Trust across Borders: GCC Digital-Identity JVs and Interoperability

A transaction framework for governing trust, liability and commercial scale across national identity systems

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Gulf digital-identity systems increasingly support authentication, signatures, government access and private-sector transactions. The next commercial question is how separate national systems can recognise trustworthy credentials and services across borders without surrendering sovereign control, weakening privacy or creating an uninsurable chain of liability. An acquisition, joint venture or strategic alliance can create scale, but only when the transaction architecture distinguishes identity proofing, authentication, credential issuance, presentation, trust services and relying-party decisions.

This paper develops a Cross-Border Digital Trust Transaction Framework for boards, investors, public authorities and corporate acquirers. It begins with the user journeys and transaction decisions that generate value. It then maps issuers, wallets, trust-service providers, verifiers, national authorities, data stores and liability owners. The framework connects assurance equivalence, technical interoperability, data minimisation, transfer rules, service levels and economics to governance rights, reserved matters, closing conditions and post-closing integration.

Primary sources show that interoperability is a governance problem as well as a protocol problem. UAE Pass is the United Arab Emirates' unified national digital identity for citizens, residents and visitors, while the UAE trust-services regime licenses providers of electronic signatures, seals, timestamps, electronic delivery and website authentication. Saudi Arabia's Nafath provides national authentication. Bahrain's eKey 2.0 combines passwordless biometric access, user control over shared data and public-private service access. Qatar's Tawtheeq and national public-key infrastructure support authentication and digital signatures, while Oman operates national electronic authentication and public-key infrastructure. International standards have also matured: W3C Verifiable Credentials Data Model 2.0 became a Recommendation in 2025; OpenID for Verifiable Presentations 1.0 and OpenID for Verifiable Credential Issuance 1.0 became final specifications in 2025; and NIST's Digital Identity Guidelines Revision 4 separate identity, authentication and federation assurance.

A wholly hypothetical regional joint venture applies the framework. Three national platforms retain their domestic identity records and roots of trust. A jointly governed trust gateway publishes assurance mappings, accredits relying parties, routes credential requests and records service evidence. The illustrative model assumes 74 million annual eligible journeys, 38 percent activation by year three, a USD 1.15 blended transaction fee and USD 18.8 million of steady-state operating cost. Every company, amount, rate and operating assumption in the case is illustrative management input. It is not observed market data, a valuation opinion, a financing proposal or a forecast.

The central conclusion is that cross-border identity value does not require a regional identity database. It requires enforceable recognition of specified credentials, comparable assurance, constrained data disclosure, reliable revocation, accountable decisions and durable commercial access. Transaction value should follow verified relying-party adoption, successful credential flows and trusted transaction contribution. Boards should reserve for gaps in assurance, licensing, data transfer, cybersecurity, service continuity and change-of-control rights, then connect deferred consideration to evidence that survives expansion across jurisdictions.

JEL Classification: G34, K24, L86, O32, O33

Keywords: digital identity, GCC, interoperability, joint ventures, verifiable credentials, trust services, data sovereignty, identity assurance, M&A, platform economics

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 TRANSACTION DECISION

The transaction decision is whether an acquisition, joint venture or strategic alliance can make trustworthy digital credentials usable across Gulf borders while each state retains authority over its national identity system. The answer depends on specified user journeys, legal recognition, assurance, technical compatibility, operational accountability and commercial demand.

A board should begin with the transactions to be enabled. Examples include opening a regulated account, forming a company, signing a commercial document, accessing a government service, onboarding a worker, verifying a professional licence or proving age or residency. Each journey requires a different set of attributes, evidence, assurance and reliance rules.

The transaction perimeter should therefore be expressed as credential-purpose pairs. A system may recognise a residency credential for travel or service access without recognising it for credit underwriting. It may accept authentication at one assurance level while requiring a qualified signature for a binding instrument. Value follows the journeys that the venture can lawfully complete, not the number of identity records connected.

Table 1. Digital-trust value layers and transaction evidence

Value layer	Minimum evidence	Principal exposure	Transaction response
National authority	Issuer mandate, legal basis and trust anchor	Recognition can be withdrawn or narrowed	Closing condition and reserved matter
Assurance	Proofing, authentication and federation profile	Same label can conceal different confidence	Assurance mapping and step-up control
Credential	Schema, issuer, status, validity and purpose	Credential is authentic but unsuitable	Purpose-specific acceptance policy
Interoperability	Tested issuance, presentation and wallet flows	Protocol support does not equal compatibility	Conformance and bilateral testing
Data rights	Purpose, disclosure, transfer and retention basis	Unlawful or excessive cross-border processing	Data minimisation and localisation design
Relying-party access	Accreditation, contract and transaction demand	Network has no commercial adoption	Milestone-based value allocation
Operations	Service levels, revocation, incidents and continuity	Trust decision fails or cannot be evidenced	Joint operating model and audit rights
Economics	Verified journeys, price and contribution	Registered users are mistaken for revenue	Underwrite completed trusted transactions

Each layer requires a defined owner, verifiable evidence and a transaction response.

2. SEPARATE NATIONAL IDENTITY FROM CROSS-BORDER RECOGNITION

A national digital identity system establishes trust under domestic law and governance. Cross-border recognition asks whether another jurisdiction or private relying party will accept a particular credential or authentication result for a defined purpose. The two functions should remain separate in transaction design.

The venture does not need a consolidated regional population register. It can use a federation or credential-exchange model in which domestic authorities retain source records and issue signed assertions or credentials. The receiving party verifies authenticity, status, assurance and policy without obtaining unrestricted access to the source database.

This separation reduces sovereignty and concentration concerns. It also clarifies valuation. The venture owns or controls the interoperability layer, accreditation process, commercial network and operating evidence. National authorities retain their identity mandates, data and root-of-trust powers. The purchase agreement or shareholders' agreement should state that distinction explicitly.

3. MAP THE GCC IDENTITY LANDSCAPE

The Gulf already contains mature national building blocks. UAE Pass is the United Arab Emirates' approved unified digital identity for citizens, residents and visitors and supports online access and digital signatures. Saudi Arabia's Nafath supports authentication for government and private services. Bahrain's eKey 2.0 provides passwordless biometric access and gives users control over information shared with service providers.

Qatar's Tawtheeq provides unified authentication, multilayer verification and digital-signature capability. Qatar also operates national public-key infrastructure with root and issuing authorities, online certificate-status services and timestamp capability. Oman's national electronic authentication service uses civil identity and mobile credentials and supports legally recognised digital signatures.

These systems differ in mandate, assurance, credential form, private-sector access, resident and visitor scope, trust-service structure and integration method. A regional transaction must respect those differences. Interoperability should be based on an agreed profile and policy mapping, not a claim that the systems are identical.

4. IDENTIFY THE TRUST DOMAINS

A trust domain is a community whose members accept defined issuers, credentials, assurance rules and liabilities. National digital identities operate within domestic trust domains. Banks, telecom operators, health systems, professional bodies and commercial platforms can form additional domains.

The venture should list each domain and define its admission rules. It should identify who may issue, hold, present, verify and rely on each credential. It should also specify whether recognition is automatic, conditional or subject to step-up checks.

Trust domains can overlap. A bank may accept a government-issued identity credential, a regulator-issued professional credential and a company-issued employment credential in one

onboarding journey. The interoperability layer must preserve the authority and policy attached to each claim. Combining signed data from several issuers does not create a new sovereign identity.

5. DISTINGUISH IDENTITY, CREDENTIALS AND TRUST SERVICES

Identity proofing establishes that a person or organisation is who it claims to be. Authentication confirms control of an authenticator. A credential expresses claims made by an issuer. A trust service can provide electronic signatures, seals, timestamps, certified delivery or website authentication. These are related but distinct assets.

The UAE's Federal Decree-Law No. 46 of 2021 and its implementing framework distinguish digital identity from regulated trust services. TDRA states that providers of trust services and qualified trust services require licensing before offering covered services in the UAE. A transaction involving a wallet or identity platform must therefore test whether it also provides a regulated trust service.

The distinction changes deal structure. A technology asset can transfer through an acquisition while a regulatory licence, qualified status or trusted-list entry may require approval or may remain entity-specific. The buyer should map every revenue line to the legal capacity needed to deliver it after closing.

6. BUILD THE CROSS-BORDER TRUST GRAPH

The trust graph links national identity authorities, credential issuers, wallets, trust-service providers, the interoperability gateway, relying parties and users. It also connects assurance policies, keys, status services, data flows, contracts and liability.

The graph should show which party creates each claim, which party holds it, which party verifies it and which party makes the final decision. A verifier may confirm that a credential is authentic and current, yet the relying party remains responsible for deciding whether the claim satisfies its business and regulatory rules.

This distinction prevents misplaced reliance. The venture can warrant protocol performance and evidence integrity without guaranteeing every downstream decision. Its contracts should allocate responsibility for issuer accuracy, wallet security, gateway routing, verifier policy and relying-party use.

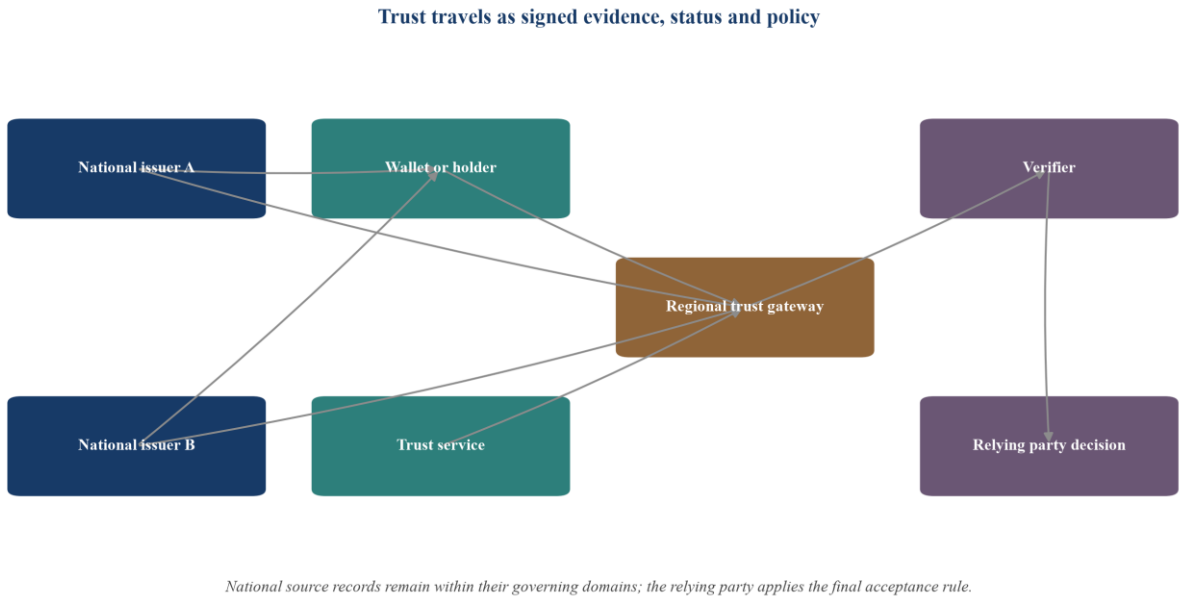

Figure 1. Cross-border digital-trust graph

The regional layer routes verifiable evidence while national authorities retain source records and roots of trust.

7. CHOOSE THE INTEROPERABILITY MODEL

Three broad models are available. A federation model passes authentication assertions between trusted parties. A verifiable-credential model allows an issuer to provide a signed credential that a holder presents to a verifier. A gateway model translates protocols and policy between existing systems.

The models can coexist. Federation suits real-time access where the identity provider remains online. Verifiable credentials can support selective disclosure and holder-mediated presentation. A gateway can preserve legacy integrations while a common credential profile develops.

The transaction should choose a model for each journey. A single architecture imposed across all states can create unnecessary replacement cost and political resistance. A layered model can leave national platforms intact, introduce common profiles and require conformance at the regional boundary.

8. USE MATURE TECHNICAL STANDARDS

Technical maturity has improved. W3C Verifiable Credentials Data Model 2.0 became a Recommendation in May 2025. It defines an issuer-holder-verifier model, credential status, schemas and privacy considerations. OpenID for Verifiable Presentations 1.0 became final in July 2025 and supports presentations of W3C credentials, ISO mobile documents and selective-disclosure credentials. OpenID for Verifiable Credential Issuance 1.0 became final in September 2025.

Standards reduce proprietary lock-in and integration cost. They do not establish legal recognition, issuer authority or liability. The venture should adopt a constrained profile that specifies credential formats, algorithms, key handling, status method, transport, wallet attestation, error handling and conformance tests.

Profile governance matters because standards evolve. Version changes should require technical review, compatibility testing and controlled migration. A reserved matter should govern changes that alter national interfaces, assurance or reliance.

9. DEFINE ASSURANCE EQUIVALENCE

NIST Revision 4 separates identity assurance, authentication assurance and federation assurance. This is useful for regional design because two systems can provide similar authentication while using different proofing or federation controls.

The venture should create an assurance-equivalence matrix. It should compare enrolment evidence, identity resolution, biometric or in-person checks, authenticator strength, phishing resistance, session controls, assertion protection, attribute release and recovery. Equivalent labels should only be assigned where the underlying controls and outcomes support them.

When equivalence is incomplete, the system should step up. A relying party may request an additional factor, a fresh presentation, a qualified signature, a source check or manual evidence. Step-up rules preserve access while preventing weak equivalence from becoming a region-wide vulnerability.

10. PRESERVE PURPOSE-SPECIFIC ACCEPTANCE

Authenticity does not establish suitability. W3C's credential model explains that a verifier evaluates the issuer, proof, subject and claims against its own policies before relying on them. A valid residency credential may support service eligibility but may not establish beneficial ownership or professional authority.

The venture should publish acceptance policies by journey. Each policy should list permitted issuers, credential types, required claims, assurance, freshness, status checks, disclosure limits and exception paths. Relying parties should be able to apply stricter rules where their regulation requires them.

Purpose-specific acceptance also constrains commercial promises. Sales materials should state which journeys are accredited and tested. Broad claims of GCC-wide identity acceptance can create liability when recognition is limited to selected credentials and relying parties.

11. APPLY SELECTIVE DISCLOSURE AND DATA MINIMISATION

Cross-border identity should disclose the minimum information needed for the transaction. A service may need confirmation that a user is over a threshold age, holds a valid residency status or controls a registered company. It may not need the full underlying identity record.

Verifiable credentials and selective-disclosure formats can support claim-level presentation. The policy layer still needs to prevent unnecessary requests, correlation and retention. W3C warns that persistent, machine-readable credentials can increase privacy risk when disparate data is collected and linked.

The venture should maintain a disclosure catalogue. Each journey should specify mandatory and optional claims, purpose, retention and onward use. The gateway should reject requests outside the accredited policy and record evidence without storing the full credential unless required.

12. DESIGN CONSENT AND USER CONTROL

Consent may support some disclosures, but it should not be treated as a universal basis for all identity processing. The legal basis depends on the purpose, party and jurisdiction. User control remains an important design property even where processing rests on law, contract or regulatory obligation.

Bahrain's eKey 2.0 is described by the Information & eGovernment Authority as giving users control over information shared with service providers. The venture can build on that pattern through clear request screens, claim-level disclosure, receipts and withdrawal or revocation paths where applicable.

Consent evidence should record the requesting party, purpose, claims, time, policy version and result. Dark patterns, bundled permissions and indefinite reuse can undermine trust and increase remediation cost. The transaction model should fund user-experience and accessibility work as core infrastructure.

13. ALLOCATE CONTROLLER AND PROCESSOR ROLES

The shareholders' agreement and data-processing contracts should reflect operational reality. An issuer may control source identity records. A wallet provider may control user-held data and telemetry. The gateway may process routing evidence and determine some security purposes. A relying party controls its final decision and downstream use.

Joint control can arise where parties jointly determine purpose and essential means. Labels alone do not settle the question. The diligence team should map decisions, data access, retention, analytics and incident response for every material flow.

Role allocation affects notices, rights requests, breach notification, security, transfer mechanisms and regulatory engagement. A regional venture should maintain a responsibility matrix that can be updated as journeys and jurisdictions expand.

14. GOVERN CROSS-BORDER DATA TRANSFERS

Digital identity interoperability can create transfers even when source records remain domestic. Personal data may be disclosed to a foreign relying party, accessed by regional support staff, logged in a shared security platform or processed by a cloud provider.

Saudi Arabia's transfer regulation sets conditions for transfers outside the Kingdom and provides mechanisms including binding common rules and standard contractual clauses. Other Gulf jurisdictions apply their own requirements. The venture should identify every transfer, remote access path and onward processor.

A localisation statement is not enough. The design should show which data remain domestic, which claims cross borders, which metadata are generated, where keys and logs reside and how deletion occurs. Transfer impact and security assessments should be closing deliverables for priority journeys.

15. USE NATIONAL TRUST ANCHORS WITHOUT CENTRALISING KEYS

Public-key infrastructure supports signatures, seals, timestamps and certificate status. The UAE Trusted List is the authoritative source for licensed trust-service providers and services. Qatar and Oman also operate national public-key infrastructures.

The venture should avoid becoming a single regional root unless participating authorities explicitly mandate that model. A bridge or trust-list approach can recognise approved national anchors while preserving domestic key governance. The regional layer can distribute signed metadata, status and policy.

Key compromise, algorithm transition and provider suspension require joint procedures. The agreement should specify who can suspend recognition, how quickly participants must propagate status, how affected transactions are treated and how evidence is preserved.

16. MAKE REVOCATION A REAL-TIME OPERATING CAPABILITY

A credential can be authentic but no longer valid. Residency, employment, licence, authority and device status can change. The verifier must check freshness and status using the method required by the credential profile.

Revocation design should consider privacy. A status check that contacts the issuer for every presentation can reveal where and when a person transacts. Status lists or privacy-preserving methods can reduce that disclosure, subject to freshness and scale requirements.

The venture should define propagation targets, cache rules, offline handling and dispute procedures. Service-level measurement should include stale-status exposure and time to suspend a compromised issuer, wallet or verifier.

17. ACCREDIT RELYING PARTIES

The commercial network is only as trustworthy as its verifiers and relying parties. Accreditation should test identity, regulatory standing, purpose, security, data handling, disclosure requests, user redress and contract capacity.

A relying party should receive credentials only for approved journeys. Its client software and redirect endpoints should be registered. High-risk sectors may require independent assessment, penetration testing or regulator approval.

Accreditation also creates a saleable asset. The venture can provide one controlled route to trusted identity services across participating systems. The board should measure active accredited relying parties and completed journeys, not signed memoranda or sandbox accounts.

18. TEST INTEROPERABILITY THROUGH CONFORMANCE

Protocol support on a product sheet does not establish interoperability. OpenID Foundation conformance and interoperability work demonstrates the value of testing independent issuers, wallets and verifiers against a common profile.

The venture should operate a reference environment and test suite. It should cover positive flows, malformed requests, expired and revoked credentials, unsupported algorithms, replay, wallet switching, cross-device journeys, offline cases and recovery.

Conformance results should be versioned and linked to production releases. A participant that changes its implementation should requalify where material. The transaction agreement should give the venture audit and suspension rights when a participant falls outside the approved profile.

19. BUILD A CREDENTIAL GRAPH, NOT A DATA LAKE

The credential graph describes issuers, credential types, schemas, status methods, assurance, permitted purposes and relying-party relationships. It need not contain the underlying personal claims.

This architecture creates a commercially useful map of trust while limiting data concentration. The venture can discover which credentials satisfy a journey, route requests and verify policy without building a regional identity database.

The graph should be governed like critical infrastructure. Schema changes, issuer admission, purpose expansion and trust removal affect many parties. Each change should be signed, versioned, tested and capable of rollback.

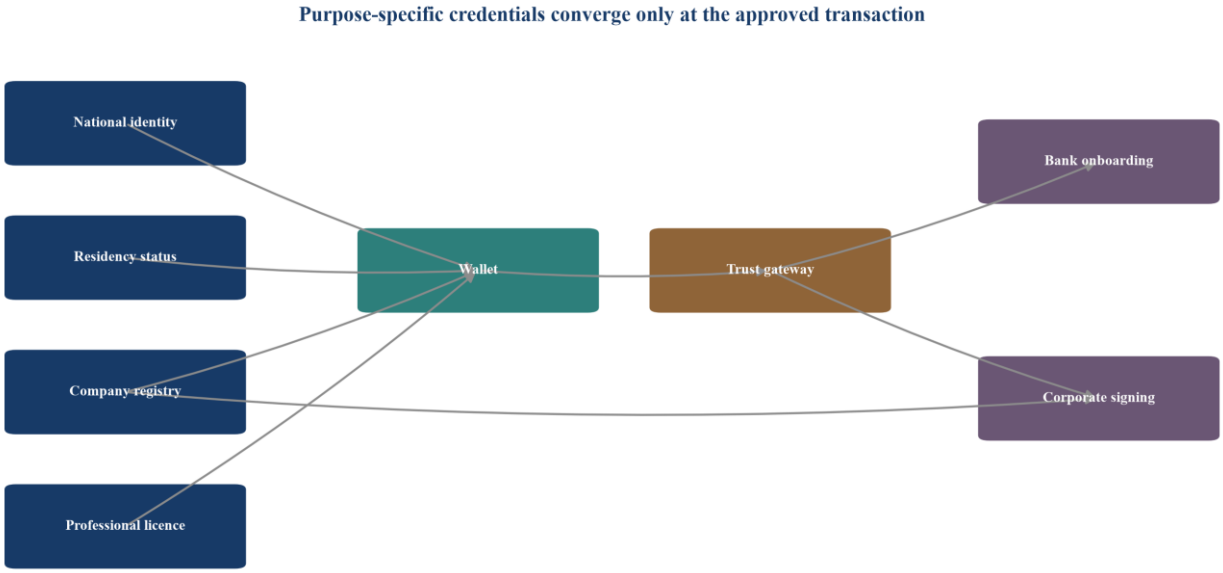

Figure 2. Credential graph for a cross-border commercial journey

A relying party assembles purpose-limited evidence from authoritative issuers without obtaining unrestricted source records.

20. DEFINE SERVICE LEVELS AROUND TRUST OUTCOMES

Availability alone is an incomplete service level. The venture should measure successful issuance, presentation and verification; latency; status freshness; exception rate; false rejection; step-up completion; incident containment; and evidence delivery.

National participants may have different operating windows and change processes. A cross-border journey should state the dependencies that determine its end-to-end commitment. Planned maintenance and emergency suspension require coordinated communication.

Service credits can compensate relying parties for outages, but they do not address invalid trust decisions. Contracts should include incident investigation, evidence preservation, corrective action and liability allocation for integrity failures.

21. DESIGN FRAUD CONTROLS ACROSS THE CHAIN

Fraud can enter during identity proofing, authenticator recovery, wallet activation, credential issuance, presentation, verifier registration or relying-party decision. A secure protocol cannot compensate for fraudulent source enrolment.

The venture should maintain a shared threat model and minimum controls. Signals can include device integrity, impossible travel, repeated recovery, credential replay, verifier anomalies and unusual disclosure requests. Data sharing should remain lawful and purpose-limited.

Fraud decisions need appeal and correction. A regional blocklist without due process can propagate error across many services. Governance should separate urgent suspension from permanent exclusion and require review, evidence and restoration paths.

22. ALLOCATE LIABILITY BY CONTROLLABLE FAILURE

Liability should follow the party that controls the failed function. An issuer controls claim accuracy and issuance authority. A wallet provider controls secure storage and presentation. The gateway controls routing, policy enforcement and evidence. The verifier controls validation. The relying party controls the final business decision.

Caps, exclusions and indemnities should reflect the consequence of each failure. A low-value service login and a high-value corporate signature should not share one undifferentiated risk allocation. Insurance availability should be tested early.

The venture should keep transaction evidence sufficient to identify the failed layer. Without signed logs, policy versions and time evidence, disputes can become joint allegations rather than attributable events.

23. CREATE A CROSS-BORDER DISPUTE MECHANISM

Disputes may involve a user, issuer, wallet, verifier and relying party in several jurisdictions. The operating model should provide one intake route, then route responsibility without forcing the user to understand the technical chain.

The agreement should distinguish credential accuracy, authentication, signature validity, service delivery and downstream commercial disputes. It should specify governing law and forum for participant contracts while respecting mandatory local rights.

Evidence access is central. Parties need a defined procedure to preserve and disclose relevant signed records without revealing unrelated credentials or personal data. Time limits should match transaction consequence and regulatory obligations.

24. TREAT CYBERSECURITY AS COMMON INFRASTRUCTURE RISK

The interoperability layer can become a high-value target. Compromise could enable credential substitution, verifier impersonation, policy manipulation or widespread denial of service. The venture should apply defence in depth, hardware-backed keys, privileged-access controls, segregation, independent monitoring and tested recovery.

National systems should retain the ability to suspend the regional connection without disabling domestic services. The gateway should fail safely when issuer status, policy or key information is unavailable.

Cyber diligence should inspect architecture, secure development, software supply chain, key ceremonies, penetration tests, incidents and recovery exercises. Remediation cost belongs in the transaction model, and material gaps should be closing conditions.

25. PLAN CRYPTOGRAPHIC AGILITY

Identity infrastructure can outlive current cryptographic algorithms. The venture should inventory algorithms, key lengths, hardware, certificates, libraries and external dependencies. It should design for migration without invalidating historic evidence.

Post-quantum transition is relevant to long-lived credentials, signatures and archives. The board should fund discovery, hybrid testing and standards monitoring. It should avoid unverified claims of quantum readiness.

Reserved matters should cover removal or addition of algorithms, trust anchors and credential formats. Migration plans should include participant testing, dual operation, evidence preservation and clear deprecation dates.

26. COMPARE TRANSACTION STRUCTURES

An acquisition provides control but can trigger licence, assignment and sovereignty concerns. A contractual alliance preserves ownership but can leave weak incentives and fragmented accountability. A joint venture can create shared governance and a dedicated operating company, subject to deadlock and capital-funding risk.

The suitable structure depends on the assets. If value sits in a private interoperability platform and customer network, acquisition may be feasible. If value depends on national recognition and regulated trust services, a joint venture or licensed alliance may preserve authority better.

Boards should separate ownership of technology, operating responsibility and recognition rights. A venture can license technology, employ the operating team and contract with national authorities without owning national identity data or sovereign trust anchors.

Table 2. Transaction-structure comparison

Structure	Control	Recognition durability	Principal weakness	Appropriate use
Acquisition	High over acquired platform	Depends on approvals and contracts	Licence or mandate may not transfer	Private platform with transferable rights
Joint venture	Shared through governance	Strong where authorities participate	Deadlock and funding complexity	Regional gateway with sovereign interfaces
Strategic alliance	Contractual	Dependent on termination terms	Limited integration authority	Early bilateral corridor
Managed service	Operational control by provider	Customer retains policy authority	Concentrated vendor dependency	Defined technology layer
Standards consortium	Collective profile governance	Broad participation	Weak execution and economics	Common specifications and conformance

The preferred structure depends on control requirements, regulatory transferability and sovereign participation.

27. DESIGN JOINT-VENTURE GOVERNANCE

Governance should protect trust and permit commercial execution. The board should include participating authorities or designated shareholders, independent technical and risk expertise, and management accountable for the operating company.

Reserved matters should cover admission of states and issuers, new credential purposes, assurance changes, trust-anchor changes, data-location changes, material outsourcing, pricing principles, cybersecurity exceptions, suspension and change of control.

Day-to-day product and sales decisions need delegated authority. A venture that requires unanimous approval for every relying party will not scale. Policy classes and risk thresholds can define what management may approve within the agreed framework.

28. PREVENT DEADLOCK FROM BECOMING AN OUTAGE

Deadlock mechanisms in ordinary joint ventures often assume time for negotiation or buy-sell resolution. Critical identity infrastructure needs continuity during disagreement.

The agreement should preserve the last approved policy and operating budget for a defined period. Emergency security actions should be available to a designated committee, with rapid review. A participant should be able to suspend its own recognition route without disabling the whole network.

Commercial disputes can use escalation, mediation or expert determination. Matters affecting sovereign mandate, legal compliance or national security may need separate procedures. The structure should identify non-transferable decisions at signing.

29. BUILD DURABLE ACCESS RIGHTS

The venture's value depends on continued access to national interfaces, keys, status services and credentials. Those rights should be documented with term, service level, permitted purpose, change process, termination and transition assistance.

Change of government policy, law, ownership or technology can alter access. The agreement should specify when a participant may suspend, when it must provide notice and how existing transactions and relying parties are handled.

Exclusivity should be used carefully. A national authority may need to support several wallets or gateways. The venture can protect investment through minimum commitments, interoperability obligations and non-discriminatory access rather than absolute exclusivity.

30. VALUE NETWORK EFFECTS CAUTIOUSLY

Digital identity networks can gain value as more issuers, wallets and relying parties participate. The effect is not automatic. Each additional node matters only if it adds demanded credentials, trusted journeys or transaction volume.

The model should measure active corridors and completed transactions. Registered users, integrated APIs and signed partners are leading indicators. They should not be treated as realised revenue without evidence of use.

Network effects can reverse. A security incident, policy dispute or major participant exit can reduce trust across the network. Concentration and common-mode risk should therefore reduce the valuation multiple or increase the reserve.

31. CHOOSE PRICING THAT SUPPORTS TRUST

Pricing can be per verification, per credential issuance, per relying party, per user, per signature, subscription or a hybrid. The price should reflect transaction value, risk, service obligations and adoption incentives.

A low-value government service may require public funding or marginal-cost pricing. A bank onboarding or corporate signature can support higher commercial pricing. Cross-subsidy should be transparent to shareholders and public participants.

The venture should avoid incentives for excessive data requests. Pricing by claim count can encourage unnecessary disclosure. A journey-based fee with approved claim bundles better aligns privacy and commerce.

32. MODEL UNIT ECONOMICS BY COMPLETED JOURNEY

Revenue should be reconciled from eligible journeys to completed trusted outcomes. The funnel includes eligible users, wallet availability, consent or authority, credential presence, successful presentation, validation, step-up and relying-party completion.

Variable cost includes cloud and network use, status checks, fraud review, support, dispute handling, certification and revenue share. Fixed cost includes security, compliance, conformance, key management, product and governance.

The board should model economics by corridor and journey. A regional average can conceal an unprofitable high-support deployment or dependence on one bank, ministry or telecom operator.

33. APPLY A TRUST-ADJUSTED VALUATION BRIDGE

The valuation bridge begins with contribution from completed accredited journeys. It adds conditional value for contracted corridors that have passed legal and technical gates. It deducts remediation, participant concentration, regulatory uncertainty, transition cost and capital requirements.

Intangible assets may include software, credential schemas, conformance tools, accreditation processes, relying-party contracts and operating evidence. Source identity data and sovereign trust anchors may remain outside the transaction.

Deferred consideration can be tied to approved corridors, successful conformance, active relying parties and verified contribution. Milestones should exclude simple registrations or memoranda that do not create operational revenue.

Table 3. Trust-adjusted valuation bridge

Item	Illustrative amount	Underwriting treatment
Steady-state trusted-transaction contribution	13.6	Base economics after direct operating cost
Contracted expansion contribution	4.2	Probability-weighted after approvals and testing
Platform and conformance capability	6.0	Replacement-cost and strategic assessment
Remediation and certification reserve	(5.4)	Deduct for known assurance and security gaps
Participant concentration reserve	(3.1)	Deduct for common-mode withdrawal exposure
Transition and integration cost	(4.0)	Deduct funded first-year programme
Indicative trust-adjusted contribution base	11.3	Basis for negotiation, not a valuation opinion

All amounts are wholly hypothetical management assumptions in USD millions.

34. USE EARN-OUTS TIED TO EVIDENCE

An earn-out can bridge uncertainty around adoption and regulatory recognition. Measures should include completed paid journeys, active accredited relying parties, service-level performance, security compliance and contribution after agreed direct costs.

The formula should exclude volume created through below-cost pricing, unsupported disclosure or unapproved corridors. It should also address policy changes outside management control.

Evidence rights matter. Sellers or minority shareholders need access to the operating records used to calculate milestones. The venture should generate those records as part of normal trust operations rather than a separate financial exercise.

35. PROTECT AGAINST PARTICIPANT CONCENTRATION

A regional venture can appear diversified while depending on one national issuer, wallet platform, cloud provider or anchor relying party. The buyer should calculate revenue, credential and journey concentration.

Stress tests should remove each critical participant. The model should estimate affected volume, recovery time, alternative route and contractual remedy. Concentration that cannot be mitigated should affect price, governance and liquidity reserves.

Minimum commitments can support fixed infrastructure, but they should be enforceable and funded. Non-binding policy support should remain outside contracted value.

36. TEST INTELLECTUAL-PROPERTY OWNERSHIP

The diligence team should identify ownership and licences for gateway software, wallet components, credential schemas, conformance tools, cryptographic libraries, fraud models and documentation. Open-source obligations should be reviewed against deployment and distribution.

Participant-developed extensions can create fragmented ownership. The agreement should define background intellectual property, venture-developed intellectual property, improvements, licence-back rights and post-termination use.

Ownership of software does not grant authority to issue or recognise credentials. The asset schedule should distinguish technology rights from regulatory and contractual access rights.

37. PROTECT DATA AND TELEMETRY RIGHTS

Operational telemetry can improve fraud detection, capacity and user experience. It can also reveal sensitive patterns across jurisdictions. The venture should define which telemetry it may collect, for what purpose, at what granularity and for how long.

Aggregated statistics should be designed to resist re-identification. Product analytics should not silently become cross-purpose identity profiling. Machine-learning use should have a separate authority, governance and evidence path.

The shareholders' agreement should specify ownership and permitted use of aggregated operating data. Participants should retain access to evidence needed for their own oversight without receiving unrelated personal data.

38. CONTROL CHANGE OF CONTROL

National-interface agreements, licences and relying-party contracts should be reviewed for assignment, ownership restrictions, sanctions and public-interest approvals. A change of control can alter trust even when software and staff remain unchanged.

The transaction timetable should identify every consent and approval. Where approval cannot be obtained before signing, value should be conditional and the long-stop date realistic.

Post-closing ownership changes should also be governed. A strategic competitor, sanctioned person or unsuitable controller may be unacceptable to public participants. Transfer restrictions and call rights should be proportionate and clearly valued.

39. BUILD THE EVIDENCE ROOM

The evidence room should include legal mandates, licences, trust-list status, interface agreements, assurance policies, credential schemas, conformance reports, key-management procedures, service levels, incidents, penetration tests, transfer assessments, customer contracts and audited transaction data.

Evidence should be linked to a production version and corridor. Policy documents that do not match live configuration provide limited comfort. Management should demonstrate flows from request to signed evidence, status check and relying-party result.

The investment committee should receive a concise exception register with owner, consequence, remediation, cost, dependency and transaction treatment. Unsupported assertions should not be converted into value.

Table 4. Priority evidence-room requests

Workstream	Evidence request	Investment question
Legal authority	Mandates, licences, recognition and transfer basis	Can the journey continue after closing?
Assurance	Proofing, authentication and federation controls	Are claimed levels comparable?
Technology	Profiles, conformance, keys and status services	Does the production stack interoperate securely?
Privacy	Role maps, disclosures, transfers and retention	Is each data flow lawful and proportionate?
Operations	SLAs, incidents, disputes and continuity tests	Can trust be maintained under stress?
Commercial	Relying-party contracts and transaction cohorts	Which adoption converts to durable revenue?
Finance	Price, variable cost and contribution by journey	What economics are verified?
Transaction	Consents, reserved matters and transition plan	Which risks require price or conditions?

Evidence should be current, version-linked and attributable to the relevant corridor.

40. APPLY THE FRAMEWORK TO A HYPOTHETICAL GCC JOINT VENTURE

Consider a wholly hypothetical joint venture formed by three national-platform participants and a private interoperability operator. National identity records and roots of trust remain domestic. The venture operates a policy registry, conformance environment, relying-party accreditation service and credential-routing gateway.

The first journeys are bank onboarding, corporate-signing authority, professional-licence verification and resident service access. Each corridor launches only after legal recognition, assurance mapping, conformance and transfer review. A national participant can suspend its corridor through an emergency process.

The case assumes 74 million eligible annual journeys by year three. It assumes 38 percent activation, resulting in 28.1 million completed trusted journeys. The assumed blended fee is USD 1.15, producing USD 32.3 million of revenue. Assumed steady-state operating cost is USD 18.8 million, leaving USD 13.5 million of contribution before corporate overhead, tax, financing and capital expenditure. All figures are illustrative management assumptions.

41. RECONCILE THE ADOPTION FUNNEL

The illustrative adoption funnel prevents eligible population from being mistaken for revenue. The largest losses arise from relying-party readiness, wallet or credential availability, consent or authority, successful presentation and step-up completion.

Management should measure cohorts by corridor and use case. A successful bank onboarding may have different economics from a government login. Support, fraud and dispute cost should follow the same cohort.

The board should set milestones for completed journeys and contribution. User registrations and technical integrations remain operating indicators.

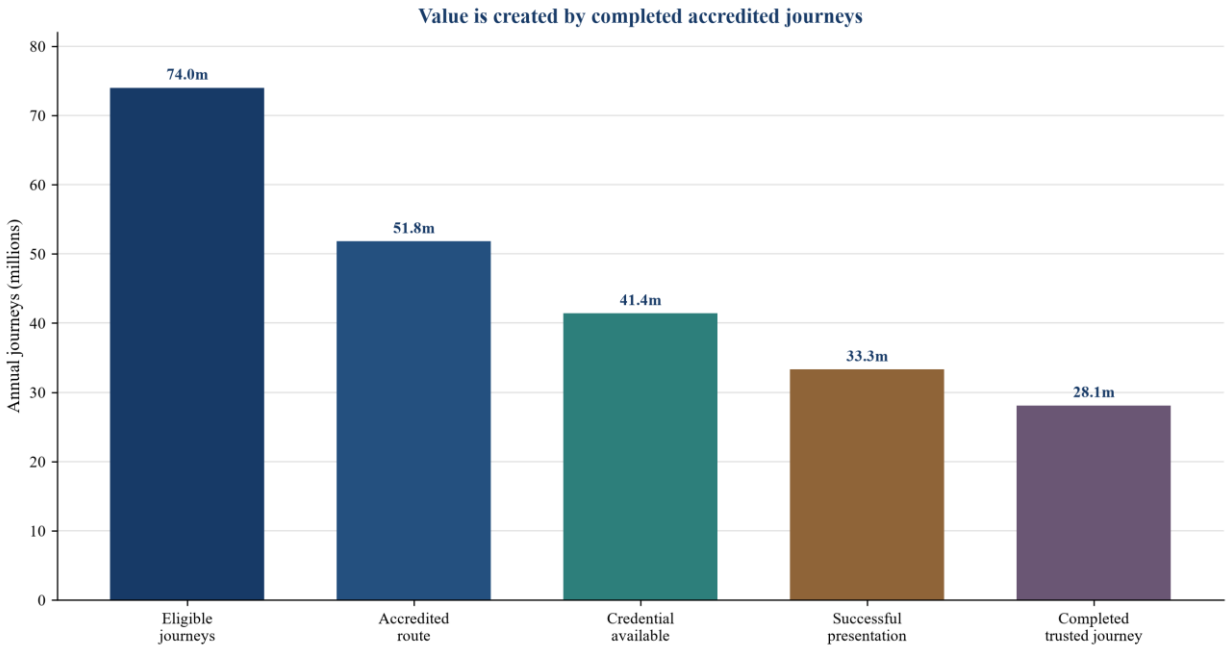

Figure 3. Illustrative cross-border trust adoption funnel

Volumes are wholly hypothetical management assumptions and do not represent observed market data.

42. BUILD THE FIRST-ONE-HUNDRED-DAYS PLAN

The first thirty days should confirm governance, trust anchors, participant interfaces, corridor owners, security authority and the exception register. The venture should freeze unapproved scope expansion and establish signed configuration baselines.

Days thirty-one to sixty should complete priority assurance mappings, data-flow reviews, credential profiles and conformance environments. Relying-party accreditation should begin with a limited set of journeys and named owners.

Days sixty-one to one hundred should run end-to-end pilots, incident and revocation exercises, dispute simulations and financial reconciliation. Commercial launch should follow evidence that the exact production versions meet the approved policy and service levels.

43. ESTABLISH THE BOARD SCORECARD

The board scorecard should combine trust, adoption and economics. Trust measures include active accredited issuers and verifiers, conformance status, revocation freshness, incidents, policy exceptions and unresolved disputes. Adoption measures include completed journeys, step-up rate, abandonment and active relying parties.

Economic measures include revenue and contribution per journey, support cost, fraud loss, concentration and committed expansion. Governance measures include overdue reserved matters, audit findings, regulatory actions and participant funding.

The scorecard should distinguish leading indicators from realised performance. Integrations, registered users and signed memoranda can support the pipeline. Completed paid journeys and collected revenue establish commercial results.

44. USE A DISCIPLINED INVESTMENT-COMMITTEE DECISION TREE

The committee should first ask whether the venture has documented authority for the proposed corridor. It should then ask whether assurance is mapped, interoperability is proven, disclosure is minimised, transfers are governed and liability is allocated.

If those gates pass, the committee can underwrite relying-party adoption and unit economics. If a gap is remediable, value can be deferred and funding reserved. If authority or transferability is absent, the related corridor should be excluded from current value.

The decision memo should state which value is verified, conditional or excluded. It should also identify every assumption that belongs to management rather than an independent source.

45. CONCLUSION

The Gulf has strong national digital-identity and trust-service foundations. Regional value can emerge when those foundations recognise specified credentials and assurance for defined commercial and public-service journeys.

The transaction architecture should preserve national identity records, roots of trust and legal mandates. The joint layer should govern profiles, accreditation, policy, evidence, service levels and economics. A common protocol helps, but durable value comes from recognised authority, reliable operations and active relying parties.

Boards should price completed accredited journeys and trusted transaction contribution. Conditional value should depend on approvals, conformance and adoption. Reserves should cover security, assurance, transfer, licensing and integration gaps. This approach turns cross-border digital identity from a broad policy ambition into an investable and governable operating system.

REFERENCES

[1] Federal Authority for Identity, Citizenship, Customs & Port Security. UAE Pass. https://icp.gov.ae/en/uae-pass/

[2] UAE Cabinet. Federal Decree-Law No. 46 of 2021 on Electronic Transactions and Trust Services. https://tdra.gov.ae/-/media/About/Trust-Services/Laws-and-regulations/Federal-Decree-Law-No-46-OF-2021-On-Electronic-Transactions-and-Trust-Services-EN.ashx

[3] Telecommunications and Digital Government Regulatory Authority. Trust Services FAQs. https://tdra.gov.ae/en/About/tdra-sectors/information-and-digital-government/departments/policy-and-programs-department/trust-services/faqs

[4] Telecommunications and Digital Government Regulatory Authority. UAE Trusted List. https://tdra.gov.ae/en/About/tdra-sectors/information-and-digital-government/departments/policy-and-programs-department/trust-services/uae-trusted-list

[5] Telecommunications and Digital Government Regulatory Authority. Information and Digital Government. https://tdra.gov.ae/en/About/tdra-sectors/information-and-digital-government

[6] Government of Dubai Media Office. UAE Pass results reported to the UAE Cabinet, 17 June 2025. https://mediaoffice.ae/ar/news/2025/june/17-06/mohammed-bin-rashid-chairs-cabinet-meeting

[7] Saudi Data and Artificial Intelligence Authority. National Single Sign-On and Nafath FAQs. https://www.sdaia.gov.sa/en/Sectors/National-Information-Center/Pages/FAQs.aspx

[8] Saudi Data and Artificial Intelligence Authority. Regulation on Personal Data Transfer outside the Kingdom. https://sdaia.gov.sa/Documents/RegulationonPersonalDataEN.pdf

[9] Saudi Data and Artificial Intelligence Authority. Standard Contractual Clauses for Personal Data Transfer. https://dgp.sdaia.gov.sa/wps/wcm/connect/016534ff-df3b-4bf4-80d7-d7145f41a926/Standard%2BContractual%2BClauses%2BFor%2BPersonal%2BData%2BTransfer.pdf

[10] Bahrain National Portal. eKey: The Digital Authentication Framework. https://www.bahrain.gov.bh/wps/portal/en/BNP/HomeNationalPortal/ContentDetailsPage/

[11] Bahrain Information & eGovernment Authority. Projects and Initiatives: eKey 2.0. https://www.iga.gov.bh/en/category/projects-and-initiatives

[12] Qatar Ministry of Transport. Ministry launches National Authentication System 1.1. https://www.mot.gov.qa/en/news/ministry-launches-national-authentication-system-11

[13] Qatar Ministry of Interior. Public Key Infrastructure. https://portal.moi.gov.qa/wps/portal/MOIInternet/pkis/

[14] Oman Digital Portal. TAM electronic authentication. https://omanuna.oman.om/tam/

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

[16] World Wide Web Consortium. Verifiable Credential Data Integrity 1.0. https://www.w3.org/TR/vc-data-integrity/

[17] OpenID Foundation. OpenID for Verifiable Presentations 1.0, Final, 9 July 2025. https://openid.net/specs/openid-4-verifiable-presentations-1_0-final.html

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

[19] OpenID Foundation. OpenID4VC High Assurance Interoperability Profile 1.0. https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-1_0.html

[20] National Institute of Standards and Technology. NIST SP 800-63-4 Digital Identity Guidelines, July 2025. https://pages.nist.gov/800-63-4/sp800-63.html

[21] National Institute of Standards and Technology. NIST SP 800-63C-4 Federation and Assertions, July 2025. https://pages.nist.gov/800-63-4/sp800-63c.html

[22] World Bank. Principles on Identification for Sustainable Development. https://id4d.worldbank.org/guide/principles

[23] World Bank. Catalog of Technical Standards for Digital Identification Systems. https://id4d.worldbank.org/technical-standards

[24] European Union. Regulation (EU) 2024/1183 establishing the European Digital Identity Framework. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

[25] 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

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.