IDENTITY IN THE DIGITAL SOCIETY

# The UbID Approach

## Privacy-Preserving Digital Identity

WHITE PAPER Global privacy, personal-data protection, blockchain/DLT, cryptographic protection

Publication date: 30 July 2026

regulatory approval.

TABLE OF CONTENTS

Contents

## Executive Summary

Identity is becoming a reusable trust infrastructure rather than a collection of isolated accounts. UbID advances this transition by combining holder-controlled credentials, selective disclosure, cryptographic verification, strong authentication, distributed recovery, multi-device continuity, encrypted document custody, institutional governance and a progressive post-quantum path.

The same architecture also addresses a central regulatory problem: organisations routinely collect and retain more personal data than they need. UbID can allow a verifier to receive a cryptographically trustworthy proof of a fact without receiving the complete underlying document or profile. This supports data minimisation, purpose limitation, privacy by design, reduced breach impact and more transparent accountability across jurisdictions.

### Principal Conclusions

? UbID is best positioned as a privacy-enhancing and compliance-enabling identity infrastructure, not as an automatic legal- compliance product. ? Selective disclosure and derived proofs can materially reduce the quantity of personal data collected by relying parties. ? Holder control strengthens transparency and autonomy, but institutions still need lawful bases, notices, contracts, retention policies and rights-response procedures. ? Distributed recovery and device lifecycle controls can reduce account-takeover risk without returning all recovery power to a single administrator. ? Biometric processing must be optional or legally justified, isolated, purpose-bound and governed by jurisdiction-specific consent, retention and security rules. ? Europe and the United Kingdom provide formal digital-identity frameworks that UbID can target, but regulated status and trust marks require independent certification and registration. ? Chile?s Law No. 21.719 creates an immediate implementation priority ahead of its 1 December 2026 effective date. ? Colombia requires strong evidence of authorisation, purpose limitation, security and effective habeas-data procedures under its current framework. ? The United States requires a configurable state-by-state and sector-by-sector compliance overlay rather than a single national privacy profile. ? A single global deployment should use versioned jurisdiction profiles rather than attempting to force all countries into one privacy configuration. ? New York and California require distinct United States overlays: New York emphasises reasonable safeguards and breach governance, while California adds broad consumer rights, sensitive-data controls, risk assessments, cybersecurity audits and automated-decision requirements. ? Latin American regimes increasingly converge on accountability, data-subject rights, sensitive-data safeguards and transfer controls, but their authorities, legal bases, procedures and implementation maturity remain jurisdiction-specific. ? Asian deployments require tailored treatment: Hong Kong is organised around six data-protection principles; South Korea applies a comprehensive PIPA regime with strict biometric and foreign-operator expectations; Japan requires separation between APPI compliance and the special My Number/JPKI ecosystem. ? UbID has been developed by Paradigma SpA, Chile, whose institutional proposition centres on secure, interoperable and fraud-resistant digital-identity ecosystems. [35]

The expanded analysis also distinguishes blockchain technology from regulated cryptoasset activity, assesses the operative perimeter in the same jurisdictions, and defines the layered cryptographic, trusted-execution and KMS controls required to protect UbID data at rest, in transit and in use. Blockchain and cryptoasset laws are treated as a separate functional overlay; no inference of licensing, authorisation or legal status is made from the use of cryptography or decentralised identity standards.

? Blockchain technology constitutes a structural component of UbID rather than a merely optional feature. The user?s cryptographic identity is linked to an STX address derived from their public key, providing a verifiable blockchain identifier and enabling proof of control over the identity without revealing the private key.

The private key remains under the user?s exclusive control and is stored within an encrypted local cryptographic vault. Therefore, the Stacks blockchain does not directly encrypt or store the private key; instead, it provides the cryptographic linkage, verifiability, and traceability required to securely associate the UbID identity with the holder?s blockchain account. ? TEE and KMS controls provide defence in depth for data in use and institutional keys, but require attestation, least privilege, key lifecycle governance, independent assurance and tested recovery. ? Regulated cryptoasset functions must be segregated from the identity platform and assessed independently in every jurisdiction.

## Scope and Method

The regulatory analysis is based on primary legislation, supervisory-authority guidance and standards current to the research cut-off date. It focuses on general personal-data protection and digital-identity obligations. Sector-specific requirements may apply in finance, healthcare, insurance, employment, education, telecommunications, government and critical infrastructure.

The word ?alignment? in this paper means that a UbID capability can support or provide evidence for a legal or governance requirement. It does not mean that every default configuration satisfies every jurisdiction, nor that an implementation has been certified, approved or recognised by an authority.

Compliance should be expressed as jurisdiction profiles and policy controls: the same credential technology can be used globally, while lawful bases, disclosure rules, retention periods, biometric conditions, incident timelines, transfer safeguards and data-subject workflows are configured for the institution and location in which processing occurs.

Jurisdiction profiles are strategic implementation baselines. They identify the principal privacy and identity frameworks, the technical contribution that UbID can make, and the controls that institutions must still implement. Local legal review remains necessary before production deployment, particularly where regulations, enforcement guidance, certification schemes or commencement dates are evolving.

## Developer and Institutional Context: Paradigma SpA Chile

UbID has been developed by Paradigma SpA, Chile. Paradigma?s official website describes the company as an organisation focused on IT management and strategic digital transformation, with a mission to architect secure, interoperable and fraud- resistant identity frameworks for institutions. [35]

Paradigma presents its identity proposition as a unified Issuer?Holder?Verifier ecosystem intended to prevent identity fraud, support institutional compliance and enable trusted digital interactions. Its broader portfolio also refers to infrastructure automation, trusted identity naming and decentralised institutional collaboration. [35]

Within this white paper, Paradigma?s contribution is expressed through the UbID architecture: holder-controlled credentials, selective disclosure, verifiable provenance, strong authentication, encrypted custody, distributed recovery, multi-device continuity, observability and a progressive post-quantum path. The regulatory analysis does not treat these capabilities as an automatic certification; it explains how institutions can configure and evidence them under applicable law.

### Paradigma?s Strategic Contribution

? A Chilean-developed identity platform designed for international interoperability rather than a single domestic identity silo. ? A privacy-enhancing architecture that enables institutions to verify claims while reducing unnecessary document replication and personal-data concentration. ? A governance model that separates issuer, holder, verifier, custodian and infrastructure responsibilities, supporting clearer accountability. ? A compliance-enabling control layer capable of applying jurisdiction, sector, purpose, assurance, retention, transfer and rights-management policies. ? A long-term security strategy combining current interoperable cryptography with controlled migration towards post- quantum protections.

## Identity in the Digital Society: The UbID Approach

Identity services are foundational to modern societies. Every country provides identity credentials?such as national identity cards, passports, residence permits, and driving licences?that serve as a root of trust for individuals interacting with public institutions, private companies, and other people.

These credentials allow citizens to demonstrate who they are in physical environments. However, their reliability depends on the integrity of the document, the issuing authority, and the verification process. When an identity document is altered, counterfeited, stolen, or fraudulently obtained, individuals become exposed to identity theft, impersonation, financial crime, and reputational damage. Institutions, in turn, face operational losses, regulatory exposure, fraud, and a progressive erosion of trust in their services.

The challenge becomes significantly more complex in digital environments. When identity must be verified remotely, physical recognition and direct inspection of an original document are no longer sufficient. A photograph, scanned document, video call, or database lookup can provide evidence, but each mechanism introduces new risks involving manipulation, synthetic identities, deepfakes, compromised databases, replay attacks, and social engineering.

Lost or stolen credentials generally require reissuance by the original authority. In digital systems, identity verification has traditionally depended on usernames, passwords, security questions, one-time codes, and different forms of multi-factor authentication. These mechanisms are usually based on something the person knows, owns, or is. Although they improve security when combined, all of them have been compromised under certain circumstances.

Passwords can be guessed, reused, phished, or leaked. Mobile phones and SIM cards can be stolen or fraudulently duplicated. Email accounts can be taken over. Biometric information can be captured, replayed, or stored insecurely. Recovery procedures are often even more vulnerable than the original authentication method, turning account recovery into one of the principal entry points for identity theft.

These risks are especially serious in high-value domains such as banking, healthcare, insurance, government services, telecommunications, critical infrastructure, and systems administration. In these sectors, a successful impersonation does not merely expose an account: it may enable financial transfers, access to sensitive medical information, fraudulent contracting, unauthorised infrastructure changes, or the assumption of a person?s legal identity.

## The limitations of centrally managed digital identity

Traditionally, digital identity has mirrored the physical identity model. A central authority creates an account, stores the individual?s attributes, defines the authentication mechanisms, and decides when access should be granted or revoked. The institution therefore becomes both the issuer of the identity and the custodian of the information associated with it.

This model has enabled the expansion of digital services, but it has also produced large concentrations of personal information. Every central identity repository becomes a potentially valuable target. A single breach can expose the information of thousands or millions of people, while individuals have limited visibility or control over how their identity data is copied, processed, shared, retained, or reused.

The model also creates fragmentation. A person may have dozens or hundreds of independent digital identities across banks, universities, hospitals, employers, government portals, social networks, and commercial services. Each organisation repeats similar identification processes, stores another copy of the same personal information, and assumes the cost and risk of protecting it.

Institutions therefore spend considerable resources repeatedly verifying information that may already have been validated by another trusted organisation. Individuals are required to submit the same documents multiple times, disclose more information than necessary, and depend on each provider?s security and recovery procedures.

## Decentralised identity and the private-key challenge

Cryptography and blockchain technologies have demonstrated that digital assets and decentralised identifiers can be controlled without depending entirely on a central operator. A person who controls a cryptographic private key can authenticate operations, sign messages, and demonstrate control over a digital identifier.

However, the widespread adoption of these technologies has been restricted by the difficulty of securely managing private keys. A private key can provide strong mathematical protection, but losing it may result in permanent loss of access. Copying it into an insecure location, storing it in plain text, or exposing it through a compromised device may allow an attacker to assume control of the identity.

Traditional recovery mechanisms often reintroduce the same centralisation that decentralised identity was intended to avoid. At the same time, advances in quantum computing create a longer-term risk for cryptographic algorithms whose security depends on mathematical problems that sufficiently capable quantum computers may eventually solve.

The challenge is therefore not merely to create decentralised identifiers. A complete digital identity architecture must protect the keys, support secure recovery, operate across multiple devices, enable controlled disclosure of personal attributes, remain interoperable with institutional systems, and provide a credible migration path towards post-quantum security.

## A new paradigm: self-managed digital identity

A new model is emerging in which individuals can manage their own decentralised identifiers and associate verifiable attributes with them. These attributes may be self-declared or issued by trusted third parties such as governments, universities, employers, banks, professional bodies, healthcare organisations, and certification authorities.

The resulting credentials remain under the holder?s control and can be cryptographically verified by authorised recipients. Instead of querying the issuer every time a person needs to prove something, a verifier can validate the credential?s integrity, provenance, validity period, status, and relationship with the holder.

This changes the digital identity model fundamentally. The person is no longer represented exclusively by accounts maintained by external organisations. The individual possesses a reusable and portable collection of cryptographically verifiable credentials that can be presented across different services and contexts.

Under this model, a person does not always need to reveal an entire identity document. They may demonstrate only the information required for a particular transaction?for example, that they are over a certain age, hold a valid professional certification, are authorised to represent an organisation, or possess an active insurance policy.

## UbID: a secure identity infrastructure centred on the person

UbID is designed to turn this emerging paradigm into a practical identity infrastructure for people and institutions. It combines decentralised identifiers, verifiable credentials, selective disclosure, strong authentication, encrypted local custody, controlled recovery, multi-device management, institutional verification, and progressive post-quantum protection.

Its purpose is not to eliminate trusted institutions. Governments, universities, banks, healthcare providers, employers, and certification bodies remain essential sources of authoritative information. UbID changes the way that trust is created, transported, verified, and controlled.

Institutions continue to issue authoritative claims, but individuals can hold and reuse those claims without requiring every verifier to maintain another isolated copy of the same data. Trust becomes portable, cryptographically verifiable, and subject to explicit control by the holder.

### Benefits for individuals

For individuals, UbID provides a digital identity that is portable and not permanently confined to a single provider, application, or device. The person can maintain control over identity credentials and decide when, where, and for what purpose they are presented.

This reduces dependence on passwords and centralised account recovery procedures. Authentication can be reinforced through passkeys, biometric verification, trusted devices, cryptographic proofs, and policy-based combinations of these mechanisms.

UbID also addresses one of the most difficult problems in self-managed identity: secure recovery. Rather than relying on a single recovery code, administrator, email account, or cloud provider, recovery can be distributed across independently protected components using threshold cryptography.

With a threshold model, no single custodian, server, or device needs to possess the complete recovery secret. A defined number of valid fragments must participate before recovery can proceed. This reduces the risk that one compromised party can take control of the identity.

Recovery can additionally be conditioned on strong evidence, including authenticated communications, device approval, biometric verification, policy checks, nonces, replay protection, and auditable authorisation events. The objective is to make recovery possible for the legitimate person while making fraudulent recovery substantially more difficult.

UbID?s multi-device model allows a person to use their identity from a controlled set of authorised devices. New devices can require explicit approval, while lost or compromised devices can be revoked without necessarily invalidating the person?s entire digital identity.

The individual may also maintain an encrypted document vault for credentials and supporting documents. Sensitive information can be encrypted locally using keys derived and protected through hardened cryptographic mechanisms. The vault is intended to minimise unnecessary exposure of unencrypted identity information to servers or intermediaries.

? Less dependence on passwords and vulnerable security questions. ? Greater control over personal information and credential disclosure. ? Reduced need to repeatedly upload copies of identity documents. ? Portability of credentials across compatible services. ? Safer enrolment of additional devices. ? Controlled revocation of lost or compromised devices. ? Stronger protection against account takeover and fraudulent recovery. ? Selective presentation of only the attributes required for a transaction. ? Cryptographic proof of credential integrity and provenance.

Most importantly, UbID separates identity from any single account. The individual?s identity is not merely a database entry owned by a platform. It becomes a set of controlled, verifiable relationships between the person, their identifiers, their devices, and the institutions that have issued credentials to them.

## Benefits for institutions

For institutions, UbID provides a mechanism to receive stronger, more structured, and cryptographically verifiable identity evidence.

Instead of accepting only photographs, photocopies, manually entered data, or unverifiable PDF files, an organisation can validate whether a credential was issued by a recognised authority, whether it has been altered, whether it remains valid, and whether the person presenting it is an authorised holder.

This can reduce document fraud, manual review, repeated identity proofing, and the operational cost of maintaining large quantities of duplicated personal data.

Institutions can issue credentials that are reusable beyond their own platforms. A university may issue a digitally verifiable academic credential. A professional body may issue a licence or certification. An employer may issue an employment or role credential. A bank may attest that a customer has completed a specific verification process. A government authority may issue identity attributes or permits.

Each credential can be verified according to defined policies without requiring the verifier to establish a proprietary integration with every original database.

UbID also supports a more privacy-preserving institutional model. Organisations can request only the attributes required for a particular purpose. This reduces the amount of personal information collected and stored, lowering both privacy risk and the impact of a potential breach.

For example, a service may need to know that a person is legally an adult but may not need their exact date of birth. An institution may need proof that a professional licence is valid but may not need the person?s complete educational history. A company may need confirmation that an individual is authorised to represent another organisation without obtaining unrelated personal data.

? Stronger assurance regarding the origin and integrity of credentials. ? Reduced exposure to forged, altered, or replayed documents. ? Lower identity-verification and manual-review costs. ? Fewer duplicated repositories of sensitive personal information. ? Improved onboarding and account-recovery security. ? Clearer credential status, expiration, suspension, and revocation handling. ? Reusable verification policies across multiple types of credentials. ? Better auditability of issuance, presentation, verification, and recovery events. ? Improved interoperability between public and private organisations. ? Reduced dependence on proprietary identity silos. ? A controlled path for introducing post-quantum cryptographic protection. ? The ability to automate verification without fully automating sensitive final decisions.

UbID can also support institutional governance models in which high-impact actions follow a controlled sequence such as prepare, validate, approve, and execute. An automated system may prepare and technically validate a credential request, while final issuance, revocation, recovery, or high-risk access remains subject to an authorised institutional decision.

This balance allows institutions to benefit from automation while retaining accountability, segregation of duties, and human oversight.

## Trust without unnecessary centralisation

UbID does not assume that every identity claim is equally trustworthy. Trust depends on the issuer, the credential type, the verification method, the current credential status, the applicable policy, and the context in which the credential is presented.

A self-issued assertion may be appropriate for a personal preference or low-risk profile attribute. A government-issued credential may be required for legal identity. A university-issued credential may establish an academic degree. A regulated professional body may attest to a licence. A biometric verification process may demonstrate that the person presenting a credential corresponds to the enrolled holder.

UbID allows these different levels and sources of trust to coexist within a common architecture. The verifier can decide which issuers, credential formats, assurance levels, cryptographic algorithms, and presentation conditions are acceptable for a specific transaction.

This creates a decentralised model without eliminating governance. Trust remains measurable, contextual, and policy- driven.

## Selective disclosure and privacy-preserving verification

Through selective-disclosure credential mechanisms, a holder may reveal only the claims required for a particular purpose while withholding unrelated information. Cryptographic proofs allow the verifier to confirm that the disclosed claims belong to a credential issued by a trusted entity and have not been modified.

? Proving legal age without revealing the complete date of birth. ? Demonstrating residency without disclosing unnecessary identity attributes. ? Confirming professional status without sharing unrelated employment records. ? Proving that a credential is active without presenting the original document. ? Demonstrating organisational authority without exposing personal information beyond what is required. ? Confirming that an identity verification was completed by a trusted institution without repeating the entire process.

This model improves privacy while also reducing institutional liability. Data that is never collected cannot be leaked from the verifier?s systems.

## Secure document and credential custody

UbID incorporates the concept of an encrypted document vault in which these materials can be protected while remaining associated with the holder?s identity.

Documents may be classified, processed through optical character recognition, examined for structured data, and subjected to different levels of verification. Verification may include QR code validation, digital-signature analysis, institutional- domain checks, document consistency checks, and confirmation against recognised issuers or external sources.

This gives individuals a more useful and secure repository, while institutions receive clearer information about the reliability of the evidence being presented.

## Strong authentication without dependence on a single factor

UbID recognises that no authentication factor is infallible. Security therefore depends on combining factors according to risk and context.

Passkeys can provide phishing-resistant authentication. Biometrics can strengthen proof that the legitimate holder is present. Device registration can limit access to known endpoints. Cryptographic keys can demonstrate control of a decentralised identifier. Institutional policies can require additional approval for high-risk actions.

The appropriate combination may vary. A low-risk credential presentation may require only a valid holder proof. A sensitive recovery event may require multiple registered devices, biometric verification, threshold approval, and cryptographic challenge-response validation.

This policy-based approach avoids treating every transaction identically and allows security controls to be proportional to potential impact.

## Recovery as a security protocol

In many systems, recovery is treated as an administrative exception. In UbID, recovery is treated as a first-class cryptographic and governance protocol.

Recovery must establish that the requester is legitimately entitled to regain control. It must prevent replay, impersonation, unilateral administrator access, and silent substitution of keys or devices. It must also produce evidence that can be audited without unnecessarily exposing the recovered secret.

Threshold cryptography allows recovery authority to be distributed. Trusted custodians, protected infrastructure components, approved devices, or secure execution environments may each participate without independently controlling the full identity.

Server-side trusted execution environments can release an authorised fragment under defined policy without reconstructing the complete secret. Edge trusted execution environments can protect sensitive operations locally on supported devices. Encrypted communications can transport recovery messages, while signed evidence records the decisions and conditions that permitted the operation.

The objective is not merely to recover access. It is to recover access in a way that preserves the credibility of the identity after the recovery has occurred.

## Multi-device identity continuity

Modern users do not interact through a single permanent device. Phones are replaced, computers are upgraded, devices are lost, and different contexts require different endpoints.

UbID supports controlled multi-device identity rather than unrestricted synchronisation. A new device must be associated with the legitimate holder and may require approval from an already trusted device or another authorised recovery mechanism.

## Preparing identity for the post-quantum era

Most current digital identity systems rely on classical public-key cryptography. These algorithms remain essential for interoperability, but the long operational lifetime of identity information requires preparation for future cryptographic transitions.

Identity credentials, recovery records, legal documents, and institutional attestations may remain sensitive or valuable for many years. Information captured today may be stored by an attacker and targeted later when stronger computational capabilities become available.

UbID therefore incorporates a progressive approach to post-quantum security. Classical algorithms can continue to support compatibility with current wallets, verifiers, and standards, while additional post-quantum signatures, key-establishment mechanisms, or cryptographic evidence can be introduced alongside them.

A hybrid approach allows an operation to benefit from both established classical cryptography and newer post-quantum algorithms. This avoids an abrupt migration that would isolate the platform from the existing ecosystem, while reducing dependence on a single cryptographic family.

For institutions, this provides a controlled migration strategy. For individuals, it strengthens the long-term protection of identity keys, recovery mechanisms, and high-value credentials.

## Interoperability rather than another identity silo

UbID is oriented towards recognised decentralised identity and credential standards, including decentralised identifiers, verifiable credentials, selective-disclosure JWT-based credentials, OpenID-based credential issuance and presentation flows, and DIDComm-based secure communications.

Interoperability protects institutions from excessive vendor dependence and gives individuals greater confidence that their credentials will remain portable.

## Auditability, observability, and institutional accountability

UbID incorporates operational observability, health monitoring, metrics, alerts, and auditable evidence. Identity issuance, verification, device registration, credential status changes, and recovery operations can produce structured records suitable for investigation and governance.

Sensitive secrets do not need to appear in these records. Instead, the system can record the cryptographic references, policy decisions, actors, timestamps, challenges, verification results, and authorisation evidence required to demonstrate what occurred.

This gives institutions greater capacity to detect anomalies, investigate incidents, satisfy internal controls, and demonstrate compliance.

## A platform for institutional collaboration

An organisation can issue a credential that another organisation verifies. The verifier does not necessarily need continuous access to the issuer?s internal systems, and the issuer does not need to learn every context in which the holder presents the credential.

Such a model can support cross-sector ecosystems involving government, education, finance, healthcare, employment, insurance, telecommunications, and professional accreditation.

A person could maintain a coherent digital identity while receiving different credentials from different authorities. Each institution remains responsible for the claims it issues, while the holder remains responsible for deciding how those claims are used.

## Enabling trusted digital agents

As artificial intelligence systems and autonomous software agents become more active in institutional processes, identity will also need to extend beyond human login sessions.

Agents must be able to discover which credentials are required, understand verification policies, prepare requests, validate technical conditions, and present information to authorised decision-makers. However, they should not automatically receive unrestricted authority to issue credentials, recover identities, or execute high-impact actions.

This creates a path towards machine-assisted identity operations without sacrificing institutional accountability or individual control.

## A new distribution of responsibility

The institution remains responsible for the truth and governance of the claims it issues. The individual gains control over the custody and presentation of those claims. The verifier remains responsible for deciding which evidence is sufficient for a transaction. The platform provides the cryptographic, operational, and interoperability mechanisms that allow those responsibilities to work together.

This model reduces the expectation that a single organisation must permanently store, control, and protect every component of a person?s identity.

It also avoids placing the entire burden on the individual. Self-managed identity should not mean that a lost device or forgotten secret results in permanent exclusion. Secure recovery, multi-device continuity, institutional credentials, protected cryptographic custody, and auditable governance are necessary to make individual control practical.

## The broader value of UbID

For society, it offers an alternative to the growing accumulation of fragmented identity databases and insecure authentication mechanisms. It enables a model in which trust can be established cryptographically, disclosed proportionally, verified independently, and governed transparently.

The ultimate objective is to allow individuals to represent themselves securely in the digital world while enabling institutions to trust the evidence they receive?without demanding unnecessary data, without depending exclusively on vulnerable intermediaries, and without surrendering long-term security or interoperability.

In this model, digital identity becomes more than an access mechanism. It becomes reusable trust infrastructure for modern society.

## Regulatory and Data Protection Contribution of UbID

Personal-data regulation does not prescribe one universal digital-identity architecture. It establishes duties concerning lawfulness, fairness, transparency, purpose, proportionality, security, retention, individual rights and accountability. UbID contributes by converting many of these duties into enforceable technical patterns and verifiable operational evidence.

The strongest regulatory value of UbID is not that it stores identity data more securely in a new central repository. Its value is that institutions can verify credentials and attributes while collecting less underlying data, holders can control presentations, credentials can remain portable, and the platform can record the policy and cryptographic evidence needed to explain why an identity operation was permitted.

### Cross-Jurisdiction Compliance Architecture

| | |
|---|---|
| Data minimisation | Selective disclosure, derived claims and verifier-specific presentations can disclose only the attributes required for a transaction. |
| Purpose limitation | Credential requests can be bound to a declared purpose, relying party, audience, nonce, transaction and policy decision. |
| Holder agency | The person can explicitly authorise issuance and presentation, inspect what is requested and control registered devices. |
| Security by design | Encryption, passkeys, device binding, threshold recovery, key rotation, secure execution and post-quantum migration reduce identity risk. |
| Accountability | Issuance, presentation, verification, status, device and recovery events can create auditable evidence without logging secret material. |
| Rights enablement | Credential and vault indexes can support access, rectification, suppression, revocation, restriction and portability workflows. |
| Jurisdiction controls | Policies can control residency, international transfer, biometric use, retention, legal basis, incident handling and automated decision thresholds. |

### Governance Boundary: What UbID Does Not Replace

? Determination and documentation of the legal basis for each processing purpose. ? Privacy notices, consent language and institutional policies appropriate to the jurisdiction and sector. ? Controller?processor, issuer?verifier and vendor contracts, including international-transfer clauses. ? Data-protection impact assessments, legitimate-interest assessments and sector-specific risk assessments where required. ? Staff authorisation, segregation of duties, training and disciplinary controls. ? Statutory retention schedules, legal holds, records-management duties and public-record obligations. ? Regulatory registrations, certification, conformity assessment, trust marks or qualified trust-service status. ? Breach notification, regulator communication and remedies for affected individuals.

UbID marketing and contractual materials should distinguish ?supports compliance?, ?configured for a regulatory profile?, ?independently assessed?, ?certified?, and ?legally recognised?. These terms are not interchangeable.

## Blockchain and Distributed-Ledger Regulatory Study

Blockchain regulation is not a single legal category. A distributed ledger may be used as an internal integrity mechanism, a public record, a payment rail, a market infrastructure, a token-issuance platform or a custody system. The applicable law follows the function, the rights represented, the parties served and the risks created?not the use of the word ?blockchain?. NIST similarly treats blockchain as a technical family of distributed, cryptographically linked ledgers rather than as a synonym for cryptocurrency. [36]

UbID?s identity vault must not be described as a cryptoasset wallet unless it actually provides cryptoasset services. Custody of a person?s identity credentials and authentication keys is legally and operationally different from custody of transferable financial value. Product language, key separation, APIs, contracts, accounting and incident procedures should preserve that boundary. If a future module adds token or value functions, it requires a separate regulatory assessment and should not inherit approval from the identity platform.

### Data Protection Rule for Blockchain Deployments

The privacy analysis applies even where a ledger stores only identifiers, addresses, hashes or encrypted values if those elements can reasonably be linked to a person. The European Data Protection Board?s final blockchain guidelines of July 2026 emphasise architecture selection, role allocation, data protection by design, minimisation and effective rights, and caution against placing personal data on-chain where this conflicts with data-protection principles. The same engineering principle is prudent across all jurisdictions in this paper.

? Keep credentials, claims, biometrics, document images, device identifiers, recovery data and presentation histories off- chain. ? If anchoring is justified, publish only a non-reversible commitment generated with domain separation, a secret salt or keyed construction; a plain hash of predictable personal data is not anonymisation. ? Do not assume that encrypting on-chain personal data solves erasure. Ciphertext, keys, metadata and future cryptanalytic risk must be assessed over the full retention period. ? Prefer permissioned governance when institutional accountability, node location, access control, correction procedures and incident response must be enforceable. ? Document node operators, controller and processor roles, consensus governance, software-change authority, jurisdiction, retention and the procedure for contested or unlawful records.

### Cross-Jurisdiction UbID Deployment Rule

Across all jurisdictions, the safest institutional position is capability separation. The core UbID product should issue, hold and verify identity evidence; a financial or cryptoasset extension should be a separately governed module with distinct keys, ledgers, operators, licences, risk assessments and incident procedures. This prevents a future token feature from contaminating the compliance assumptions of the identity platform and allows each institution to demonstrate precisely which regulated function it performs.

? No personal data, credential payload, biometric template or recovery shard on a public blockchain. ? No transferable value or investment right in an identity credential. ? No institutional ability to move holder assets merely because it can help recover identity access. ? Separate legal entities, service descriptions and key hierarchies where regulated cryptoasset services are added. ? A versioned jurisdiction profile must record the legal perimeter, regulator, licence, effective date, permitted activities and prohibited functions.

## Cryptographic Protection, TEE and KMS

UbID?s protection model should be evaluated across three states of information: data at rest, data in transit and data in use. Encryption of a database protects only one state. Strong identity infrastructure requires cryptographic separation of duties, controlled key release, hardware-backed or confidential execution for the most sensitive operations, recoverability without a universal administrator secret, and evidence that the authorised code and policy?not merely an authenticated user?permitted an operation.

### Layered Security Architecture

The architecture should preserve a hierarchy in which holders control credentials, applications receive only narrowly scoped cryptographic services, KMS governs institutional keys, and TEEs protect high-risk computation in use. No layer is a substitute for the others: a TEE without sound key management can receive the wrong secret; a KMS without attested execution can release a correct secret to compromised code; and strong algorithms do not correct excessive privileges, weak recovery or poor audit governance.

### Trusted Execution Environments and Data in Use

A TEE creates a hardware-isolated execution environment intended to protect code and data while they are being processed. The relevant property for UbID is remote attestation: a relying component can verify measurements of the platform and workload before releasing a shard or key. AMD SEV-SNP protects confidential virtual machines and adds memory-integrity protections; Intel TDX isolates hardware-backed trust domains; AWS Nitro Enclaves provides isolated compute with attestation; and OP-TEE is an Arm TrustZone-based companion environment for non-secure Linux. [37] [38] [39] [32]

A TEE does not make arbitrary code trustworthy, eliminate software vulnerabilities or replace secure boot, patching, access control, logging and independent review. Attestation evidence must be checked against an approved measurement and policy, including firmware and security-version requirements. Secrets must not be released to debug builds, outdated trusted computing bases or measurements that cannot be linked to a signed release. GlobalPlatform?s TEE Protection Profile provides an evaluation reference for mobile TEEs, but product-specific certification and deployment assurance remain necessary. [40]

### Custodian TEE and Edge TEE Profiles

The UbID Custodian TEE Profile is an infrastructure worker running in a server-class confidential-computing environment such as SEV-SNP, TDX or Nitro Enclaves. It validates the authenticated DIDComm request, challenge, nonce, transaction context, replay window, policy decision and attestation state, then releases only one authorised recovery shard. It never reconstructs the holder?s complete secret and produces signed, minimised evidence of the decision.

The UbID Edge TEE Profile uses OP-TEE or a comparable trusted environment on a suitable Arm device, gateway or IoT platform. It can receive three authorised shards, reconstruct locally, use the recovered secret for the narrowly approved operation and zeroise transient material without exporting the complete secret to the normal operating system. OP-TEE is complementary to server TEEs: it protects the final edge computation, while the custodian TEEs protect independent shard release.

### Attested Key and Shard Release Protocol

? The holder initiates recovery and receives a transaction identifier, cryptographically random challenge, nonce and short validity window. ? The edge or destination TEE produces attestation bound to an ephemeral public key, approved workload measurement, security version and the recovery transaction. ? Each custodian independently validates holder authentication, device and recovery policy, nonce freshness, replay state, jurisdiction controls and TEE attestation.

? KMS authorises only the required cryptographic operation or wraps one shard to the attested ephemeral key; the shard is never returned in plaintext to the ordinary service. ? Three shards are reconstructed only inside the approved edge TEE or designated holder environment. The complete secret is not logged, persisted or exposed through diagnostics. ? The environment performs the approved re-key, vault-open or recovery action, zeroises transient values and emits signed evidence containing identifiers and outcomes but no secret material.

## Post-Quantum Cryptography and Crypto-Agility

NIST FIPS 203 standardises ML-KEM for post-quantum key establishment and FIPS 204 standardises ML-DSA for digital signatures. [29] [30] UbID?s appropriate migration model is hybrid and format-aware: use classical cryptography for current interoperability, add ML-KEM-768 to protect long-lived recovery and custodian exchanges against harvest-now-decrypt- later risk, and attach ML-DSA-65 evidence where verifiers and formats can validate it.

The compact interoperable SD-JWT should not be given an ad hoc second signature that breaks external wallet and verifier compatibility. Until standard consuming formats support post-quantum signatures, UbID can keep the credential interoperable and expose a separately bound PQC proof or use a multi-signature container only in controlled ecosystems. Every artifact must state whether PQC is experimental, parallel evidence or required verification; silent fallback from hybrid to classical-only validation must be prohibited for flows that claim post-quantum assurance.

## Blockchain Anchoring and Cryptographic Safety

A blockchain hash proves, at most, that a particular byte string or commitment existed in relation to a ledger event; it does not prove that the source document was authentic, lawfully obtained, accurate, current or linked to the correct person. Those properties come from issuer governance, identity proofing, signatures, status, holder binding and verifier policy. UbID should therefore treat blockchain anchoring as optional timestamp or integrity evidence, never as a replacement for credential validation.

If anchoring is adopted, each credential should use a randomised commitment or Merkle construction that prevents dictionary recovery and cross-context correlation. The chain should contain no DID that directly resolves to personal data, no document hash derived from predictable fields, no biometric material, no revocation reason and no presentation history. Off-chain systems must retain the legal basis, purpose, retention and rights workflow, while the ledger governance must support software defects, compromised signing keys and contested entries.

## Production Governance and Assurance Requirements

? Maintain a signed cryptographic bill of materials covering algorithms, libraries, key sizes, protocols, certificate profiles, hardware roots of trust and deprecation dates. ? Classify each key by owner, purpose, environment, sensitivity, exportability, rotation, backup, revocation and destruction procedure. ? Use separate KMS mounts, keys and policies for JWT signing, credential issuance, document encryption, recovery wrapping, audit integrity and test environments. ? Require dual control for root-token generation, policy escalation, unseal and recovery-share operations; preserve evidence without recording the shares. ? Verify TEE attestation, firmware status, workload measurement, security version and revocation information before every sensitive release. ? Exercise KMS restore, seal/unseal, token revocation, key rotation, compromised-issuer-key response, TEE measurement rollover and full recovery at least on a defined risk-based schedule. ? Commission threat modelling and penetration testing for side channels, replay, rollback, confused-deputy paths, malicious custodians, supply-chain compromise and observability leakage. ? Represent implementation status accurately: architecture target, proof of concept, tested staging control and production-assured control are distinct claims.

These controls strengthen confidentiality, integrity, availability and accountability, but they do not by themselves create legal compliance or formal certification. Institutions remain responsible for role allocation, lawful processing, sector rules, risk acceptance, independent assurance, incident notification and the suitability of the selected TEE and cryptographic module for each jurisdiction and use case.

## UbID Regulatory Control Profile

A production deployment should translate regulatory obligations into a versioned machine-readable control profile. The profile should be evaluated at issuance, presentation, verification, recovery, device registration, document ingestion and administrative exception points. It should support country, state or province, sector and institutional-role overlays while retaining the exact policy version used for every historical transaction.

| |
|---|
| Jurisdiction and sector Country, state or region; public/private sector; finance, health, education, employment, insurance or other domain. |
| Institutional role Controller, processor, issuer, verifier, holder-service provider, custodian, orchestration provider or trust- service provider. |
| Lawful basis Consent, contract, legal obligation, public task, legitimate interests or other authorised ground, with special-category conditions. |
| Purpose and audience Declared purpose, requesting institution, intended audience, transaction identifier and prohibited secondary uses. |
| |
| |
| Rights handling Access, correction, deletion, suppression, opposition, restriction, portability, complaint and appeal workflows. |
| Retention and status Credential validity, revocation, evidence retention, legal hold, vault deletion and biometric destruction periods. |
| |
| Incident obligations Detection, escalation, regulator and individual notification timelines, evidence preservation and recovery. |
| Automated decisions Human approval thresholds, explanation, contestability, bias monitoring and prohibited automated actions. |
| |
| Legal version and effective date Enacted law, operative date, transitional provision, regulation, authority guidance and internal approval date. |
| Consent and notice model Required notice language, consent granularity, withdrawal handling, alternative lawful grounds and evidence format. |
| Sensitive and biometric data Classification, necessity test, alternatives, template location, access, retention, destruction and anti- replay requirements. |
| International transfers Origin, destination, recipient, legal mechanism, localisation rule, onward-transfer conditions and remote-access controls. |
| Incident and regulator workflow Detection thresholds, assessment standard, notification deadlines, competent authority, affected- person communication and evidence retention. |
| Automated decision controls Applicable profiling or ADMT rules, explanation, human review, objection, opt-out and risk-assessment requirements. |
| Legal-change monitoring Owner, review cadence, trigger events, counsel approval, profile supersession and migration of pending operations. |

Comparative Jurisdiction Matrix

| Jurisdiction | Primary framework | Regulatory emphasis | UbID contribution | Residual institutional obligations |
|---|---|---|---|---|
| European Union | GDPR; EUDI/eIDAS 2.0 | Lawful basis, minimisation, rights, DPIA, transfers, regulated wallet/trust roles | | |
| United Kingdom | UK GDPR; DPA 2018; DUAA 2025; DVS TF | Privacy by design, complaints, DVS assurance and certification | Holder service, passkeys, confidence and audit metadata | ICO duties, CAB certification, OfDIA registration |
| Canada | PIPEDA; Privacy Act; provincial regimes | Appropriate purposes, consent, safeguards, access, breach records, trust frameworks | | |
| United States ? federal | FTC; HIPAA; GLBA; COPPA; sector laws | Unfair/deceptive practices, security and sector duties | Configurable overlays, strong authentication, audit evidence | |
| New York State | SHIELD Act; NYDFS Part 500 | Reasonable safeguards, breach reporting, financial cybersecurity | | |
| California | CCPA/CPRA; 2026 regulations; Delete Act | Rights, sensitive data, risk, cyber audits, ADMT and opt-out | | |
| Mexico | 2025 private/public data laws | Legality, purpose, consent, proportionality, ARCO, security, transfers | | |
| El Salvador | Decree 144/2024; cybersecurity law | Emerging comprehensive privacy and security governance | | |
| Colombia | Law 1581; Decree 1074; Law 527 | Authorisation, purpose, restricted circulation, habeas data | Holder approval, minimisation, complaints evidence | Policies, RNBD, SIC incidents and transfers |
| Peru | Law 29733; DS 016-2024-JUS | Consent, ARCO, data banks, security, sensitive data, transfers | | |
| Brazil | LGPD; ANPD regulations | Legal bases, rights, sensitive/children data, accountability, transfers | | |
| Chile | Law 19.628; Law 21.719; cyber law | Modernised rights, oversight, security, transfers | Pre-compliance architecture, rights workflows, observability | |
| Paraguay | Law 7593/2025 | New comprehensive framework; implementation transition | | |
| Argentina | Law 25.326; Decree 1558/2001 | Consent, habeas data, security, databases, transfers | Holder approval, rights index, encryption and provenance | |
| Hong Kong | PDPO and six DPPs | Collection, retention, use, security, openness, access/correction | | |
| South Korea | PIPA; PIPC guidance | Granular consent, sensitive IDs, biometrics, transfers, security | Minimisation, policy receipts, biometric isolation | Foreign operator, representative, ISMS- P/sector duties |
| Japan | APPI; My Number Act/JPKI | Purpose, security, transfers, rights; special My Number controls | | |

## Regulatory Value Proposition

For regulators and auditors, UbID can produce a clearer chain of responsibility: who issued the credential, who controlled it, what the verifier requested, what was disclosed, which policy permitted the operation, what security controls were applied and how the institution responded to rights or incidents.

The strategic contribution is therefore not merely decentralisation. It is accountable minimisation: reliable identity proof with less unnecessary personal-data concentration, combined with governance strong enough for institutions to trust the result.

## Limitations and Legal Notice

This white paper is a strategic and technical analysis, not legal advice. Laws, regulations, supervisory guidance, certification schemes and enforcement practice change over time. Each institution must complete its own role mapping, legal-basis analysis, data-protection impact assessment, contractual review, sector analysis and regulatory engagement before deployment in Canada, the United States, New York State, California, Mexico, El Salvador, Colombia, Peru, Brazil, Chile, Paraguay, Argentina, the United Kingdom, the European Union, Hong Kong, South Korea or Japan.

The analysis describes capabilities and potential alignment. It does not represent that UbID or Paradigma SpA has already obtained European Digital Identity Wallet status, qualified trust-service status, UK DVS certification, Canadian or Asian government accreditation, United States state approval, Latin American regulatory authorisation, sector approval or any equivalent certification unless supported by separate current evidence.

## References

https://www.gov.uk/government/publications/uk-digital-verification-services-trust-framework-1-0/uk-digital-verification-services-trust- framework-1-0-pre-release

[38] Intel. Trust Domain Extensions (Intel TDX) overview.
https://www.intel.com/content/www/us/en/developer/tools/trust-domain- extensions/overview.html