown states.
Decision latency	P50, P95, and P99 latency for cached evidence, refreshed evidence, and human-review paths.
False positives and false negatives	Valid actions incorrectly held or rejected; actions that should have been escalated or prohibited but were allowed.
Status propagation	Time from authoritative or institutional state change to enforcement by online and cached verifiers.
Manual workload	Reviews, overrides, support interventions, and staff time by transaction cohort compared with baseline.
Commit control integrity	Percentage of committed transactions with final Allow, fresh status, capacity reservation, required approvals, matching digest, and valid unused EAC.
Audit retrieval	Time to produce a complete independently verifiable identity, authority, evidence, policy, decision, execution, and outcome package.
Privacy and disclosure	Percentage of responses meeting minimum-disclosure policy; unauthorized, excessive, or prohibited disclosure events.
Exception continuity	Percentage of later returns, reversals, recalls, chargebacks, and disputes recorded without alteration of the original Valitorum.

Claims discipline

Provable Compliance is designed to reduce stale, unsupported, out-of-scope, insufficiently evidenced, and incorrectly disclosed decisions. It is not represented as fixed-cost, universally real-time, fraud-proof, or automatically compliant with every law. Performance, accuracy, propagation, and cost claims should be based on measured deployment data.

11. Implementation Priorities and Controlled Deployment

The shared Authority Protocol definitions and flows are controlled by CIT-PA-WP-7.0. The compliance implementation should therefore be developed as a companion layer rather than as a parallel authority system. The immediate work should preserve that division and validate the evidence, policy, decision, disclosure, and lifecycle interfaces described here.

Priority	Required outcome
1. Canonical schemas	Freeze Evidence Assertion VDT, CPP, BRE predicate, Compliance Decision VDT, review-case, disclosure-tier, and status/freshness schemas.
2. Authority interface	Define the exact Compliance Decision Permits interface to Session Eligibility Decision VDT and Transaction Policy Decision VDT; prohibit direct EAC issuance from a compliance result.
3. Subject model	Implement individual, group/quorum, and organizational representative inputs, including organization-controlled scheduled-workflow initiations, together with Agent Subject Profile inputs, without creating conflicting authority semantics.
4. Evidence-provider inventory	Document source class, fields, permitted purpose, coverage, confidence, latency, cost, refresh model, dispute path, outage behavior, and retention for each provider.
5. Policy and workflow governance	Version CPPs; separate predicate evaluation, risk-tier assignment, disposition mapping, manual review, override authority, and policy approval.
6. Freshness and status	Define source-specific maximum ages, event-driven invalidation, status epochs, live-verification triggers, degraded-mode behavior, and propagation measurements.
7. Privacy and disclosure	Implement audience-specific responses, restricted evidence stores, SAR confidentiality, selective disclosure, correction/redress, and access audit.
8. Lifecycle integration	Link compliance decisions to the exact session or transaction artifacts, Execution Authorization Lifecycle VDTs, Valitorum, and Supplemental Valitorum.
9. Conformance and adversarial testing	Test stale evidence, source outages, false matches, changed digests, concurrent requests, incomplete controls, improper EAC issuance, unauthorized disclosure, and later exceptions.
10. Patent and publication review	Reconcile the final implementation against filed support and complete any required priority or new-matter work before external technical disclosure.

11.1 Open implementation questions

- Which evidence providers and authoritative-source interfaces are contracted, available by jurisdiction, and permitted for each purpose?
- Which policy-profile templates will ChainIT provide, and which logic remains solely institution-configured?
- How will risk-tier assignment, manual override, and policy approval be governed and independently tested?
- What status-epoch, live-query, and evidence-refresh service levels can be supported for each source and partner?
- How will false positives, disputes, corrections, consumer notices, and adverse actions be routed and evidenced?
- What data may be disclosed to subjects, counterparties, payment partners, auditors, regulators, and law enforcement?
- Which session and transaction artifacts are currently implemented, in pilot, or proposed, and how will that status be represented externally?
- How will rail-specific execution and later exceptions be linked to the compliance record without altering the original Valitorum?

12. Conclusion

The most important compliance question is not whether a check occurred once. It is whether the evidence and rule set required for the present reliance event are current enough, applicable, and sufficiently certain for the organization's configured policy. That question cannot be answered by a universal badge because

sanctions, PEP status, AML risk, background information, identity assurance, licensing, KYC/KYB, and payment-transparency obligations have different sources, volatility, legal effects, and disclosure constraints.

ChainIT Provable Compliance turns those differences into a verifiable compliance layer. ChainIT ID and ChainIT Org ID establish the subjects. Evidence Assertion VDTs preserve sourced and institution-generated facts with provenance and freshness. A versioned CPP selects the rules. The BRE returns deterministic, reason-coded predicates. The organization's Workflow Engine assigns risk tier where applicable and composes the predicates into a signed, time-bounded Compliance Decision VDT. That decision gates present exercise without rewriting the ARP or creating authority.

The final Authority Protocol remains controlling. The Compliance Decision VDT supplies the Compliance Decision Permits predicate to the Session Eligibility Decision VDT or Transaction Policy Decision VDT. A SAC enables proposal activity but is never payment authority. A transaction can commit only after final Allow, fresh status, exact-digest matching, required approvals, atomic capacity reservation, and a valid unused EAC. Execution Authorization Lifecycle VDTs preserve credential treatment, the Valitorum seals the terminal evidence graph, and Supplemental Valitorums preserve later exceptions without modifying history. [23]

The resulting control is neither "trust the onboarding file" nor "query every database for every action." It is a disciplined point-of-reliance decision: rely on signed evidence while it remains fresh enough; refresh when source, risk, or policy requires; preserve uncertainty as Review, Hold, or Stale/Unknown; apply prohibitions only to the scope they actually govern; disclose only what the audience may receive; and supply the final Authority Protocol with a verifiable compliance predicate before consequence. That is the zero-trust compliance foundation for scalable human, organizational, and agentic commerce.

References and Source Basis

Regulatory references are stated as current through August 31, 2026 based on the official sources listed in this edition. Each source should be revalidated immediately before publication and before deployment-specific reliance. ChainIT patent and application materials support the identity, authority, VDT, BRE, Pactvera, conditional-execution, and Valitorum foundations described here; CIT-PA-WP-7.0 controls the shared Authority Protocol definitions and flows. [17]–[23]

[1] FinCEN, CDD Rule FAQs, consolidated and updated May 6, 2026; and February 13, 2026 CDD exceptive relief. https://www.fincen.gov/resources/statutes-and-regulations/cdd-rule-faqs

[2] FinCEN, Anti-Money Laundering and Countering the Financing of Terrorism Programs, Notice of Proposed Rulemaking, April 7, 2026. https://www.fincen.gov/resources/statutes-regulations/federal-register-notices/anti-money-laundering

[3] FinCEN and federal banking agencies, Statement on BSA Due Diligence Requirements for Customers Who May Be Considered Politically Exposed Persons, August 21, 2020.

[4] FATF, Guidance: Politically Exposed Persons (Recommendations 12 and 22). https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Peps-r12-r22.html

[5] OFAC FAQ 560, digital currency and fiat sanctions obligations, including the 50 Percent Rule. https://ofac.treasury.gov/faqs/560

[6] OFAC, Sanctions Compliance Guidance for the Virtual Currency Industry, October 15, 2021. https://ofac.treasury.gov/recent-actions/20211015

[7] AAMVA, Driver's License Data Verification Service, accessed August 2026. https://www.aamva.org/technology/systems/verification-systems/dldv

[8] Federal Trade Commission and EEOC, Background Checks: What Employers Need to Know. https://www.ftc.gov/business-guidance/resources/background-checks-what-employers-need-know

[9] FinCEN, SAR disclosure prohibition and confidentiality materials, https://www.fincen.gov/disclosure-prohibited; statutory basis at 31 U.S.C. § 5318(g)(2); see also FinCEN Advisories FIN-2010-A014 and FIN-2012-A002.

[10] Guiding and Establishing National Innovation for U.S. Stablecoins Act, Pub. L. No. 119-27, July 18, 2025. https://www.govinfo.gov/app/details/PLAW-119publ27

[11] U.S. Department of the Treasury, Treasury Seeks Public Comment on GENIUS Act Proposed Rulemaking, August 17, 2026. https://home.treasury.gov/news/press-releases/sb0605/

[12] FinCEN and agencies, Proposed Rule to Implement GENIUS Act Customer Identification Program Requirement, June 18, 2026.

[13] U.S. Department of the Treasury, Proposed Rule to Implement GENIUS Act Illicit-Finance Requirements, April 8, 2026. https://home.treasury.gov/news/press-releases/sb0435

[14] OCC Bulletin 2026-3, GENIUS Act Regulations: Notice of Proposed Rulemaking, February 25, 2026. https://www.occ.treas.gov/news-issuances/bulletins/2026/bulletin-2026-3.html

[15] FATF, Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, July 16, 2026.

[16] FATF, Public Consultation on Guidance to Increase Payment Transparency, June 24, 2026.

[17] ChainIT, Portable Self-Sovereign Digital Identity with Immutable Trust & Privacy-Preserving Verification, application materials.

[18] ChainIT, Pactvera Application B, System and Method for Verifiable Tokenized Transaction Execution and Conditional Compensation, application materials.

[19] ChainIT, System and Method for Managing Verified Digital Identities, Tokenized Assets, and Conditional Transactions in a Blockchain-Based Marketplace, filed application materials.

[20] U.S. Patent No. 11,288,761 B2, Decentralized System for Verifying Participants to an Activity.

[21] U.S. Patent No. 11,216,772 B2, Use of Blockchain-Based Distributed Ledger and Smart Contracts for a Construction Project.

[22] U.S. Patent No. 12,321,940 B2, System for Verification and Management for Digitally Cash Transactions.

[23] ChainIT, Provable Authority: A Protocol for Verifiable Authority Resolution and Control Across Human, Organizational, and Agentic Transactions, CIT-PA-WP-7.0, August 2026.