Identity That Travels: Reusable Trust across Regulated Workflows

A transaction and operating framework for acquiring, scaling and governing reusable digital-credential platforms

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Reusable digital identity promises to replace repeated document collection with verified claims that can be presented across banking, employment, government, healthcare and other regulated workflows. The commercial opportunity is attractive: an identity provider can amortise proofing cost across many transactions, a verifier can shorten onboarding, and a user can disclose fewer attributes. The transaction problem is harder. Technical portability does not create legal reliance, regulatory acceptance, revocation coverage or transferable economics by itself.

This paper develops a Reusable Trust Transaction Framework for boards, investors, acquirers and regulated institutions. It separates proofing, credential issuance, wallet custody, presentation, verification, consent, revocation, fraud response, recordkeeping and legal reliance. It translates those functions into a trust graph, liability allocation, regulatory map, unit-economics model, diligence tests and post-completion integration plan. The framework treats a reusable credential as a living evidence object whose value depends on the issuer, assurance level, freshness, permitted purpose and verifier's continuing obligations.

Current primary sources show a market moving from broad concepts to implementable standards. NIST Special Publication 800-63-4, finalised in 2025, defines risk-based requirements across proofing, authentication and federation. W3C Verifiable Credentials Data Model 2.0 became a Recommendation in May 2025. OpenID for Verifiable Credential Issuance 1.0 became final in September 2025. The European Digital Identity Framework and implementing regulations create a legal and technical architecture for wallets and electronic attestations. The United Kingdom's statutory Digital Verification Services framework links certification to a public register. UAE Pass, Saudi national digital identity and Central Bank of the UAE guidance demonstrate how national identity rails and regulated customer due diligence can intersect.

A wholly hypothetical acquisition case values a credential-network company through verified transaction volume, reuse, gross contribution and liability-adjusted retention. The base scenario starts with 3.0 million annual presentations, a USD 1.25 verifier fee and a 32 percent first-year reuse rate. It tests value under higher adoption, lower prices, fraud losses, refresh cost and jurisdiction-specific acceptance. Every amount, rate and operating assumption in the case is illustrative management input. It is not observed company data, a market forecast, a valuation opinion or an offer of financing.

The central conclusion is that reusable trust travels only as far as its evidence and governance. Acquirers should price proven relying-party acceptance, credential freshness, liability clarity, interoperability and workflow conversion. They should discount registrations, wallet downloads and

issued credentials that do not lead to accepted regulated transactions. A durable platform makes assurance visible, limits disclosure, supports revocation and recovery, preserves audit evidence and gives each verifier enough information to decide whether reliance is lawful for the particular purpose.

JEL Classification: G21, G24, G34, K22, K24, L15, L86, O31, O33

Keywords: reusable digital identity, verifiable credentials, digital wallets, regulated workflows, identity assurance, credential portability, trust frameworks, M&A, compliance, interoperability

This paper is an educational and structural analysis prepared for research purposes. It is not investment advice, an offer, or a solicitation. It contains no client information.

1. DEFINE THE REUSABLE-TRUST ASSET

A reusable-trust asset allows an individual or authorised representative to present verified identity or attribute evidence to more than one relying party. The asset can include an identity-proofing service, issuer, wallet, credential registry, presentation protocol, verifier, trust list and governance rules. The commercial product is therefore a system of coordinated functions, not a single app.

Boards should define the asset through accepted outcomes. A credential has economic relevance when a regulated workflow accepts it, the verifier can establish provenance and status, and the transaction produces a defensible record. Issuance volume without acceptance can become inventory rather than network activity.

The investment thesis should identify which attributes travel, which parties issue them, where they are accepted, which assurance level applies, how status is checked and who carries loss when evidence is wrong or stale. Those questions define the addressable workflow and the transaction perimeter.

Table 1. Reusable-trust value layers and transaction evidence

Value layer	Required evidence	Principal transaction question	Typical protection
Proofing	Evidence policy, assurance mapping and fraud results	Was the subject established to the required standard?	Warranty, audit and performance covenant
Issuance	Authority, schema, signing controls and lifecycle	Is the issuer entitled and technically able to make the claim?	Trust-list condition and key-control schedule
Wallet	Binding, consent, recovery and privacy controls	Can the holder control presentation securely?	Security baseline and recovery test
Verification	Policy engine, status check and decision record	Can a relying party lawfully accept the credential?	Acceptance criteria and evidence retention
Network	Active issuers, verifiers and accepted workflows	Does reuse produce repeat transactions?	Earn-out linked to verified usage
Liability	Error, fraud, outage and redress allocation	Who pays when reliance fails?	Caps, insurance, indemnities and reserves

Each layer requires a named owner, measurable service and enforceable obligation.

2. SEPARATE IDENTITY FROM ELIGIBILITY

Regulated workflows often need a decision about eligibility rather than a complete identity file. A service may need proof that a person is over a threshold age, licensed for a role, authorised to

represent a company or resident in a jurisdiction. Selective disclosure can reduce unnecessary data collection when the governing rule permits it.

The credential model should separate foundational identity attributes from derived or purpose-specific claims. A full legal name and date of birth may support customer identification. An age-over-threshold credential can support a narrower transaction. An employment credential can confirm role and organisation without exposing salary or home address.

Acquirers should examine whether the target's schemas support minimum disclosure, whether verifiers actually request it, and whether product economics depend on collecting more personal data than the workflow needs. Privacy-preserving design can reduce data exposure while requiring careful policy mapping and verifier education.

3. MAP THE TRUST GRAPH

The trust graph links the subject, evidence source, proofing provider, credential issuer, wallet, verifier, regulated institution, auditor, regulator and redress channel. Each edge represents authority, data flow, assurance or liability. A weakness at one edge can invalidate the transaction outcome.

The issuer must know which evidence supports the claim. The wallet must protect the holder's key and consent. The verifier must authenticate the issuer, validate the credential, check its status and apply a use-case policy. The regulated institution remains responsible for obligations that cannot be delegated.

The data room should contain a machine-readable inventory and a governance view. The inventory shows identifiers, schemas, protocols, trust lists, keys and status mechanisms. The governance view shows contracts, certification, audit, complaints, insurance and regulator interfaces.

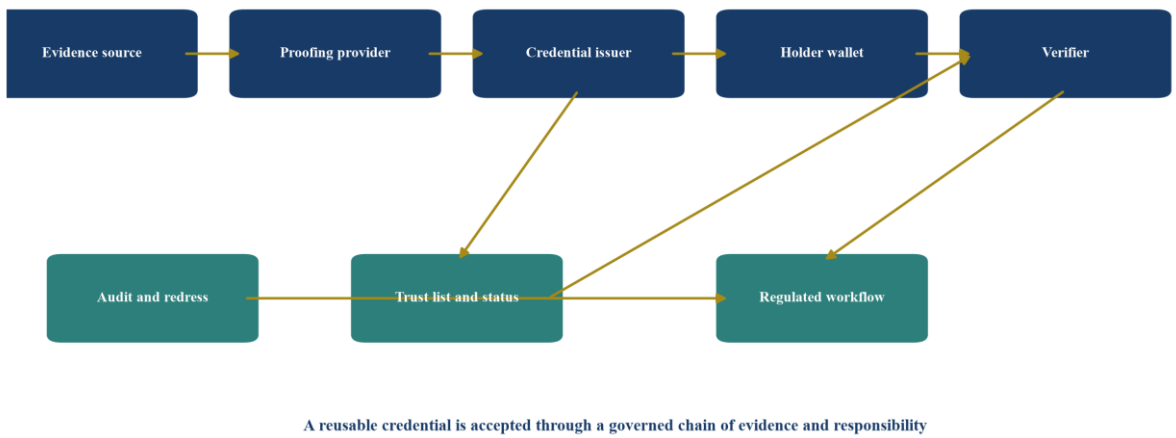

Figure 1. Reusable digital-credential trust graph

The verifier's decision depends on evidence provenance, credential status, holder control and use-case policy.

4. START WITH THE REGULATED DECISION

The correct design begins with the decision a regulated institution must make. Customer identification, right-to-work checking, professional licensing, benefits eligibility and patient access have different statutory purposes, evidence requirements, retention rules and consequences.

The transaction team should define the decision, accountable entity, applicable rule, minimum evidence, assurance level, refresh requirement and record. A credential that is sufficient for a low-risk service may be insufficient for a higher-risk product or enhanced due diligence.

The platform should express policy at workflow level. A generic verified badge provides weak evidence. A verifier requires the issuer, credential type, assurance, validity, status, disclosed attributes, presentation binding and decision policy used at the relevant time.

5. DISTINGUISH PROOFING, AUTHENTICATION AND FEDERATION

NIST SP 800-63-4 separates identity proofing, authentication and federation. Proofing establishes confidence in the claimed identity. Authentication establishes that the claimant controls an authenticator. Federation conveys assertions between parties. A reusable-credential platform can touch all three and should not collapse them into one score.

The target's assurance mapping should show which evidence and controls support each level. A strong authenticator does not cure weak original proofing. High-quality proofing does not prevent later account takeover. A valid federation assertion does not establish that every relying party may use the data for its chosen purpose.

Acquisition diligence should reproduce the assurance mapping from raw controls, samples and audit reports. Marketing labels should not substitute for standards-based evidence. Gaps should flow into pricing, remediation and conditions precedent.

6. TREAT CREDENTIAL ISSUANCE AS A REGULATED PRODUCTION PROCESS

Issuance converts proofed evidence into a signed claim. The issuer needs authority, schema governance, key management, lifecycle controls and a defined relationship with the subject. It should prevent duplicate or conflicting credentials, control delegated issuance and maintain traceable records.

OpenID for Verifiable Credential Issuance 1.0 defines an OAuth-protected issuance API and supports multiple credential formats. The standard enables interoperable delivery. It does not decide whether the issuer is legally trusted, whether proofing was sufficient or whether the verifier can rely on the claim.

The acquirer should inspect signing-key custody, rotation, compromise response, schema change, credential refresh and deferred issuance. A platform's issuance throughput has little value if operational controls cannot support regulatory acceptance.

7. ASSESS WALLET CONTROL AND RECOVERY

The wallet binds credentials to a holder and mediates presentation. Its security depends on device binding, key protection, authentication, consent, backup and recovery. Recovery is commercially essential and can create a route for fraud if it is weaker than initial enrolment.

The diligence team should test lost-device, number-change, key-rotation, death, incapacity and account-compromise scenarios. It should identify whether the issuer, wallet provider or national identity rail re-establishes control. Recovery events should be logged and available to status and risk systems.

Wallet portability also matters. A credential ecosystem can claim user control while binding accepted credentials to one proprietary wallet. The transaction model should distinguish portable formats from practical migration, including key binding, issuer policy and relying-party acceptance.

8. MAKE PRESENTATION PURPOSE-BOUND

A presentation should disclose the attributes necessary for a defined transaction. The request should identify the verifier, purpose, requested claims and retention expectations. The wallet should allow the holder to understand and authorise the disclosure.

Purpose binding supports privacy and dispute resolution. It helps distinguish a legitimate request from credential harvesting. It also allows the verifier to retain evidence of consent and policy without storing every source document.

Selective disclosure and derived claims should be assessed in the legal context of the workflow. Technical ability to reveal less data does not automatically change a regulated recordkeeping requirement. The platform should preserve policy evidence for both the disclosed result and the decision to request it.

9. VALIDATE STATUS AT THE MOMENT OF RELIANCE

Credential validity is time-sensitive. Employment ends, licences expire, sanctions status changes, keys are compromised and source records are corrected. A signed credential can remain cryptographically intact while becoming inappropriate for reliance.

The verifier should know whether to check expiry, revocation, suspension, refresh or the authoritative source. Status mechanisms should minimise correlation and data leakage while giving the verifier timely evidence. Availability and latency become part of the service level.

The acquirer should measure the share of presentations with a completed status check, average status age, failed checks, stale credentials and false declines. Liability terms should reflect what the verifier can observe and what the issuer promises to update.

10. BUILD THE CREDENTIAL GRAPH

The credential graph records relationships among schemas, issuers, evidence sources, wallets, verifiers and workflows. It allows the owner to see where one credential supports several services and where one workflow depends on several credentials.

Graph quality matters more than raw node count. A thousand issued credential types with few accepting verifiers can create maintenance cost. A smaller set of well-governed credentials

accepted across high-frequency workflows can support stronger reuse and contribution economics.

The graph should carry assurance, jurisdiction, version, validity, status method, legal basis and acceptance policy. It should support impact analysis when a key, issuer, schema or regulation changes.

11. DEFINE INTEROPERABILITY IN LAYERS

Interoperability has several layers: syntax, protocol, cryptography, semantics, trust and legal acceptance. Two systems can exchange a credential and still disagree about attribute meaning, issuer authority or permitted reliance.

W3C Verifiable Credentials Data Model 2.0 defines a common data model. OpenID4VCI defines issuance flows. Presentation protocols, credential formats and trust frameworks add further layers. Production interoperability requires agreed profiles, conformance tests and verifier policy.

The target should maintain a versioned implementation profile that identifies supported formats, algorithms, identifiers, schemas, protocols, status methods and trust lists. Deviations and extensions should be visible. Proprietary extensions can differentiate a service and increase switching cost.

12. PRICE STANDARDS MATURITY CORRECTLY

Standards can be recommendations, final specifications, drafts or implementation profiles. Maturity affects change cost and integration risk. A platform should not receive the same valuation credit for a production deployment on a final profile as for a pilot built on moving drafts.

The acquirer should record the status and dependency of every critical standard at the valuation date. It should test how the target manages version changes and backward compatibility. A standards roadmap should link development spend to customer obligations and migration windows.

Open standards reduce some forms of lock-in. They also move differentiation toward trust governance, workflow integration, user experience, fraud controls and distribution. The valuation should identify which advantages remain proprietary and defensible after interoperability improves.

13. MAP LEGAL RECOGNITION SEPARATELY FROM TECHNICAL ACCEPTANCE

The European Digital Identity Framework gives wallets and electronic attestations a defined legal architecture. The United Kingdom uses certification and a statutory register for Digital Verification Services. National identity platforms in the Gulf operate within different legal and institutional arrangements. These regimes should not be assumed equivalent.

The regulatory map should identify issuer recognition, wallet requirements, verifier obligations, certification, audit, cross-border treatment, electronic-signature effects, data protection and redress. It should also show whether acceptance is mandatory, permitted or left to a sector regulator.

A global product may therefore require local trust adapters rather than one universal compliance claim. The platform's reusable core can include protocols, policy engine and evidence ledger. Local modules can manage trust lists, assurance mapping, retention and liability.

Table 2. Illustrative regulatory acceptance map

Market	Primary trust mechanism	Reuse opportunity	Diligence focus
European Union	EUDI Wallet regulation, implementing acts and recognised trust services	Cross-border public and private use cases	Wallet certification, relying-party registration and attribute authority
United Kingdom	Statutory DVS trust framework, certification and public register	Certified verification across designated and commercial services	Scope of certification, supplementary codes and register status
United Arab Emirates	UAE Pass, digital signatures and sector-specific rules	Government and private-sector identity use	National-rail integration, CDD duties and recordkeeping
Saudi Arabia	National digital identity and Nafath services	Government and private-service authentication	Service agreement, biometric controls and local governance
United States	Risk-based assurance profiles and sector requirements	Federated government and private workflows	NIST mapping, state rules and relying-party policy

Transaction teams must confirm current law and sector rules for each workflow.

14. PRESERVE REGULATED-ENTITY ACCOUNTABILITY

A bank, employer, healthcare provider or public authority may use an identity provider and remain accountable for the regulated decision. Outsourcing evidence collection does not transfer every duty. The institution needs enough information to assess reliability and respond to exceptions.

Central Bank of the UAE guidance addresses digital identity for customer due diligence and states that portability and interoperability can allow credentials to support new relationships. It also makes clear that identity verification is only part of wider CDD, including beneficial ownership, purpose and ongoing monitoring.

Contracts should preserve audit, information, incident, regulator-access and exit rights. The service description should state which control the provider performs and which decision remains with the customer. Sales materials that imply complete compliance can create conduct and liability risk.

15. ALLOCATE RELIANCE LIABILITY

Loss can arise from incorrect source data, weak proofing, issuer error, wallet compromise, stale status, verifier policy, user fraud or service outage. Each cause sits with a different actor. A generic limitation of liability can leave the network commercially unusable.

The liability schedule should map event, evidence owner, prevention control, notification, remediation, financial responsibility and insurance. It should distinguish direct service loss from regulatory penalty, fraud loss, identity harm and consequential business interruption.

Caps can vary by control and fault. A provider can accept stronger responsibility for failure to follow its certified process than for an authoritative source error it could not detect. The verifier

should bear decisions outside the agreed policy. Shared-fault rules need evidence and dispute mechanisms.

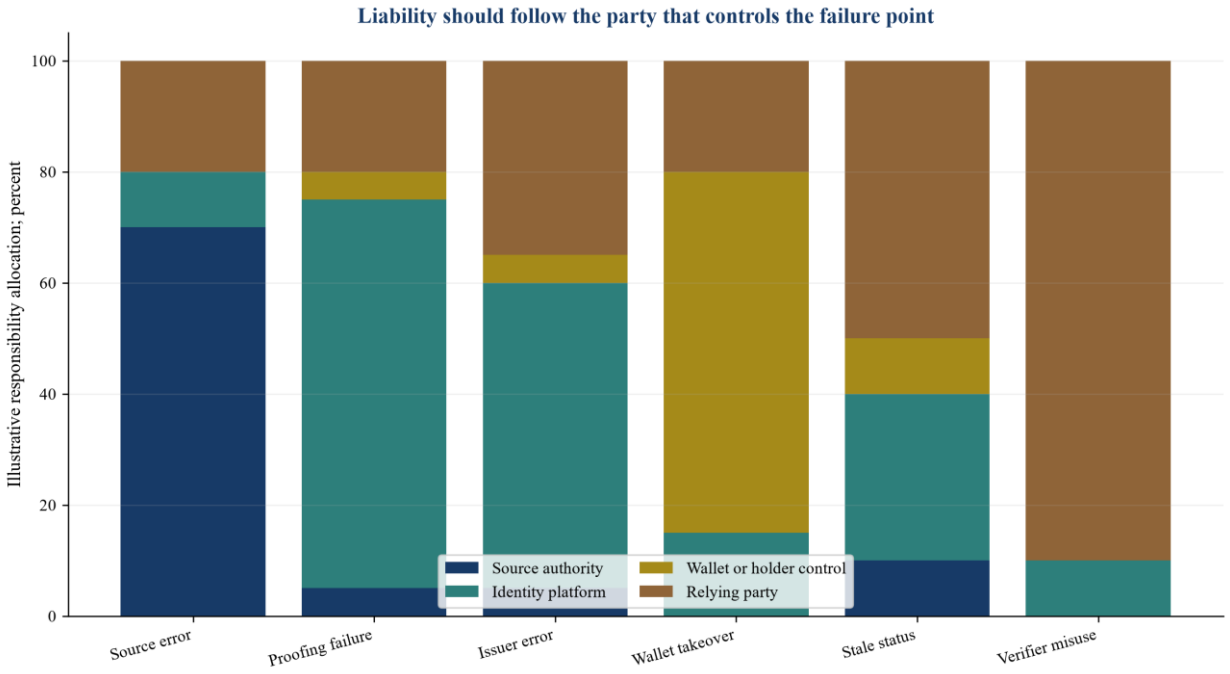

Figure 2. Liability allocation across the credential lifecycle

Commercial responsibility should follow control, evidence and the ability to prevent loss.

16. MODEL FRAUD AS A NETWORK COST

Fraud affects proofing cost, support, chargebacks, customer retention, insurance and regulatory confidence. Reuse can lower repeated proofing expense and propagate a compromised identity if lifecycle controls fail. The model should therefore treat fraud as a dynamic network cost.

The target should report attack type, attempted events, prevented events, confirmed loss, customer harm, recovery time and control changes. Rates should use consistent denominators. A low confirmed-loss rate can reflect weak detection or loss allocation to customers.

Acquisition modelling should include fraud loss, manual review, step-up checks and remediation. It should test whether higher reuse improves signal through known history or increases correlated exposure. Scenario design should avoid assuming that scale automatically improves trust.

17. BUILD PRIVACY INTO THE ECONOMICS

Data minimisation can reduce storage, breach exposure and customer friction. It can also limit secondary data monetisation. A platform whose valuation depends on unrestricted identity data may face legal, contractual and reputational constraints.

The unit-economics model should identify revenue from verification, orchestration, issuer services, wallet services and workflow software separately from data use. It should assign compliance, security, deletion and subject-rights cost to the relevant product.

Selective disclosure, pairwise identifiers and privacy-preserving status checks can reduce correlation. The diligence team should test actual configuration and logs. Privacy features that exist in a protocol but are disabled in production should receive no operating credit.

18. ASSESS BIOMETRIC DEPENDENCE

Biometrics can support proofing and authentication. They introduce accuracy, presentation-attack, demographic, consent, storage and recovery risks. A reusable platform should state where biometric templates or derived signals reside and which parties can access them.

The acquirer should review testing methodology, operating thresholds, false acceptance, false rejection, manual review and accessibility. Results should be disaggregated where lawful and appropriate. Vendor claims should be reconciled with the target's own population and environment.

Biometric failure should not exclude legitimate users without a workable alternative. The operating model needs exception and redress routes. A national identity rail may supply a high-trust assertion while the relying party still manages its product-specific risk.

19. ENGINEER INCLUSION AND ASSISTED ROUTES

Digital identity systems can reduce friction for many users and exclude people with limited documentation, devices, connectivity, digital skills or matching records. Inclusion is an operating requirement and can affect adoption, regulator support and customer economics.

The United Kingdom's trust framework emphasises inclusive design and monitoring. A target should measure completion, abandonment, manual referral and complaint rates by relevant pathway. It should maintain vouching or assisted alternatives where the applicable framework permits them.

The valuation should include the cost of support and exception handling. High automated completion achieved by excluding difficult cases can overstate market coverage. A buyer should value reliable service across the intended population.

20. DESIGN REDRESS AS PART OF TRUST

Users need a way to challenge incorrect attributes, failed verification, account takeover and unauthorised disclosure. Issuers, wallets and verifiers should know which party owns each correction. A redress journey that sends the user around the trust graph erodes acceptance.

The service should provide case ownership, evidence collection, response time, urgent suspension and appeal. Corrected source data should propagate to credential status and reissuance. The platform should preserve a record without retaining unnecessary personal data.

Acquirers should inspect complaint samples, root causes, ageing and outcomes. Redress cost belongs in unit economics. Repeat complaints linked to one issuer, schema or verifier can reveal a structural weakness.

21. BUILD THE OPERATING CONTROL PLANE

The control plane should manage issuer onboarding, schema approval, trust lists, keys, policies, status, monitoring, incidents and audit evidence. It converts a collection of integrations into a governed network.

Every material change should have an owner, approval, effective date and rollback. Trust-list additions require due diligence and periodic review. Schema changes require versioning and verifier migration. Key events require coordinated status and communication.

The buyer should decide which controls remain central and which can be delegated to jurisdictions or business units. Central standards support reuse. Local authority is necessary where law, language, evidence and regulator expectations differ.

22. ESTABLISH CYBERSECURITY AND CRYPTOGRAPHIC GOVERNANCE

The platform handles identity evidence, signing keys, wallet interactions and verifier decisions. Security architecture should cover privileged access, key management, software supply chain, encryption, secrets, logging, vulnerability response, penetration testing and incident notification.

Cryptographic agility matters because algorithms, libraries and regulatory profiles evolve. The target should inventory algorithms and dependencies, support rotation and maintain a migration plan. Long-lived credentials can outlast a technology assumption.

The diligence team should test compromise scenarios: issuer key theft, malicious schema change, wallet malware, trust-list poisoning and status outage. Recovery objectives should reflect the systemic effect of the service.

23. MEASURE THE ACCEPTANCE FUNNEL

The commercial funnel begins with eligible users and ends with accepted regulated transactions. Intermediate counts include enrolled users, issued credentials, active wallets, presentation attempts, verified presentations, workflow completion and subsequent reuse.

Each stage needs a stable definition. A wallet installation should not be counted as a credential. A successful cryptographic verification should not be counted as regulatory acceptance if the workflow later rejects the evidence. A repeat presentation within one session may not represent meaningful reuse.

The buyer should cohort results by issuer, verifier, workflow, jurisdiction and credential age. This analysis reveals whether network effects are broad or concentrated in one anchor customer.

Table 3. Acceptance-funnel metrics for transaction diligence

Stage	Core metric	Quality test	Valuation relevance
Eligible population	Addressable users in contracted workflows	Legal and technical eligibility	Market ceiling
Issuance	Valid credentials delivered	Proofing assurance and activation	Supply creation
Presentation	Holder-approved attempts	Binding, consent and protocol success	Engagement
Verification	Credential and status validated	Trust-list and policy completion	Technical utility
Workflow acceptance	Regulated decision completed	Customer evidence and exception rate	Revenue quality
Reuse	Accepted use at another time or verifier	Independent transaction and retention	Network value

Value should be linked to accepted workflow outcomes rather than registrations alone.

24. DEFINE REUSE PRECISELY

Reuse can mean a second presentation to the same verifier, a different product at one institution, a different institution in one sector, or a cross-sector transaction. These events have different commercial and regulatory significance.

The transaction model should define qualified reuse. A strong definition can require a separate workflow, valid consent, successful status check and accepted outcome. Cross-verifier reuse provides stronger evidence of portability than repeated login.

The platform should report time to reuse, credentials per holder, accepting verifiers per credential and accepted workflows per active holder. Concentration should be visible. A reuse rate driven by one mandatory government service may not transfer to commercial workflows.

25. CONSTRUCT CONTRIBUTION ECONOMICS

Revenue can be charged per proofing, issuance, active wallet, presentation, verification, subscription or completed workflow. Cost can include evidence checks, biometrics, data sources, cloud, fraud, support, certification, insurance and integration.

The model should assign one-time proofing cost and recurring lifecycle cost separately. Reuse can improve contribution when later verifications avoid repeated evidence acquisition. That benefit may be shared among issuer, wallet, network and verifier through pricing.

The buyer should model price compression as standards and national rails mature. Defensibility can move toward workflow integration, assurance, distribution and risk performance. A per-verification fee without switching cost or differentiated acceptance may decline.

26. BUILD THE HYPOTHETICAL ACQUISITION CASE

The illustrative target supports 3.0 million annual credential presentations. The base scenario assumes a USD 1.25 verifier fee, a 32 percent qualified reuse rate, 72 percent gross retention of verifier revenue before central operating cost, and USD 0.18 of average lifecycle and status cost per presentation.

The case separates recurring verifier revenue from implementation fees. It excludes data monetisation. It includes fraud and redress reserves as explicit costs. A higher-reuse scenario increases accepted volume and lowers average proofing cost. A stress scenario reduces price, delays verifier onboarding and raises fraud response cost.

These assumptions explain a valuation method. They are not claims about any company or market. A real acquisition requires customer-level contracts, cohort data, audited revenue, cost allocation and regulatory confirmation.

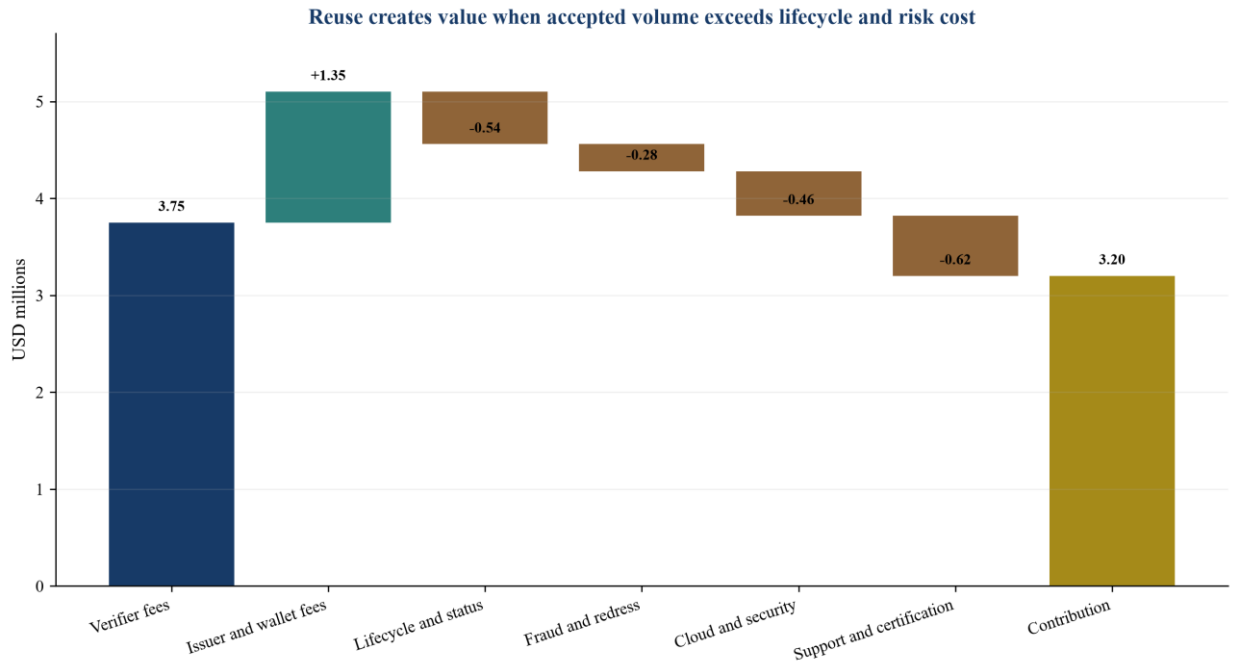

Figure 3. Hypothetical annual contribution bridge for a reusable-credential platform

Illustrative management assumptions in USD millions; values are not observed company data.

27. TEST SENSITIVITY BEFORE APPLYING A MULTIPLE

The principal variables are accepted presentation volume, qualified reuse, price, gross retention, proofing cost, fraud loss, customer concentration and regulatory acceptance. The model should expose each variable before applying a revenue or earnings multiple.

The base case can test reuse at 20, 32 and 50 percent; verifier price at USD 0.85, USD 1.25 and USD 1.60; and fraud-plus-redress cost at 3, 7 and 14 percent of revenue. Interaction matters because aggressive growth can lower price and increase exception cost.

Valuation should distinguish contracted volume, observed cohort behaviour and management pipeline. Pipeline should be probability-weighted only with clear evidence. Mandatory regulatory change can create demand and implementation bottlenecks at the same time.

Sensitivity note. Illustrative contribution ranges from USD 0.89 million to USD 3.52 million.

28. VALUE NETWORK EFFECTS CAUTIOUSLY

A reusable credential can become more valuable as more issuers and verifiers participate. Network effects require compatible governance, accepted schemas and low incremental connection cost. Participant count alone is weak evidence.

The buyer should measure cross-side activation: whether each new issuer creates accepted transactions across existing verifiers and whether new verifiers increase reuse of existing credentials. It should assess multihoming and switching. Standards can make networks more connected and reduce exclusivity.

The strongest asset can be a trusted distribution position in regulated workflows. That position may depend on certification, national-rail access, customer integration and proven risk performance. Each dependency should be tested for transferability after a change of control.

29. TEST CUSTOMER CONCENTRATION AND PORTABILITY

An anchor institution can create initial volume and shape the product. It can also dominate revenue, schemas, workflow and pricing. The acquirer should know whether the platform is a network or a customised service for one customer.

Customer-level analysis should show revenue, accepted presentations, credentials, integrations, support cost, contract term, termination rights and data restrictions. Code and policy should be separated into reusable core and customer-specific components.

Portability can be tested by onboarding a second verifier to an existing credential with limited custom work. The elapsed time, cost, policy change and exception rate provide evidence of scalability.

30. EXAMINE CONTRACTS FOR HIDDEN CONTROL

Critical contracts include evidence-source access, biometric and document vendors, national identity rails, cloud, wallets, issuers, verifiers, auditors and insurers. Change-of-control provisions can determine whether the acquired network survives completion.

The diligence team should identify exclusivity, volume commitments, price resets, audit rights, data-use restrictions, subcontracting, localisation, security, liability, termination and transition. A contract may allow technical integration and prohibit use for another sector or jurisdiction.

Related-party and reseller arrangements should be traced to the end verifier. Reported transaction volume may pass through a partner that owns the customer relationship and can replace the platform.

31. PROTECT INTELLECTUAL PROPERTY AND FREEDOM TO OPERATE

The platform can combine proprietary policy engines, orchestration, user experience, fraud models and connectors with open standards and third-party libraries. The acquirer should identify which assets are owned, licensed or subject to reciprocal obligations.

Schema definitions, test suites, trust-list operations and workflow rules can carry material know-how. Their provenance and rights should be documented. Customer-funded developments may restrict reuse.

Freedom-to-operate work should cover patents, standards implementation, cryptographic libraries, biometric components and open-source licences. Compliance should include build artefacts, notices and dependency scanning, not only a policy statement.

32. PREPARE FOR POST-QUANTUM MIGRATION

Identity credentials can remain valid for years, and trust infrastructure can persist longer. The target should inventory signature algorithms, certificates, secure elements, libraries and hardware dependencies. It should know which components can be upgraded without reissuing every credential.

Post-quantum planning should focus on cryptographic agility, transition governance and data whose confidentiality or authenticity must endure. The paper does not assume a universal migration date. It recommends that the buyer quantify dependency and replacement effort.

Contracts with wallet, issuer and hardware providers should support algorithm change. Test environments should allow dual or staged operation. A roadmap without funded engineering and partner commitments remains a weak control.

33. STRUCTURE THE ACQUISITION CONSIDERATION

Upfront value should reflect proven contracted economics and transferable controls. Deferred consideration can be linked to accepted presentations, qualified reuse, gross contribution, certification renewal and customer diversification.

Earn-out definitions should exclude failed presentations, duplicate events, internal test traffic and volume that does not satisfy the agreed assurance policy. Revenue measures should address pass-through fees, related parties, credits, fraud loss and collection.

Regulatory milestones should be within the seller's influence and objectively evidenced. A broad approval milestone can create disputes when timing depends on an authority. Consideration can instead follow completed submissions, remediation and continued operation under agreed conditions.

34. USE WARRANTIES AND INDEMNITIES SELECTIVELY

Warranties should cover certification, audits, security incidents, data processing, key control, intellectual property, customer metrics and regulatory correspondence. They should be tied to disclosed evidence and materiality.

Specific indemnities can address known breaches, unresolved complaints, unauthorised data use, compromised credentials or historic regulatory exposure. Insurance can support some risks and rarely replaces operational remedy.

The buyer should retain rights to suspend an issuer, schema, wallet or verifier when evidence fails. Continuity and user redress may matter more than financial recovery after a systemic identity incident.

35. PLAN INTEGRATION WITHOUT BREAKING TRUST

Identity networks are sensitive to domain, key, certificate, policy, support and privacy changes. A rapid technical merger can invalidate integrations or confuse users and relying parties. Integration should preserve trust anchors and evidence.

The first phase should stabilise governance, incident response, regulator contact, trust lists, keys and customer service. Branding, infrastructure and account consolidation should follow controlled migration and communication.

The buyer should maintain a credential-continuity register showing which credentials remain valid, which require reissuance, how holders are notified and how verifiers migrate. Success should be measured through uninterrupted accepted workflows.

36. BUILD THE FIRST 100-DAY PLAN

The first 100 days should confirm the trust graph, key inventory, certification scope, material contracts, regulatory obligations and metric definitions. The board should approve issuer onboarding, schema governance, incident and redress authorities.

Commercial work should validate the acceptance funnel and reconcile billing with verifier logs. Product work should identify the highest-value reusable workflows and retire unsupported claims. Security work should test key compromise, wallet recovery and status outage.

The plan should assign an owner, evidence and due date to every material issue. Deferred consideration and integration decisions should use the same metrics established during diligence.

37. CREATE THE BOARD DASHBOARD

The dashboard should track accepted presentations, qualified reuse, active verifiers, active issuers, status freshness, fraud loss, exception rate, redress time, availability, certification and contribution. It should show concentration and cohort trends.

Definitions should be fixed and independently reproducible. Each metric should trace to logs, billing, customer acceptance and finance. Management forecasts should be presented separately from observed results.

Risk indicators should include compromised keys, revoked credentials, unresolved critical findings, stale schemas, untested recovery paths and contracts approaching termination. The board needs decision thresholds and named owners.

38. ESTABLISH THE DILIGENCE WORKPLAN

The team should include identity architecture, cybersecurity, privacy, regulation, financial crime, commercial, finance, tax, accounting, intellectual property and human-capital specialists. Workstreams should use one trust graph and issue register.

Technical work should reproduce issuance, presentation, status and recovery. Regulatory work should confirm the accepted use cases and provider status. Commercial work should reconcile cohort activity with contracts and revenue. Finance should rebuild contribution by workflow.

Priority deal-breakers include unavailable source authority, invalid certification, non-transferable national-rail access, compromised key control, unlawful data use, unallocated systemic liability and customer economics dependent on rejected transactions.

39. PREPARE THE DATA ROOM

The data room should include governance, certifications, audit reports, regulator correspondence, architecture, protocols, schemas, assurance mappings, key inventories, status design, incident records, complaints, contracts, customer cohorts, billing and cost allocations.

Samples should link the full chain from evidence through accepted workflow. The buyer should be able to select a transaction and reconstruct proofing, issuance, consent, presentation, status, policy decision, customer acceptance and billing.

Documents should be current, attributable and versioned. Dashboards should be supported by source records. Missing evidence should remain an open issue rather than being replaced with a narrative assertion.

40. APPLY A GO, REPRICE OR STOP DECISION

A go decision requires lawful acceptance, transferable trust relationships, secure lifecycle operations, reproducible metrics and economics linked to accepted workflows. A reprice decision

is appropriate when remediation, concentration or adoption uncertainty can be quantified and protected.

A stop decision is appropriate when the target cannot evidence authority, control keys, lawfully process data, preserve regulated acceptance or contain systemic liability. The strategic attractiveness of digital identity should increase the evidence threshold.

The investment committee should record facts, scenario assumptions, unresolved matters, mitigations and owners. It should state which value depends on future adoption and how consideration is protected.

Table 4. Board and acquisition scorecard

Domain	Minimum evidence	Red flag	Decision response
Legal acceptance	Current certification, trust-list status and use-case mapping	Generic compliance claim without workflow authority	Condition or stop
Assurance	Reproducible proofing and authentication mapping	Strong login masking weak enrolment	Reprice and remediate
Interoperability	Versioned profile and multi-party production tests	Proprietary extension blocks alternative wallet or verifier	Defer value
Lifecycle	Key, status, refresh, recovery and redress evidence	Stale credentials remain accepted	Cure before scale
Commercial	Accepted presentations, qualified reuse and customer cohorts	Registrations presented as network usage	Rebuild valuation
Liability	Event-by-event allocation, caps, insurance and reserves	Systemic loss falls into a contractual gap	Restructure
Security	Tested compromise and recovery controls	Key custody or trust list cannot be recovered	Stop or isolate
Transferability	Change-of-control consents and portable customer integrations	National rail or anchor contract terminates	Condition precedent

Minimum evidence should be agreed before signing and monitored after completion.

41. RECOGNISE LIMITATIONS

This framework supports transaction and operating analysis. It does not determine whether a digital identity service is lawful, secure, accurate, inclusive or suitable for a particular regulated workflow. Qualified legal, regulatory, cybersecurity, privacy, financial-crime, technical, tax, accounting and valuation advice is required.

Standards and national frameworks continue to evolve. Certification scope, trust-list status and sector acceptance should be checked at the transaction date. A credential accepted in one workflow or jurisdiction should not be assumed acceptable elsewhere.

The hypothetical case demonstrates a method. Actual volume, price, cost, fraud, reuse, liability and valuation require company-specific evidence. No figure in the case is a forecast, valuation opinion or recommendation.

42. CONCLUDE WITH PORTABLE EVIDENCE AND LOCAL ACCOUNTABILITY

Reusable digital identity can reduce repeated proofing, improve privacy and accelerate regulated services. Its value depends on accepted evidence, visible assurance, current status, lawful purpose and clear responsibility.

The disciplined sequence is to begin with the regulated decision, map the trust graph, test assurance and interoperability, allocate liability, measure accepted reuse, rebuild contribution economics and stage consideration against verified outcomes. Post-completion integration should preserve keys, trust lists, certification and user redress.

Identity travels when technical standards and local accountability meet. A buyer should pay for workflows that accept the credential and continue to do so under controlled lifecycle operations. Everything else remains adoption potential until evidence converts it into trusted transactions.

REFERENCES

[1] National Institute of Standards and Technology. NIST SP 800-63-4: Digital Identity Guidelines. August 2025. https://doi.org/10.6028/NIST.SP.800-63-4

[2] National Institute of Standards and Technology. Digital Identity Guidelines, Revision 4. 2025. https://pages.nist.gov/800-63-4/

[3] World Wide Web Consortium. Verifiable Credentials Data Model v2.0. W3C Recommendation, 15 May 2025. https://www.w3.org/TR/vc-data-model-2.0/

[4] World Wide Web Consortium. Verifiable Credentials Data Model publication history. https://www.w3.org/standards/history/vc-data-model-2.0/

[5] OpenID Foundation. OpenID for Verifiable Credential Issuance 1.0. Final Specification, 16 September 2025. https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-final.html

[6] OpenID Foundation. OpenID for Verifiable Credential Issuance 1.0 Final Specification Approved. 16 September 2025. https://openid.net/openid-for-verifiable-credential-issuance-1-final-specification-approved/

[7] European Parliament and Council. Regulation (EU) 2024/1183 establishing the European Digital Identity Framework. 11 April 2024. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

[8] European Commission. European Digital Identity Wallet Architecture and Reference Framework. https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

[9] European Commission. EU Digital Identity Wallet Pilot Implementation. https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation

[10] European Commission. Questions and Answers on Digital Identity. https://digital-strategy.ec.europa.eu/en/faqs/qa-digital-identity

[11] European Commission. Implementing Regulation (EU) 2024/2977 on person identification data and electronic attestations of attributes. https://eur-lex.europa.eu/eli/reg_impl/2024/2977/oj

[12] European Commission. Implementing Regulation (EU) 2024/2982 on protocols and interfaces for the European Digital Identity Framework. https://eur-lex.europa.eu/eli/reg_impl/2024/2982/oj

[13] UK Government, Office for Digital Identities and Attributes. UK Digital Verification Services Trust Framework. 9 June 2026. https://www.gov.uk/government/collections/uk-digital-verification-services-trust-framework

[14] UK Government. UK Digital Identity and Attributes Trust Framework 0.4. Updated 9 June 2026. https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-04

[15] UK Government. Certification Scheme for the UK Digital Verification Services Trust Framework. Updated 21 September 2026. https://www.gov.uk/guidance/certification-scheme-for-the-uk-digital-identity-and-attributes-trust-framework

[16] UK Government, Office for Digital Identities and Attributes. Annual Report on Part 2 of the Data (Use and Access) Act 2025. 2026. https://www.gov.uk/government/publications/office-for-digital-identities-and-attributes-2026-annual-report/ofdia-2026-annual-report-on-the-operation-of-part-2-of-data-use-and-access-act-2025

[17] Central Bank of the United Arab Emirates. Guidance for Licensed Financial Institutions on Digital Identification for Customer Due Diligence. In force from 31 October 2022. https://rulebook.centralbank.ae/en/rulebook/guidance-licensed-financial-institutions-digital-identification-customer-due-diligence

[18] Central Bank of the United Arab Emirates. Guidance for Licensed Financial Institutions on Customer Due Diligence, Know Your Customer and Record-Keeping. 2025. https://rulebook.centralbank.ae/en/rulebook/guidance-licensed-financial-institutions-customer-due-diligenceknow-your-customer-and

[19] United Arab Emirates Government. The UAE Pass. https://u.ae/en/about-the-uae/digital-uae/digital-transformation/platforms-and-apps/the-uae-pass-app

[20] Saudi Data and AI Authority. Access to Government and Private Services through Nafath. https://sdaia.gov.sa/en/Services/Pages/ServiceDetails.aspx?ServiceID=1

[21] National Information Center, Saudi Arabia. Saudi National Digital Identity Management. https://www.iam.gov.sa/about.html

[22] Digital Government Authority, Saudi Arabia. Digital Government Policies, Version 2.0. 2024. https://dga.gov.sa/sites/default/files/2024-03/Digital%20Government%20Policies%20-%20V2.0.pdf

[23] Financial Action Task Force. Guidance on Digital Identity. 2020. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf.coredownload.pdf

ABOUT THE AUTHOR

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds — bridging the boardroom view to hands-on execution and close.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners he is Managing Partner, leading the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.

https://www.linkedin.com/in/ckadya/

https://www.matchpoint-partners.com/team/ck-adya.html

This paper is part of a continuing series on the structure of private and alternative markets. The views expressed are the author's own. The paper is for information only, describes market structure in general terms, and does not constitute investment, legal, tax or regulatory advice or a recommendation in respect of any security, vehicle or counterparty.