SWISSI AI JOURNAL

Credentials and Triangulated Trust Signals on a Single Accountable Identifier

A Hash-Anchored Distributed-Ledger Framework for Portable Identity across Jurisdictions

Walter Kurz[1]

[1]Swissi Institute for AI, kurz@swissi-ai.institute

ISSN 3043–1921 | Volume 2026 | https://journal.swissi-ai.institute | journal@swissi-ai.institute | CC BY 4.0
Article SAIJ-zpd6gvtrfaun | DOI: 10.5281/zenodo.21901243 | https://journal.swissi-ai.institute/doi/zpd6gvtrfaun
Submitted 05/26; Revised 06/26; Published 07/26

Abstract

Digital identity remains structurally rigid when it is bound to provider accounts, mutable handles, single social contexts, and local wallet schemes. This paper defines an accountable hash-anchor tier above wallets and credential schemes. Building on a companion model of legal identity assurance, the tier binds an inert root anchor to an event-backed Entity Actor Identity (EAID) assurance state, supports unlinkable profile anchors for distinct contexts, and lets relying parties evaluate gate-specific assurance-at-time over disclosed independent confirmation-event clusters. The formal model states the identifier and capability separation invariant, defines root and profile anchors, models disclosure and lawful resolution as constraints, and gives a two-layer erasure construction for retained commitments and off-chain personal linkage. It also models trust as a reliance event in which pseudonymous interaction becomes rational when a presentation satisfies the requested gate and recourse can reach the legally relevant imputation point. The result is a scheme-agnostic aggregation layer that complements national wallets, supports natural, juridical, and machine actor constellations, and states conditions under which pseudonymity, lawful access, data erasure, and retention can be jointly satisfied.

Keywords: digital identity; verifiable credentials; accountable pseudonymity; distributed ledger; selective disclosure; identity assurance; self-sovereign identity; hash anchor

1 Introduction

Digital identity becomes rigid when it is bound to a provider account, a mutable contact handle, a single social context, and one legal scheme. Natural persons move between family, professional, civic, and pseudonymous contexts, and they may also hold several jurisdictional identities. Platform accounts collapse these audiences into one presentation surface, a dynamic studied as context collapse and as audience management in social interaction.Goffman, 1959; Marwick and boyd danah, 2011 The privacy problem is contextual as well: a datum may be appropriate in one relationship and inappropriate in another, even when it is true and lawfully held.Nissenbaum, 2010

Four rigidities follow from that account-level design. Anchor rigidity appears when identity is welded to a phone number, email address, platform account, or wallet instance instead of a portable root. Context rigidity appears when one identifier must serve family, work, public, and pseudonymous interaction at once. Portability rigidity appears when an identity check performed by one institution cannot be reused by another without repeated collection. Jurisdiction rigidity appears when one scheme carries one legal frame while the actor's life and transactions cross borders. The common cause is architectural: flexible use requires an identity object above wallets, providers, and local schemes.

Regulatory pressure points converge on the same architectural need. Data-protection law grants erasure and minimisation rights, while anti-money-laundering law requires customer due diligence and retention of identity records.European

Union, 2016, 2024b Electronic-identity law supports selective disclosure and pseudonym use, while regulated activity still requires lawful identifiability and recourse.European Union, 2024a These duties can be stated in separate legal instruments, but a system that mediates legally relevant digital acts must implement them together. The missing architecture is an accountable middle layer: ordinary interaction remains pseudonymous and minimal, while defined conditions preserve resolution, audit, and responsibility.

The companion paper supplies the legal identity-assurance substrate for that layer.Kurz, 2026b It defines natural, juridical, and machine entities; distinguishes entities from actors; represents assurance through Entity Actor Identity (EAID) coordinates over assertion rows and source classes; records confirmation and reliance as events; and states capability gates as predicates over that assurance state. It also fixes the machine-actor caveat used here: a machine may act technically, but legal responsibility is imputed through a natural or juridical actor under present law. This paper starts above that substrate and defines the hash-anchor tier that binds, separates, presents, and aggregates the legal assurance state.

From a systems-theory perspective, the hash anchor is an observation point for operations rather than a digital person. The system registers credential issuance, confirmation, presentation, consent, resolution, revocation, reliance, and dispute as events around an inert anchor, while legal identity remains reachable only through governed linkage.Luhmann, 1995 The design question is cybernetic: how much independent, fresh, and legally reachable evidence gives a relying party enough variety to let a pseudonymous counterparty act with credible recourse.Ashby, 1956

This paper contributes five linked elements. First, it defines an above-wallet hash-anchor tier that binds to Paper 14's event-backed assurance state and bridges credential schemes inside and outside the European Union. Second, it defines root and profile anchors so that context separation and accountable pseudonymity can coexist. Third, it defines gate-specific triangulated assurance-at-time over independent confirmation-event clusters, with freshness, revocation, source independence, binding strength, and jurisdiction evaluated at reliance time. Fourth, it models disclosure, lawful resolution, governed erasure, and retention as constraints that can be jointly satisfied under stated assumptions. Fifth, it models assurance-mediated trust as a reliance event in which verifiable gate satisfaction and credible recourse let pseudonymous parties transact.

2 Related Work

Identifier and credential standards supply the technical substrate for holder-presented identity. Decentralized identifiers define identifiers whose associated control material can be resolved without relying on a single account provider.World Wide Web Consortium, 2022 Verifiable credentials define an issuer-holder-verifier pattern in which holders receive credentials and present derived proofs to verifiers.World Wide Web Consortium, 2025 Selective-disclosure JSON Web Tokens, OpenID for Verifiable Presentations, and mobile credential profiles such as ISO/IEC 18013-5 specify presentation and disclosure mechanisms.Fett et al., 2025; International Organization for Standardization, 2021; Terbu et al., 2025 Self-sovereign-identity research frames these mechanisms around holder control, selective disclosure, and data minimisation.Schardong and Custódio, 2022 This standards layer explains how claims are represented and presented. Paper 15 addresses the layer where many claims bind when a relying party needs profile separation, cross-scheme aggregation, and recourse.

Privacy-preserving credential systems and pairwise identifiers are the closest technical prior art for profile anchors. Anonymous-credential systems based on Camenisch-Lysyanskaya signatures, U-Prove, Hyperledger AnonCreds, and BBS-based verifiable credential cryptosuites support selective disclosure, zero-knowledge presentations, and unlinkable derived proofs.Camenisch and Lysyanskaya, 2001; Hyperledger AnonCreds Project, 2026; Paquin and Zaverucha, 2013; World Wide Web Consortium, 2026 DID Core and the Peer DID method describe pairwise identifiers for relationship-specific pseudonymity and warn that reused verification material and endpoints can recreate correlation.Decentralized Identity Foundation, 2026; World Wide Web Consortium, 2022 These mechanisms are primitives for Paper 15. The contribution is the layer that connects profile-scoped presentation to Paper 14's legal assurance state, gate semantics, reliance records, and governed recourse.

Assurance frameworks and national wallet schemes define strong scheme-level comparators. NIST SP 800-63 separates identity proofing, authentication, and federation as assurance categories.Grassi et al., 2024 The European Digital Identity Framework and the EUDI Architecture and Reference Framework specify wallet-based identity and attribute presentation in the European Union.European Commission, 2025; European Union, 2024a Switzerland's state electronic identity supplies a comparable sovereign-wallet reference outside the European Union.Swiss Confederation, 2024 These frameworks are essential credential sources for the architecture proposed here. Their operating unit is the scheme,

wallet, credential, or federation assertion. Paper 14 supplies legal assurance grammar around events and gates; Paper 15 supplies the hash anchor that binds that grammar above wallet instances.Kurz, 2026b

Reusable KYC and organizational-identity systems show that reuse and cross-party identity infrastructure already matter in regulated practice. Swift's KYC services and the Nordic Invidem utility exemplify shared due-diligence infrastructures for financial institutions.Business Information Industry Association, 2020; Society for Worldwide Interbank Financial Telecommunication, 2026 The Legal Entity Identifier gives legal entities a global register-anchored identifier, and the verifiable LEI extends organizational identity into verifiable credentials for entities and roles.Global Legal Entity Identifier Foundation, 2024, 2025 These systems address institutional reuse, organizational identification, and role presentation. Paper 15 generalises the reuse question into a profile-anchor tier over a reusable legal assurance state for natural, juridical, and machine actor constellations.

Ledger and self-certifying identifier systems provide adjacent infrastructure for integrity and control. KERI derives identifiers from key-event state and gives that state portability across ledgers.Smith, 2021 Sovrin demonstrated operational deployment of ledger-based self-sovereign identity.Sovrin Foundation, 2018 Distributed-ledger systems can also provide tamper-evident notarisation for proofs, consents, and dispute records, a substrate developed for agent orchestration in a companion framework.Kurz, 2026a In Paper 15, these systems support evidentiary integrity around an anchor tier whose legal semantics come from Paper 14 and whose verifier-facing assurance is scoped to a concrete presentation.

The resulting gap is the accountable aggregation tier above wallets and credential schemes. Existing work supplies identifiers, credentials, presentation protocols, assurance categories, sovereign wallets, reusable institutional due diligence, organizational identifiers, anonymous-credential primitives, pairwise pseudonyms, and ledger notarisation. The proposed tier joins those components around one design question: how a relying party can receive the minimum profile-scoped presentation needed for an act, while the system preserves independent confirmation-event clusters, lawful recourse, and a point-in-time reliance record. Adjacent regimes for crypto-assets European Union, 2023, artificial intelligence European Union, 2024c, and legal identity for all United Nations, 2015 make that question practically urgent.

3 Contribution

The building blocks are standards, privacy-preserving credential primitives, and the legal assurance substrate supplied by Paper 14. Paper 15 contributes the anchor tier that makes that substrate presentable, separable across contexts, and usable for trust decisions.

First, the paper defines an above-wallet hash-anchor tier. A root hash anchor commits to the off-chain EAID assurance state, while profile anchors let the same entity act in distinct contexts without disclosing the root anchor during ordinary interaction. The tier consumes credentials and wallet presentations as evidence packages and treats Paper 14 confirmation events as the units of assurance.

Second, the paper states the identifier and capability separation invariant for the anchor tier. The hash anchor names and commits; private keys authenticate; explicit consent and gate satisfaction authorize. This separation explains why the anchor can be public, why credentials and capabilities remain off-chain, and why erasure can target linkage and profile-binding state rather than the ledger commitment itself.

Third, the paper defines gate-specific triangulated assurance-at-time. The model evaluates independent confirmation-event clusters against a concrete gate predicate D_g at reliance time. The function discounts shared issuers, ceremonies, status authorities, and proof failure modes, while accounting for binding strength, freshness, revocation, and jurisdictional fit.

Fourth, the paper combines accountable pseudonymity, lawful resolution, and governed erasure as constraints in one architecture. Profile anchors support ordinary pseudonymous interaction; threshold-governed resolution preserves recourse under valid legal process; the two-layer erasure model preserves required records while removing personal linkage when retention no longer applies.

Fifth, the paper models assurance-mediated trust over reliance events. A relying party can transact with a profile anchor when the presentation satisfies the gate and a dispute can reach the legally relevant imputation point. This connects identity assurance to practical cooperation between parties that start without direct knowledge of each other.

4 System Model and Formal Framework

4.1 Inputs from legal identity assurance

This paper builds on the legal identity-assurance substrate developed in the companion paper.Kurz, 2026b That substrate distinguishes entities from actors: an entity exists, while an actor is an entity in the act being evaluated. It defines natural entities (N), juridical entities (J), and machine entities (M). A machine entity can act technically, but, under the present legal framing, it is not the terminal bearer of legal responsibility. Legally relevant machine action is presented through an admissible constellation, such as N+M, restricted J+M, or J+N+M, where a natural or juridical entity supplies the imputation point. A standalone M presentation is inadmissible for legally consequential gates unless future law supplies an independent legal identity for that machine entity; until then, J+M and J+N+M presentations also require role, mandate, or control evidence that connects the machine-mediated act to the accountable natural or juridical record.

The same substrate defines the Entity Actor Identity (EAID) coordinate grammar. An EAID coordinate, such as `EAID-N6-S7`, names one assertion row and one source-of-information rung: what identity-relevant item is disclosed, and who or what stands behind that item. Filled cells are supported by confirmation events. A confirmation event records the checked cells, source class, binding evidence, valid time, record time, revocation or status pointer, policy version, and proof package. A reliance event records the consuming-side act: who relied, for which capability, under which gate, law, actor constellation, time, and liability boundary. Paper 15 takes that legal grammar as input. It defines the hash-anchor layer that binds to it, presents it, and aggregates independent confirmation-event clusters for a concrete relying-party gate.

Definition 1 (Identifier and anchor)**.** *The Paper 15 root anchor is a self-issued, public, inert hash h that commits to an off-chain EAID assurance state and confers no capability. It is registered on a distributed ledger as a tamper-evident, timestamped commitment. A profile anchor h_i is a public, inert pseudonymous commitment for a defined context. Its public commitment is context-specific; its relation to h is held in the encrypted binding registry of Definition 4 and is shown to a relying party only through a gate-specific predicate proof or through lawful resolution. In this paper,* hash anchor *names this ledger fixed point. It is distinct from the jurisdictional anchor of the companion paper, which is a time-indexed legal relation used to evaluate an act under a governing law.*

Definition 2 (Evidence set)**.** *For a hash anchor h, let $\mathcal{E}(h)$ denote the set of confirmation events bound to the corresponding root EAID state. Each event may be carried by a verifiable credential, presentation, status entry, ledger proof, or other signed evidence package, but the unit of assurance is the confirmation event rather than the credential container.Terbu et al., 2025; World Wide Web Consortium, 2025*

4.2 Anchors and separation

Definition 3 (Separation invariant)**.** *An identifier names; it never authorises. All capability derives solely from possession of private keys (authentication) together with an explicit, fresh, consented grant (authorisation). Formally, knowledge of h alone yields no admissible action.*

Definition 3 separates three functions that legacy identifiers conflate: the anchor names, keys prove, and consent permits. Two consequences follow. The anchor is safe to publish and to anchor on a public ledger, because it is inert. The sensitive material is the off-chain linkage between the accountable legal record and the anchor, together with the private keys.

Definition 4 (Anchor hierarchy)**.** *An entity holds one root hash anchor h within a governance domain and may hold profile anchors $h_1, \ldots, h_m$. The binding registry $B(h) = \{h_1, \ldots, h_m\}$ between root and profile anchors is held off-chain and encrypted, like the linkage $L(h)$ between the accountable legal record and root anchor. The registry is never published. From h_i and h_j alone, an observer should not be able to determine whether both profile anchors bind to the same root, provided the implementation also partitions capabilities and correlation channels across profiles.*

The hierarchy resolves context rigidity. Familial, professional, and pseudonymous relationships each address a distinct profile anchor, while reusable legal identity assurance binds to the root. A presentation through a profile anchor proves that the root EAID state satisfies a gate predicate without revealing the root or any sibling profile. The construction uses the anonymous-credential and unlinkable-proof family discussed in the related work, while the complete root/profile predicate primitive remains an assumption of this paper. Lawful resolution applies uniformly: under the constraint of

Equation (3), a profile anchor resolves first to its root through $B(h)$ and then to the legal linkage $L(h)$, so context separation preserves accountability.

Unlinkability is a property of the whole capability surface, not of identifiers alone. Any capability shared across profile anchors, such as a common payment instrument, a common recovery handle, or correlated transport metadata, constitutes a linkage channel that collapses the separation. The threat model treats cross-profile capability sharing as an attack surface, and a conforming implementation partitions capabilities per profile.

4.3 Triangulated assurance and disclosure

A relying party declares a gate g for a concrete capability. Its demand predicate D_g imports Paper 14's gate grammar: required EAID cells, source floors, freshness windows, jurisdictional anchors, revocation conditions, and admissible actor constellations. For a disclosure response ρ through a profile anchor, let $\mathcal{E}_\rho(D_g, t) \subseteq \mathcal{E}(h)$ be the confirmation events that are disclosed, or predicate-proven, as supporting D_g at time t. The verifier-facing assurance calculation is limited to events presented through ρ. Events are equivalent, written $e \sim_{D_g} e'$, when they share a confirmer, ceremony, custody path, status authority, or proof failure mode relevant to D_g. Only equivalence classes count as independent corroboration.

Let $w_{[e]} \in [0,1]$ be the independence weight of an event class, $b_{[e]} \in [0,1]$ its binding and source-strength term, and $\varphi_{[e]}(D_g, t) \in [0,1]$ its gate-specific validity, freshness, revocation, and jurisdiction term. Where several events collapse into one equivalence class, the gate policy specifies the class summary rule, with the conservative default taking the weakest applicable binding, status, and freshness term. The verifier-facing triangulated assurance-at-time of response ρ for gate g is

$$A_\rho(D_g, t) = 1 - \prod_{[e] \in \mathcal{E}_\rho(D_g,t)/\sim_{D_g}} \Big(1 - w_{[e]}\, b_{[e]}\, \varphi_{[e]}(D_g, t)\Big). \tag{1}$$

Equation (1) is a gate-specific attribution-resilience form. It composes the independent confirmation-event clusters presented in ρ, discounts shared failure modes, and reads status and freshness at reliance time. General reputation scoring remains outside the model. The value is evaluated after the mandatory gate predicates have been addressed; by itself it grants no permission. Several official identities, addresses, payment-control events, and jurisdictional anchors can raise assurance for a gate when they supply source-diverse corroboration. Repeated evidence resting on the same issuer or ceremony is collapsed into its event class, and the loss or revocation of one event leaves only the remaining independent event classes available. The product form is a simple independence-adjusted fusion rule for this architecture, while broader trust and evidence-fusion formalisms remain comparators rather than prerequisites.Jøsang, 2016

A disclosure response ρ to a relying party r is admissible only if it carries explicit holder consent, discloses no more than requested, presents only holder-bound evidence packages, and presents only fresh, non-revoked evidence packages. With each factor in $\{0,1\}$,

$$\mathrm{adm}_g(\rho, t) = C_{\mathrm{consent}}(\rho) \cdot C_{\mathrm{min}}(\rho, g) \cdot C_{\mathrm{bind}}(\rho) \cdot C_{\mathrm{fresh}}(\rho, t) \cdot C_{\mathrm{status}}(\rho, t) \cdot C_{\mathrm{gate}}(\rho, g, t), \tag{2}$$

and ρ is released to r if and only if $\mathrm{adm}_g(\rho, t) = 1$. The final factor means that the disclosed package satisfies the declared gate predicate, including the required EAID cells, source floors, freshness windows, jurisdictional anchor, and constellation family. Where a gate also declares an assurance threshold θ_g, the factor includes $A_\rho(D_g, t) \geq \theta_g$. The threshold filters otherwise admissible presentations; it never replaces required cell, status, binding, or constellation predicates. Credential and presentation standards supply the carrying format; the gate semantics come from the legal identity-assurance model.Fett et al., 2025; Kurz, 2026b; Terbu et al., 2025; World Wide Web Consortium, 2025

4.4 Resolution, erasure, and trust

Lawful resolution of the linkage $L(h)$ between the anchor and the accountable legal record is governed rather than unilateral. It requires a valid legal order O and a quorum Q of at least k of n escrow key-holders,

$$\mathrm{resolve}_{\mathrm{law}}(h) = 1 \iff C_{\mathrm{legal}}(O) = 1 \ \wedge\ |Q| \geq k. \tag{3}$$

Equation (3) describes authorised resolution as a legal-state predicate. Threshold secret sharing can ensure that fewer than k key-holders cannot reconstruct the escrowed secret.Shamir, 1979 Collusion by k key-holders without a valid order is a governance and audit breach rather than a cryptographic impossibility. The architecture addresses it by separating operator access from key custody and by notarising every resolution event for later attribution.

Definition 5 (Two-layer erasure)**.** *Immutable on-ledger artifacts are commitments and proofs, and they are retained. While the linkage $L(h)$ exists, they constitute pseudonymised personal data and are processed under a retention basis European Data Protection Board, 2025; European Union, 2016. The linkage $L(h)$ and the binding registry $B(h)$ are held off-chain and encrypted. On an erasure request at time t, deletable linkage and profile-binding entries are removed unless a retention obligation $R(h_i, g, \ell, t) = 1$ holds for the affected profile, gate, reliance event ℓ, dispute window, or regulated record class. Deletion is deferred only for the obligated entries and performed when the obligation lapses. After deletion, the design claim is limited to removal of operator-side attribution means under the stated threat model; prior relying parties and institutions that lawfully retain disclosed preimages remain governed by their own retention duties.*

Definition 5 reconciles the right to erasure with retention duties at the architecture level: the chain is preserved, the personal linkage is removed subject to law, and anonymisation is pursued by erasing linkage rather than records. The architecture defends a sequenced claim, pseudonymous while linkage exists and anonymous only when the remaining data and reasonably available auxiliary information no longer permit attribution under a context-specific legal assessment. Together, Equations (2) and (3) with Definition 5 state sufficient architectural conditions under which pseudonymity, lawful access, erasure, and retention can coexist.

Consider a verifier P deciding whether to transact with a pseudonymous counterparty Q in a reliance event for gate g at time t. The verifier sees an admissible presentation through a profile anchor, plus the gate-specific assurance value $A_\rho(D_g, t)$. If Q defects, it gains u, but defection triggers recourse with probability $p(A_\rho(D_g, t), \chi)$, where χ denotes the legal reachability of the submitted actor constellation and resolution path. Recourse imposes a penalty s.

Proposition 1. *Cooperation is Q's best response whenever $u < p(A_\rho(D_g, t), \chi)\, s$. If recourse is sufficiently credible and punitive that $p(1, \chi)\, s > u$, and if p is increasing in gate-specific assurance for the submitted constellation, there exists a threshold A_g^* such that for $A_\rho(D_g, t) \geq A_g^*$ cooperation dominates defection. A gate policy that uses assurance as a transaction screen should set $\theta_g \geq A_g^*$ for the relevant act. If $p(1, \chi)\, s \leq u$, assurance for that gate falls short of deterring defection, and the rational verifier declines or collateralises the transaction.*

Proposition 1 formalises the central claim: trust between strangers comes from a verifiable, gate-scoped assurance presentation coupled with credible recourse. The relying party need not learn the civil identity during ordinary interaction. It needs to know that the profile anchor is backed by a root EAID state that satisfies the gate, and that a dispute can reach the legally relevant imputation point through the governed resolution path.

Six threats and their mitigations follow from the model. A borrowed or replayed presentation is defeated by the holder-binding factor C_{bind} in Equation (2). The compromise or coercion of a single confirmer is bounded by the event-cluster form of Equation (1), since gate-specific assurance does not rest on any one issuer, ceremony, or status authority. Assurance inflation by corroboration farming is bounded by the equivalence relation $\sim_{D_g}$ and by the independence weights $w_{[e]}$, whose governance Section 7 leaves open. Tampering with evidence is detected by ledger notarisation of proofs, consents, and dispute records. Unauthorised resolution of identity is constrained operationally by threshold custody, legal approval, separation of duties, and notarised resolution events; collusion by a valid quorum remains a governance breach with forensic evidence rather than an impossible act. Cross-profile linkage through shared capabilities is excluded only if an implementation partitions payment, recovery, and transport capabilities per profile anchor (Definition 4). Two residual risks remain: registry-level scraping of inert anchors, which grants no capability under Definition 3, and coercion of the holder, which no holder-bound scheme eliminates.

5 Discussion

The assurance presentation is evaluated over an actor constellation rather than over an isolated identifier alone. A relying party needs to know which constellation presented the anchor, which confirmation-event clusters support the requested gate, and which recourse path exists if the operation later becomes disputed. The hash-anchor layer carries or resolves to enough structured state for the relying party to distinguish a natural actor acting alone, a juridical actor acting through an accountable natural actor, a juridical actor acting through a natural anchor and a machine actor, a restricted juridical-machine constellation with legally sufficient delegation evidence, and a natural actor acting with a

machine actor. Standalone machine presentations are treated as technical action without terminal legal imputation in the present legal frame. The reliance question is whether this constellation is credible for the requested operation and whether recourse can reach the appropriate imputation point.

The construction shows conditions under which requirements usually treated as competing can be jointly satisfied. Selective disclosure and pseudonymity coexist with lawful identifiability through accountable pseudonymity and threshold-governed resolution; the right to erasure coexists with retention through the two-layer model. Because authorised resolution requires both a legal order and a key quorum, accountability is preserved while the operator lacks unilateral resolution power.

5.1 Applications across the Agnostyca core

The tier serves natural, juridical, and machine-mediated actor constellations across several application domains. A family-safety application uses accountable pseudonymity and contact gating directly. Platform attestations already instantiate part of the pattern in production: the declared age range of a mobile operating system Apple Inc., 2026 is an attested claim, verification-backed in some jurisdictions, that a relying party could consume as one confirmation event for an age-related gate without disclosure of the underlying data. A higher-education application uses credential binding and gate-specific assurance for enrolment and for signed, ledger-timestamped academic work. An enterprise artificial-intelligence application binds agent identity, attestations, and accountable action to the same anchor tier, so that one agent can evaluate whether another presents the required constellation and recourse path for a requested operation. The companion agent-orchestration framework Kurz, 2026a governs how actors coordinate; the present tier governs which assurance and imputation state they present, and the two share a ledger substrate.

5.2 Complementarity with national wallets

The tier can consume and present national credentials as high-quality confirmation sources when their issuance and presentation satisfy the relevant gate. A relying party that accepts the EU Digital Identity Wallet European Commission, 2025; European Union, 2024a receives a routed presentation; a relying party with a scheme-specific legal requirement receives the specific credential, while a relying party that accepts event-backed corroboration receives the gate-specific assurance result of Equation (1). A natural person who holds, for example, an Austrian credential, a Swiss credential Swiss Confederation, 2024, and a non-European credential can bind all three to one root assurance state while presenting only the profile and evidence package required for the act. By accepting credentials already held by the user, the tier gives new deployments an initial evidence base across schemes and jurisdictions.

6 Conclusion

Digital identity is rigid when provider accounts, wallet instances, context, and jurisdiction are fused into one operational identity. This paper has argued that the missing layer sits above wallets: an accountable hash-anchor tier that binds to Paper 14's legal assurance state, separates root and profile anchors, and lets relying parties evaluate gate-specific assurance-at-time over disclosed independent confirmation-event clusters. The hash anchor is deliberately inert. It names and commits, while keys authenticate, consent permits, gate predicates authorise, and governed resolution preserves recourse.

The model makes that architecture inspectable. The root/profile hierarchy separates contexts while preserving a lawful route to the accountable record. The assurance equation evaluates disclosed confirmation-event clusters at reliance time, discounting shared issuers, ceremonies, status authorities, and proof failure modes. The disclosure predicate fixes consent, minimisation, holder binding, freshness, status, and gate satisfaction as release conditions. The resolution, erasure, and reliance constructions then state how pseudonymity, lawful access, erasure, retention, and rational trust can hold together under the paper's assumptions.

For the paper series, P15 supplies the anchor and assurance-at-time layer between progressive legal identity assurance and accountable ledger operation. P14 defines the actor grammar, confirmation events, reliance events, jurisdictional anchors, and capability gates. P15 turns that state into root and profile anchors that can be presented, separated, resolved, erased, and relied on. The following ledger layer can then bind validator identities, observer records, and evidentiary commitments to anchors whose assurance state is already gate-scoped, replayable, and legally attributable.

DOI: 10.5281/zenodo.21901243 | Machine-readable record: https://journal.swissi-ai.institute/doi/zpd6gvtrfaun

7 Limitations and Future Research

Several constraints bound the present work. Registry-level invisibility is a soft property with residual access risk, even when the separation invariant prevents the anchor from carrying capability. Holder binding assumes secure key storage and a workable cross-device recovery model, which is the most operationally demanding component. Confirmation-event governance, including which events enter Equation (1), which shared failure modes define $\sim_{D_g}$, which summary rule applies within each event class, and which weights apply to event classes, requires an institutional process that this paper specifies only in outline. The model also treats event-class weights as scalar terms, while real evidence sources may have pairwise or higher-order correlations, for example two credentials drawing on the same civil registry. Modelling that correlation structure is future work. Presentations from profile anchors assume a predicate-proof primitive that proves gate satisfaction without revealing the root anchor, sibling profiles, or a stable cross-relying-party correlator. Anonymous credentials, AnonCreds, U-Prove, and BBS-style derived proofs supply important parts of that primitive; a complete construction binding those proofs to the root/profile hierarchy and the legal assurance state remains future work.Camenisch and Lysyanskaya, 2001; Hyperledger AnonCreds Project, 2026; Paquin and Zaverucha, 2013; World Wide Web Consortium, 2026 Threshold custody also requires a legal and operational design for key-holders, collusion controls, and the orders that trigger authorised resolution. The erasure claim remains context-specific: deleting linkage and profile-binding state removes operator-side attribution means, while prior relying parties, AML records, dispute files, and other lawful preimage holders remain governed by their own legal bases. The model is analytical; empirical validation through a reference implementation and a cross-jurisdiction pilot is future work, as is formal verification of the joint-satisfiability claim under adversarial confirmation-event behaviour.

References

Apple Inc. (2026). *Declared age range*. Apple Developer Documentation. Retrieved June 6, 2026, from https://developer.apple.com/documentation/declaredagerange/

Ashby, W. R. (1956). *An introduction to cybernetics*. Chapman & Hall. Retrieved June 9, 2026, from https://www.inist.org/library/1956.Ashby.Introduction%20to%20Cybernetics.Chapman%20and%20Hall.pdf

Business Information Industry Association. (2020, August 25). Nordic banks' agreement on one KYC standard a unique advantage for new utility. Retrieved June 9, 2026, from https://www.biia.com/nordic-banks-agreement-on-one-kyc-standard-a-unique-advantage-for-new-utility/

Camenisch, J., & Lysyanskaya, A. (2001). An efficient system for non-transferable anonymous credentials with optional anonymity revocation. *Advances in Cryptology, EUROCRYPT 2001, 2045*, 93–118. https://doi.org/10.1007/3-540-44987-6_7

Decentralized Identity Foundation. (2026). *Peer DID method specification*. Decentralized Identity Foundation. Retrieved July 24, 2026, from https://identity.foundation/peer-did-method-spec/

European Commission. (2025). *The european digital identity wallet architecture and reference framework*. European Commission. Retrieved May 26, 2026, from https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework

European Data Protection Board. (2025). *Guidelines 02/2025 on processing of personal data through blockchain technologies*. European Data Protection Board. Retrieved June 6, 2026, from https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data-through_en

European Union. (2016). *Regulation (eu) 2016/679 general data protection regulation*. Official Journal of the European Union. Retrieved May 26, 2026, from https://eur-lex.europa.eu/eli/reg/2016/679

European Union. (2023). *Regulation (eu) 2023/1114 on markets in crypto-assets*. Official Journal of the European Union. Retrieved May 26, 2026, from https://eur-lex.europa.eu/eli/reg/2023/1114

European Union. (2024a). *Regulation (eu) 2024/1183 amending regulation (eu) no 910/2014 as regards establishing the european digital identity framework* [eIDAS 2.0]. Official Journal of the European Union. Retrieved May 26, 2026, from https://eur-lex.europa.eu/eli/reg/2024/1183

European Union. (2024b). *Regulation (eu) 2024/1624 on the prevention of the use of the financial system for money laundering or terrorist financing*. Official Journal of the European Union. Retrieved May 26, 2026, from https://eur-lex.europa.eu/eli/reg/2024/1624

European Union. (2024c). *Regulation (eu) 2024/1689 laying down harmonised rules on artificial intelligence (ai act)*. Official Journal of the European Union. Retrieved May 26, 2026, from https://eur-lex.europa.eu/eli/reg/2024/1689

Fett, D., Yasuda, K., & Campbell, B. (2025). *Selective disclosure for jwts (sd-jwt)*. IETF, Internet-Draft. Retrieved May 26, 2026, from https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/

Global Legal Entity Identifier Foundation. (2024). The verifiable LEI (vLEI). Retrieved July 24, 2026, from https://www.gleif.org/en/organizational-identity/introducing-the-verifiable-lei-vlei

Global Legal Entity Identifier Foundation. (2025). The legal entity identifier (LEI) and the ISO 17442 standard. Retrieved June 9, 2026, from https://www.gleif.org/en/about-lei/iso-17442-the-lei-code-structure

Goffman, E. (1959). *The presentation of self in everyday life*. Doubleday.

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2024). *Digital identity guidelines* (NIST Special Publication No. 800-63). National Institute of Standards and Technology. Retrieved May 26, 2026, from https://pages.nist.gov/800-63-4/

Hyperledger AnonCreds Project. (2026). *AnonCreds specification*. Linux Foundation Decentralized Trust. Retrieved July 24, 2026, from https://hyperledger.github.io/anoncreds-spec/

International Organization for Standardization. (2021). *Iso/iec 18013-5 personal identification, iso-compliant driving licence, part 5 mobile driving licence (mdl) application*. ISO. Retrieved May 26, 2026, from https://www.iso.org/standard/69084.html

Jøsang, A. (2016). *Subjective logic: A formalism for reasoning under uncertainty*. Springer. https://doi.org/10.1007/978-3-319-42337-1

Kurz, W. (2026a). Generic ai-dlt enterprise system [Architecture and methodology for scalable domain adaptation from a unified core framework].

Kurz, W. (2026b). Multi-jurisdictional actor identity assurance for capability gating [A Design-Science Proposal for Tiered, Reusable Identity Assurance of Natural, Juridical, and Machine Actors].

Luhmann, N. (1995). *Social systems* (J. Bednarz & D. Baecker, Trans.). Stanford University Press.

Marwick, A. E., & boyd danah, d. (2011). I tweet honestly, i tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114–133. https://doi.org/10.1177/1461444810365313

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Paquin, C., & Zaverucha, G. (2013). U-prove cryptographic specification v1.1, revision 3. *Microsoft*. Retrieved July 24, 2026, from https://www.microsoft.com/en-us/research/publication/u-prove-cryptographic-specification-v1-1-revision-3/

Schardong, F., & Custódio, R. (2022). Self-sovereign identity: A systematic review, mapping and taxonomy. *Sensors*, *22*(15), 5641. https://doi.org/10.3390/s22155641

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *22*(11), 612–613. https://doi.org/10.1145/359168.359176

Smith, S. M. (2021). *Key event receipt infrastructure (keri)*. arXiv. Retrieved June 6, 2026, from https://arxiv.org/abs/1907.02143

Society for Worldwide Interbank Financial Telecommunication. (2026). Know your customer (KYC). Retrieved July 24, 2026, from https://www.swift.com/risk-and-compliance/know-your-customer-kyc

Sovrin Foundation. (2018). *Sovrin: A protocol and token for self-sovereign identity and decentralized trust*. Sovrin Foundation, whitepaper. Retrieved June 6, 2026, from https://sovrin.org/library/sovrin-protocol-and-token-white-paper/

Swiss Confederation. (2024). *Federal act on electronic proof of identity and other electronic credentials (e-id act)*. Federal Council of Switzerland. Retrieved May 26, 2026, from https://www.eid.admin.ch/

Terbu, O., Lodderstedt, T., Yasuda, K., & Looker, T. (2025). *Openid for verifiable presentations*. OpenID Foundation. Retrieved May 26, 2026, from https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

United Nations. (2015). *Sustainable development goal 16.9, legal identity for all including birth registration*. United Nations. Retrieved May 26, 2026, from https://sdgs.un.org/goals/goal16

World Wide Web Consortium. (2022). *Decentralized identifiers (dids) v1.0*. W3C Recommendation. Retrieved May 26, 2026, from https://www.w3.org/TR/did-core/

World Wide Web Consortium. (2025). *Verifiable credentials data model*. W3C Recommendation. Retrieved May 26, 2026, from https://www.w3.org/TR/vc-data-model-2.0/

World Wide Web Consortium. (2026). *Data integrity BBS cryptosuites v1.0*. W3C Candidate Recommendation Draft. Retrieved July 24, 2026, from https://www.w3.org/TR/vc-di-bbs/

Declarations

CITE THIS ARTICLE (BIBTEX)

```
@article{saijzpd6gvtrfaun,
   author  = {Kurz, W.},
   title   = {Credentials and Triangulated Trust Signals on a Single Accountable Identifier: A Hash-Anchored
              Distributed-Ledger Framework for Portable Identity across Jurisdictions},
   journal = {Swissi AI Journal},
   year    = {2026},
   volume  = {2026},
   note    = {Article SAIJ-zpd6gvtrfaun},
   issn    = {3043-1921},
   doi     = {10.5281/zenodo.21901243},
   url     = {https://journal.swissi-ai.institute/doi/zpd6gvtrfaun}
}
```

PAPER INFORMATION

AFFILIATIONS	[1]Swissi Institute for AI, kurz@swissi-ai.institute
CORRESPONDING AUTHOR	Walter Kurz, kurz@swissi-ai.institute, ORCID 0009-0006-8045-4775

ARTICLE TYPE	Research Article
SWISSI ADDRESS	`Sw2:academic01:obj:p1:zpd6gvtrfaungxr7pdoqhjkjyegvntecpvh6kzpzwxadbo2ap7ga:9bb91bcf`

PAPER DECLARATIONS

AUTHOR CONTRIBUTIONS	The author is solely responsible for this article.
FUNDING	This research received no external funding.
CONFLICTS OF INTEREST	The author declares no conflicts of interest.
DATA AND CODE AVAILABILITY	The data and code supporting this article are available from the corresponding author on reasonable request.
USE OF AI TOOLS	Generative AI tools were used for editorial work only, such as language editing and formatting, in accordance with international scientific standards. The author verified the content and remains fully responsible for the article.

JOURNAL INFORMATION

PUBLISHER	Swissi AI Journal
EDITORIAL DATES	Submitted 05/26; Revised 06/26; Published 07/26
LICENCE	CC BY 4.0
OPEN ACCESS	https://journal.swissi-ai.institute/authors#open-access
CREDIT TAXONOMY	https://journal.swissi-ai.institute/authors#credit-taxonomy
JOURNAL CONTACT	https://journal.swissi-ai.institute | journal@swissi-ai.institute