



ROOT ZERO VAULT

Digital Inheritance Is a Governance Problem:

How Constitutional Trust Infrastructure Enables Durable, Cross-Jurisdiction Estate Continuity

Hosameldeen (Deen) Saleh

Founder & CEO, Root Zero Vault, Inc.

Designer, Recursive Stage-Based Identifier System (RSBIS)

Published: January 20, 2026

Correspondence: deen.saleh@rootzerovault.com

Abstract

Digital assets now constitute a multi-trillion-dollar component of global estate value, yet inheritance remains ad hoc, vendor-dependent, and unenforceable across jurisdictions. When individuals die, families chase passwords across fragmented platforms. Executors possess legal authority without technical means. Cross-border estates lack portable proof. Digital continuity depends on corporate cooperation, not structural law.

This paper demonstrates that digital inheritance is fundamentally a governance problem requiring deterministic validation of succession claims under declared policy with durable, court-verifiable evidence that survives vendor bankruptcy, platform shutdown, and jurisdictional boundaries.

We present the Recursive Stage-Based Identifier System (RSBIS)—a constitutional trust infrastructure addressing these requirements. RSBIS enables succession-by-structure through: (i) immutable identity parcels (Deeds) declaring succession policy with M-of-N witness requirements and geographic/role diversity constraints; (ii) tamper-evident succession execution recorded in append-only Journals with hash-chain integrity; (iii) Registry receipts providing economic finality independent of vendor operations; (iv) continuity bundles enabling offline verification by courts without vendor subpoenas; (v) cryptographic commitment (CVIDs) binding succession claims to recomputable proof.



ROOT ZERO VAULT

We include normative governance specimens demonstrating deterministic acceptance of valid succession (US estates, UAE estates, global defaults, subset inheritance) and deterministic rejection of invalid claims (post-hoc redefinition attempts, broken succession proofs, grandchild scope violations). A complete end-to-end walkthrough demonstrates how cross-border estate succession operates from Deed creation through court verification without vendor cooperation.

The contribution demonstrates that constitutional governance transforms digital inheritance from vendor-dependent contingency to structural law, enabling families and executors to prove legitimate succession across platforms, borders, and decades—with evidence that remains valid regardless of corporate viability, platform availability, or cryptographic primitive longevity. We explicitly scope what constitutional trust infrastructure does and does not do, clarifying that RSBIS provides verifiable proof to support legal authority, not a replacement for probate courts or statutory succession law.

RSBIS further demonstrates that digital inheritance shares constitutional infrastructure with fifteen other trillion-dollar problems, evidencing that high-stakes institutional actions across domains require the same governance property: deterministic validation under explicit policy with permanent, recomputable evidence.

1. Introduction: The Multi-Trillion-Dollar Governance Gap

1.1 The Scale of Digital Inheritance

Digital assets in estates now include:

- **Financial accounts:** Cryptocurrency wallets, investment platforms, digital banking, payment systems
- **Intellectual property:** Digital creative works, software repositories, NFTs, domain names, trademarks
- **Business assets:** SaaS subscriptions, cloud infrastructure, customer databases, operational systems
- **Personal records:** Photos, communications, social media accounts, health data, location history
- **Access credentials:** Password managers, two-factor authentication devices, API keys, recovery codes



ROOT ZERO VAULT

Conservative estimates place digital estate value at **\$2.5 trillion globally** and growing exponentially as individuals and businesses digitize assets and operations. By 2030, nearly all estates will include substantial digital components requiring succession management.

1.2 Current Failure Modes

When individuals die, succession typically fails in predictable ways:

Vendor dependency: Families must convince each platform individually to grant access. Some cooperate through formal processes; many refuse citing privacy policies or terms of service. Platform policies vary arbitrarily across jurisdictions and change without notice. Executors possess legal authority from probate courts but lack technical means to enforce that authority against uncooperative platforms, particularly those operating in foreign jurisdictions.

Password fragmentation: Critical access credentials are scattered across email accounts, password managers, handwritten notes, verbal communications, and browser-saved logins. No systematic recovery mechanism exists that doesn't depend on the decedent's active cooperation (which is definitionally impossible post-death). Secure password practices that protect against unauthorized access during life become barriers to legitimate succession after death.

Cross-border complexity: Decedent owns assets in multiple jurisdictions with conflicting legal frameworks. A probate court in jurisdiction A lacks authority to compel compliance from platforms operating in jurisdiction B. International coordination requires separate legal proceedings in each country, manual evidence gathering, and often translation and authentication of foreign court orders—a process costing tens of thousands of dollars and taking years when it succeeds at all.

Platform shutdown: Vendor bankruptcy or platform termination destroys access permanently. When platforms fail, no portable proof of ownership or succession authority survives corporate liquidation. Assets become permanently inaccessible orphans with no recovery mechanism.

Executor helplessness: Legal authority to manage estates—granted through letters testamentary, trust instruments, or court appointment—doesn't translate to technical authority over digital platforms. Courts can issue orders; platforms can ignore them, especially foreign platforms beyond jurisdictional reach. Executors report spending months attempting to access critical business systems necessary for ongoing operations.

Evidence ephemeral: Succession proof relies on live systems, mutable logs, and vendor cooperation. Five years later, when disputes arise or beneficiaries need to prove legitimacy for



secondary transfers, the original evidence may be impossible to reconstruct. Vendors purge records, systems migrate, personnel change, and institutional memory disappears.

1.3 Why Current Approaches Fail

Legal frameworks assume physical assets: Probate law developed for real estate, bank accounts, and tangible personal property. These assets have clear physical location, obvious jurisdiction, and cannot simply disappear when a corporation fails. Digital assets exist simultaneously across borders with no single jurisdictional anchor, can vanish instantly when servers shut down, and often lack clear ownership records independent of platform attestation.

Platform terms of service override statutory law: Vendors unilaterally write succession policies in terms of service that may prohibit transfer entirely, require specific forms of death certification, or demand indemnification executors cannot provide. In practice, legal authority proves insufficient against uncooperative platforms protected by jurisdictional arbitrage and limited liability.

Evidence is operationally dependent: Succession proof requires vendor attestations, live account access, or administrator cooperation—all of which depend on continuous operation of systems that may fail precisely when succession becomes necessary (corporate bankruptcy, natural disaster, cyber attack, regulatory shutdown). When vendors fail or refuse cooperation, proof disappears.

No portable verification standard: Each jurisdiction and each platform requires separate, incompatible proof formats. An executor with letters testamentary from a US state court must navigate different requirements for every platform, many of which won't accept US court orders at all. No universal mechanism exists for cross-border or cross-platform succession verification that different legal systems and platforms will recognize.

Cryptographic primitives expire: Evidence signed with RSA or ECC today becomes vulnerable to quantum computing attacks within decades. No systematic migration path exists to preserve legitimacy of succession claims across cryptographic generations. A cryptographically-signed succession claim from 2025 may become unverifiable by 2035 when quantum computers break RSA-2048.

1.4 The Governance Requirement

What digital inheritance actually requires:



1. **Succession policy declared in advance** – Before death, individuals specify beneficiaries, witness requirements, execution conditions, and asset mappings in a format that cannot be unilaterally altered post-death
2. **Structural enforcement** – Mathematical constraints preventing unauthorized succession claims, not reliance on platform discretion
3. **Witness diversity requirements** – M-of-N signatures with geographic and role separation preventing single-point compromise or collusion
4. **Tamper-evident execution recording** – Succession events recorded in append-only logs with cryptographic hash-chain integrity making alterations detectable
5. **Offline verification capability** – Courts and beneficiaries can recompute succession legitimacy without vendor cooperation, live systems, or ongoing platform operation
6. **Cross-border portability** – Succession proof valid across jurisdictions without requiring bilateral treaties or multiple probate proceedings
7. **Vendor-independent validity** – Evidence remains verifiable regardless of platform survival, corporate viability, or vendor cooperation
8. **Cryptographic agility** – Succession claims remain recomputable across cryptographic transitions (RSA → ECC → post-quantum)

This is not estate planning in the traditional sense of drafting wills and organizing physical assets. This is **constitutional governance** where succession authority becomes mathematically verifiable through structural constraints, not operationally attested through vendor discretion.

2. Legal and Governance Requirements for Digital Inheritance

2.1 Estate Authority: Sources and Limitations

Executor authority sources:

Testamentary appointment: Individual dies with valid will naming executor. Probate court issues letters testamentary granting authority to act on behalf of estate.

Administrator appointment: Individual dies intestate (no will). Probate court appoints administrator under statutory priority (typically spouse, then children, then other relatives).



ROOT ZERO VAULT

Trustee authority: Assets held in revocable living trust. Upon death, successor trustee assumes authority per trust instrument without probate court involvement.

Personal representative: Broader term encompassing executors, administrators, and trustees acting in fiduciary capacity for estate.

Critical limitation: All these authority sources are **legal**, not **technical**. Courts grant authority to act; they do not (and cannot) grant technical capability to access digital systems. An executor with letters testamentary possesses legal right to access decedent's email account but no technical means to compel Google's cooperation if Google refuses.

2.2 Conflict of Laws: Jurisdiction Complexity

Domicile vs. situs vs. platform jurisdiction:

Domicile: Where decedent was legally resident at death. Probate proceedings typically occur in domicile jurisdiction.

Situs: Physical location of asset. Real estate, vehicles, and tangible personal property have clear situs determining which jurisdiction's law governs.

Platform jurisdiction: Where digital platform is incorporated, where servers are located, where users reside. Often deliberately obscured through offshore incorporation, distributed systems, and jurisdictional arbitrage.

The digital asset problem: A US resident dies holding:

- Cryptocurrency in wallet controlled by Cayman Islands exchange
- Cloud storage with Luxembourg-based provider
- Domain names registered through Irish registrar
- Software repositories hosted on US servers owned by foreign corporation

Which jurisdiction's law governs? Which court has authority to compel access? Platforms invoke conflicting jurisdictions defensively: "We follow Luxembourg privacy law" (when US court issues order), "We require US court order" (when Luxembourg executor requests access).

2.3 RUFADAA: What It Grants and What It Doesn't



ROOT ZERO VAULT

The Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), adopted in most US states, provides executors statutory authority to access digital assets. However:

What RUFADAA grants:

- Legal authority for executors to request digital asset access
- Override of general terms of service prohibitions against account transfer
- Priority for user-directed succession instructions (in online tool, will, trust, power of attorney)

What RUFADAA does NOT grant:

- Technical means to access accounts without platform cooperation
- Authority over platforms operating outside RUFADAA jurisdictions
- Mechanism for cross-border enforcement
- Portable proof format platforms must accept
- Remedy when platforms refuse cooperation

Practical outcome: RUFADAA clarifies that executors *should* get access, but provides no enforcement mechanism when platforms refuse. It establishes legal right without technical capability.

2.4 Evidentiary Standards: Authenticity and Chain of Custody

Courts evaluating succession claims require evidence meeting standards for:

Authenticity: Proof that document is what it purports to be (e.g., actual will, not forgery)

Traditional approach: Witness testimony, notary attestation, original document examination, handwriting analysis

Digital challenge: Electronic signatures may become unverifiable when cryptographic primitives expire or key management fails

Chain of custody: Continuous accountability for evidence from creation through presentation

Traditional approach: Physical custody tracking, sealed envelopes, vault storage



ROOT ZERO VAULT

Digital challenge: Mutable logs can be altered retroactively; vendor attestations depend on continuous corporate existence

Business records exception: Documents created in ordinary course of business may be admitted despite hearsay rule

Traditional approach: Bank statements, medical records, corporate minutes

Digital challenge: Platform records are hearsay; platform witnesses may be unavailable or expensive to depose; records may be purged or irretrievable

The governance gap: Existing evidentiary standards assume:

- Physical documents that cannot be silently altered
- Witnesses available for testimony
- Custodians who maintain continuous possession
- Evidence that doesn't depend on technology requiring specialized verification

Digital succession claims violate all these assumptions. Constitutional trust infrastructure addresses this by making evidence **recomputable** rather than **custodial**.

2.5 What Constitutional Governance Provides to Legal Framework

RSBIS does not replace probate law or override statutory succession. Instead, it provides:

Verifiable proof supporting legal authority: Executor receives letters testamentary from probate court (legal authority) AND presents continuity bundle (mathematical proof of succession validity)

Portable evidence across jurisdictions: Single proof format verifiable by any court without requiring jurisdiction-specific legal proceedings

Recomputable authenticity: Instead of relying on notary attestation or witness testimony, succession validity is mathematically recomputable from cryptographic commitments

Durable chain of custody: Hash-chained journals provide tamper-evident custody tracking that survives vendor failure and corporate bankruptcy



ROOT ZERO VAULT

Admissible business records: Journal entries constitute self-authenticating records through cryptographic verification, not vendor testimony

The constitutional governance role: RSBIS sits beneath statutory law, providing mathematical infrastructure that makes legal authority technically enforceable. Courts retain full authority; they gain tools to verify succession claims independently of vendor cooperation.

3. Complete End-to-End Succession Walkthrough

3.1 Scenario: Cross-Border Estate with Cloud, Exchange, and IP Assets

Decedent profile:

- Name: Sarah Chen
- Domicile: United States (California)
- Assets: Cryptocurrency (Cayman exchange), cloud infrastructure (EU data centers), software IP (GitHub repositories), domain portfolio (international registrars)
- Family: Spouse (Beijing), two adult children (one in US, one in Singapore)
- Estate value: \$4.2M (60% digital assets, 40% traditional)

Challenge: Three jurisdictions (US, China, Singapore), five platform jurisdictions (Cayman, Ireland, Netherlands, US, various domain registrars), conflicting legal frameworks, no bilateral succession treaties.

3.2 Phase 1: Deed Creation (While Alive)

Action: Sarah creates Estate Deed declaring succession policy

Technical steps:

1. **Deed issuance request** submitted to Root Zero:

yaml

deed_request:

holder: Sarah Chen

type: Estate_Succession



ROOT ZERO VAULT

jurisdiction_primary: US_California

witnesses_required: 4-of-6

witness_diversity:

geographic: [US, China, Singapore]

role: [family, legal, financial]

2. Succession policy declaration:

yaml

succession_policy:

beneficiaries:

primary: Spouse_Beijing

contingent_equal: [Child_US, Child_Singapore]

execution_conditions:

death_attestation: M-of-N witnesses

witness_requirements:

minimum: 4

total: 6

geographic_diversity: min_2_jurisdictions

role_diversity: [family_2, professional_2]

asset_mapping:

crypto: Cayman_Exchange_Account

cloud: EU_Infrastructure_Tenant

ip: GitHub_Organization

domains: Portfolio_Registrar_List

3. Canonical representation:

- Policy serialized to canonical YAML (NFC Unicode, LF line endings, lexicographic key sorting)
- No YAML anchors, aliases, or comments
- Deterministic byte-for-byte representation

4. CVID commitment:



ROOT ZERO VAULT

BLAKE3 hash of canonical policy → cvid:blake3:a7f3e9...

5. Deed issuance:

- Root Zero generates unique identifier: RootZero0047
- Records CVID commitment binding policy
- Issues Deed to Sarah with immutable succession policy reference

Legal effect: Sarah now possesses structural Estate Deed declaring succession rules. Policy cannot be unilaterally altered post-death (immutability enforced through CVID commitment).

3.3 Phase 2: Witness Pre-Authorization (While Alive)

Action: Sarah designates six witnesses and obtains their cryptographic public keys

Witness selection (satisfying diversity requirements):

Witness	Role	Jurisdiction	Public Key
Spouse	Family	China (Beijing)	ed25519:pub:witness1
Child A	Family	US (California)	ed25519:pub:witness2
Child B	Family	Singapore	ed25519:pub:witness3
Attorney	Legal	US (California)	ed25519:pub:witness4
Accountant	Financial	US (California)	ed25519:pub:witness5
Bank Officer	Financial	Singapore	ed25519:pub:witness6

Technical recording:

- Each witness's public key recorded in Estate Deed
- Geographic diversity: 3 jurisdictions ✓
- Role diversity: 3 family, 1 legal, 2 financial ✓
- Minimum witness count: 6 total, 4 required ✓

Legal effect: Witness authorization is structural, not discretionary. Upon Sarah's death, exactly these witnesses (4-of-6 minimum) must cryptographically sign succession claim or it will be deterministically rejected.

3.4 Phase 3: Death Event and Attestation



ROOT ZERO VAULT

Event: Sarah dies in January 2026

Action: Witnesses provide cryptographic signatures attesting to death

Attestation process:

1. Death event canonicalized:

yaml

death_attestation:

deed: RootZero0047

decedent: Sarah Chen

date: 2026-01-15

jurisdiction: US_California

certificate: Death_Cert_CA_2026_xxxxx

2. Witness signatures collected:

- Spouse (China): sig:ed25519:witness1:3a7f... ✓
- Child A (US): sig:ed25519:witness2:8e2c... ✓
- Attorney (US): sig:ed25519:witness4:1b9d... ✓
- Accountant (US): sig:ed25519:witness5:9f4a... ✓

Count: 4 signatures (meets 4-of-6 requirement)

Geographic diversity: China (1), US (3) → 2 jurisdictions ✓

Role diversity: Family (2), Legal (1), Financial (1) → satisfies requirements ✓

3. Journal entry created:

yaml

journal_entry:

deed_id: RootZero0047

event_type: DEATH_ATTESTATION



ROOT ZERO VAULT

timestamp: 2026-01-20T14:32:00Z

canonical_payload_hash: cvid:blake3:8b3e...

witness_signatures: [sig1, sig2, sig4, sig5]

previous_entry_hash: blake3:e4d2...

entry_hash: blake3:7a9c...

Hash-chain integrity: Each journal entry includes hash of previous entry, creating tamper-evident chain.

Legal effect: Sarah's death is now structurally attested with 4 cryptographic signatures from geographically and role-diverse witnesses. This attestation is recorded in append-only Journal with hash-chain integrity.

3.5 Phase 4: Succession Execution

Action: Primary beneficiary (Spouse) receives structural authority

Validation process:

1. Succession request submitted:

yaml

succession_request:

deed: RootZero0047

beneficiary: Spouse_Beijing

authority_claim: Primary_Beneficiary_Per_Policy

supporting_evidence:

death_attestation: Journal_Entry_2026_01_20

witness_signatures: [4-of-6 verified]

policy_reference: CVID_a7f3e9...

2. Vault Logic validation (deterministic, bounded):

Predicate 1: Death attestation verified?

- Journal entry exists? YES



ROOT ZERO VAULT

- Timestamp valid? YES
- Result: PASS

Predicate 2: Witness requirements met?

- Signature count (4) >= Required (4)? YES
- Geographic diversity (2 jurisdictions) >= Min (2)? YES
- Role diversity satisfied? YES (family=2, legal=1, financial=1)
- All signatures cryptographically valid? YES
- Result: PASS

Predicate 3: Beneficiary valid?

- Claimed beneficiary (Spouse_Beijing) == Policy primary beneficiary? YES
- Primary beneficiary not predeceased? YES (no prior attestation)
- Result: PASS

Predicate 4: Policy unchanged?

- CVID of current policy (cvid:blake3:a7f3e9...) == CVID at Deed issuance? YES
- No post-death modification? YES
- Result: PASS

Validation outcome: ACCEPT

Reason code: None (successful validation)

3. Succession execution recorded:

yaml

journal_entry:

deed_id: RootZero0047

event_type: SUCCESSION_EXECUTION

timestamp: 2026-01-25T09:15:00Z

beneficiary: Spouse_Beijing

authority_transferred: Primary_Estate_Authority

asset_mappings: [crypto, cloud, ip, domains]



ROOT ZERO VAULT

validation_result: ACCEPT

previous_entry_hash: blake3:7a9c...

entry_hash: blake3:2f5e...

4. Registry receipt issued:

yaml

registry_receipt:

deed: RootZero0047

event: Succession_Execution

beneficiary: Spouse_Beijing

economic_finality: 2026-01-25T09:15:00Z

receipt_id: ADES_RZ0047_20260125

Legal effect: Spouse receives structural authority over estate assets. This authority is:

- Deterministically validated (not discretionary)
- Recorded in tamper-evident Journal
- Anchored in public Registry receipt
- Verifiable offline without vendor cooperation

3.6 Phase 5: Continuity Bundle Creation

Action: Complete succession proof packaged for cross-border verification

Continuity bundle contents:

yaml

continuity_bundle:

deed:

identifier: RootZero0047

holder: Sarah Chen (deceased)

succession_policy_cvid: cvid:blake3:a7f3e9...

policy_canonical_yaml: [embedded]

witness_public_keys: [6 keys embedded]



ROOT ZERO VAULT

journal_segment:

entries:

- death_attestation (2026-01-20)
- succession_execution (2026-01-25)

hash_chain: [entry hashes showing continuity]

registry_receipt:

receipt_id: ADES_RZ0047_20260125

economic_finality_timestamp: 2026-01-25T09:15:00Z

witness_signatures:

- witness1: sig:ed25519:witness1:3a7f...
- witness2: sig:ed25519:witness2:8e2c...
- witness4: sig:ed25519:witness4:1b9d...
- witness5: sig:ed25519:witness5:9f4a...

validation_logic:

vault_logic_version: v1.0

predicate_dag: [embedded deterministic rules]

signature_policy:

declared: ed25519-only

future_migration: ed25519+pqc dual (post-2028)

Legal effect: Spouse now possesses self-contained proof bundle enabling verification by any court in any jurisdiction without requiring:

- Platform cooperation
- Vendor attestation
- Live system access
- Additional legal proceedings



3.7 Phase 6: Cross-Border Court Verification (Singapore Dispute)

Scenario: Child B (Singapore) disputes succession, claims Spouse (China) is not legitimate beneficiary

Singapore probate court proceeding:

1. **Spouse presents continuity bundle** to Singapore court (no separate Singapore probate needed)
2. **Court performs offline verification:**

Step A: Policy authenticity

- Recompute canonical YAML hash → Compare to CVID commitment
- Result: `cvid:blake3:a7f3e9...` (matches) ✓
- **Verdict:** Policy is authentic, unchanged since Deed issuance

Step B: Death attestation validity

- Verify 4 witness signatures cryptographically using public keys in Deed
- Check geographic diversity: China (1), US (3) → 2 jurisdictions ✓
- Check role diversity: Family (2), Legal (1), Financial (1) ✓
- **Verdict:** Death properly attested per declared policy

Step C: Succession authorization

- Policy specifies primary beneficiary: `Spouse_Beijing`
- `Spouse_Beijing` presented succession claim
- No evidence of primary beneficiary predeceasing decedent
- **Verdict:** Spouse is authorized primary beneficiary per immutable policy

Step D: Hash-chain integrity

- Verify each journal entry includes hash of previous entry
- Recompute hashes: all match ✓
- No gaps or tampering detected
- **Verdict:** Journal integrity confirmed



ROOT ZERO VAULT

Step E: Registry finality

- Registry receipt shows succession executed 2026-01-25
- Economic finality timestamp recorded
- **Verdict:** Succession finalized with public anchor

3. Court ruling:

Singapore court determines:

- Succession policy is authentic (CVID verification)
- Death was properly attested (witness signature validation)
- Spouse is legitimate primary beneficiary (policy compliance)
- Succession was executed validly (deterministic validation recomputed)
- Evidence is tamper-evident (hash-chain integrity)

Court accepts Spouse's succession authority without requiring:

- Separate Singapore probate proceeding
- Platform testimony
- Vendor cooperation
- Translation of foreign court orders
- Bilateral succession treaty

Legal effect: Child B's dispute dismissed. Spouse's authority mathematically verified. Same continuity bundle could be presented to:

- US courts (for US-based assets)
- Chinese courts (for Chinese assets)
- Cayman courts (for cryptocurrency exchange)
- Any jurisdiction worldwide

All would reach same deterministic conclusion through offline recomputation.

3.8 What This Walkthrough Demonstrates

The end-to-end scenario proves:



ROOT ZERO VAULT

- ✓ **Cross-border succession without bilateral treaties** – Singapore court verified US decedent's succession to Chinese beneficiary using mathematical proof, not legal cooperation
- ✓ **Vendor-independent verification** – No platform testimony, cooperation, or attestation required
- ✓ **Offline recomputability** – Court verified legitimacy without live systems or online access
- ✓ **Dispute resolution through cryptography** – Contested succession resolved via mathematical validation, not evidence interpretation
- ✓ **Immutability enforcement** – Post-death policy manipulation prevented through CVID commitment
- ✓ **Witness diversity** – Geographic and role separation requirements structurally enforced
- ✓ **Tamper-evident chain** – Hash-chained journal entries prevent retroactive alteration
- ✓ **Portable proof** – Same continuity bundle valid across all jurisdictions

This is constitutional governance in practice: succession authority becomes mathematically verifiable rather than legally ambiguous.

4. What Constitutional Trust Infrastructure Does NOT Do

4.1 RSBIS Does Not Replace Courts or Statutory Law

What RSBIS provides:

- Mathematical proof of succession validity under declared policy
- Portable evidence format courts can verify deterministically
- Tamper-evident recording of succession execution
- Cryptographic validation of witness signatures

What RSBIS does NOT provide:



- Legal authority to override statutory succession law
- Jurisdiction to adjudicate inheritance disputes
- Ability to compel platform cooperation absent court order
- Replacement for probate court proceedings where legally required

The relationship: RSBIS sits beneath statutory law. Courts retain full authority to:

- Determine which jurisdiction's law applies
- Rule on succession disputes
- Interpret ambiguous provisions
- Invalidate fraudulent claims
- Override declared policies when they violate public policy

RSBIS provides evidence supporting these determinations, not verdicts replacing them.

4.2 RSBIS Does Not Compel Platform Cooperation

What RSBIS provides:

- Verifiable proof of succession authority
- Evidence platforms can validate independently
- Structural basis for executor's legal claim

What RSBIS does NOT provide:

- Technical ability to force platform access
- Authority to override platform terms of service
- Bypass of platform security measures
- Direct control over platform-custodied assets

The relationship: Executor presents continuity bundle proving succession authority. Platform can:

- Validate proof cryptographically and grant access (cooperation)
- Refuse cooperation and force court proceeding
- Be compelled by court order backed by mathematical proof

RSBIS strengthens executor's position by providing court-verifiable evidence, but doesn't eliminate platform discretion absent court intervention.



4.3 RSBIS Does Not Eliminate Fraud or Coercion

What RSBIS prevents:

- Unauthorized succession claims (insufficient witnesses)
- Post-death policy manipulation (CVID immutability)
- Forged witness signatures (cryptographic validation)
- Scope violations (structural beneficiary constraints)

What RSBIS does NOT prevent:

- Coercion of witnesses to sign fraudulent attestations
- Collusion among M-of-N witnesses
- Fraudulent death certificates
- Deception of decedent into declaring disadvantageous policy

The relationship: RSBIS provides same security as traditional probate (witness attestation, notarization) but makes it:

- Cryptographically verifiable
- Recomputable offline
- Portable across jurisdictions
- Tamper-evident through hash chains

Residual fraud risks exist in both systems. RSBIS reduces ambiguity and evidence disputes while maintaining equivalent anti-fraud protections.

4.4 RSBIS Does Not Guarantee Asset Recovery

What RSBIS provides:

- Proof of succession authority
- Portable evidence for asset claims
- Durable record surviving platform failure

What RSBIS does NOT provide:

- Recovery of lost passwords or private keys
- Resurrection of defunct platforms



ROOT ZERO VAULT

- Discovery of unknown assets
- Retrieval of permanently deleted data

The relationship: RSBIS proves WHO has authority over WHAT, but cannot recover assets that are:

- Technically inaccessible (lost encryption keys)
- Permanently destroyed (platform bankruptcy without backup)
- Unknown to executors (asset discovery still required)
- Custodied by uncooperative parties absent legal enforcement

RSBIS makes succession authority verifiable; it doesn't solve technical loss or make asset discovery automatic.

4.5 RSBIS Does Not Override Beneficiary Disputes

What RSBIS provides:

- Clear record of declared succession policy
- Deterministic validation of policy compliance
- Tamper-evident execution recording

What RSBIS does NOT provide:

- Resolution of ambiguous beneficiary designations
- Adjudication of "undue influence" claims
- Determination of beneficiary eligibility
- Interpretation of beneficiary intent

The relationship: If policy clearly specifies "Spouse_Beijing" as primary beneficiary and Spouse_Beijing executes succession validly, RSBIS proves compliance. But courts retain authority to:

- Determine if "spouse" means legal spouse or common-law partner
- Rule on claims of undue influence in policy creation
- Interpret ambiguous beneficiary descriptions
- Apply jurisdictional rules on beneficiary eligibility



ROOT ZERO VAULT

RSBIS reduces disputes over "what was declared" but doesn't eliminate disputes over "what was meant" or "was it valid."

4.6 The Proper Scope

Constitutional trust infrastructure provides **mathematical certainty about governance compliance**, not **legal certainty about all outcomes**.

RSBIS transforms questions like:

- ❌ "Did the decedent really intend this?" → ❌ Still requires legal interpretation
- ✅ "What policy was declared and committed?" → ✅ Mathematically verifiable
- ✅ "Were witness requirements satisfied?" → ✅ Cryptographically provable
- ✅ "Has policy been altered post-death?" → ✅ CVID immutability confirms
- ✅ "Can this be verified across borders?" → ✅ Recomputable offline proof
- ❌ "Should courts override this policy?" → ❌ Courts retain authority

This scoping is intentional. RSBIS provides infrastructure that makes legal determinations more certain, faster, and less expensive—but doesn't replace legal judgment where judgment is appropriate.

5. Canonical Succession Governance Specimens

5.1 Acceptance Specimens (Valid Succession Under Bounded Policy)

RootZero0240020400_SuccessionVault_US_Example

Demonstrates standard US estate succession with witness diversity and statutory compliance.

Key features:

- Decedent domiciled in US (California)
- 3-of-5 witness requirement (spouse, 2 adult children, attorney, accountant)
- Geographic diversity: 2 witnesses in different US states (California, New York)
- Role diversity: family (3), professional (2)



ROOT ZERO VAULT

- Beneficiary priority: spouse → children → grandchildren
- Asset mapping: cryptocurrency wallets, cloud storage, domain names

Validation:

- All witness signatures cryptographically verified ✓
- Geographic diversity (2 states) meets minimum (2 jurisdictions) ✓
- Role diversity (family + professional) satisfied ✓
- Succession policy conditions met ✓
- Journal records transfer with hash-chain integrity ✓
- Registry receipt anchors economic finality ✓

Outcome: ACCEPT. Spouse receives structural authority. Court can verify offline from continuity bundle without platform cooperation.

RootZero0240020401_SuccessionVault_UAE_Example

Demonstrates UAE estate succession with Sharia-compliant Islamic inheritance distribution.

Key features:

- Decedent domiciled in UAE
- 4-of-6 witness requirement (family, religious authority, legal counsel)
- Geographic diversity: witnesses in UAE, Saudi Arabia, Egypt (3 jurisdictions)
- Role diversity: family (2), religious (2), legal (2)
- Beneficiary distribution per Islamic law (sons, daughters, spouse with Quranic fractional shares)
- Asset mapping: business holdings, financial accounts, real estate tokens

Validation:

- 4 witness signatures verified (meets 4-of-6 requirement) ✓
- Sharia distribution ratios validated against declared policy ✓
- Geographic diversity (3 countries) exceeds minimum (2) ✓
- Role diversity (family + religious + legal) satisfied ✓



ROOT ZERO VAULT

- Journal records transfers with proper fractional allocations ✓
- Registry receipts anchor each beneficiary's specific share ✓

Outcome: ACCEPT. Distribution executed per declared Islamic law. Cross-border verification possible without bilateral treaties. Sharia courts in UAE, Saudi Arabia, and Egypt can independently verify legitimacy from single continuity bundle.

RootZero0240020402_InheritanceScenarioA

Demonstrates standard succession with contingent beneficiaries (primary beneficiary alive).

Key features:

- Primary beneficiary: spouse
- Contingent beneficiaries: adult children (equal shares if spouse predeceases)
- 2-of-4 witness requirement
- Asset custody: cryptocurrency wallets, cloud infrastructure, intellectual property

Validation:

- Spouse alive (primary beneficiary status active) ✓
- Children listed as contingent but not activated (policy conditions) ✓
- 2 witness signatures verified (meets 2-of-4 requirement) ✓
- Policy conditions satisfied ✓

Outcome: ACCEPT. Spouse receives full estate authority (primary beneficiary alive). Children retain contingent claims provable from same continuity bundle if spouse subsequently dies.

RootZero0240020403_InheritanceScenarioB

Demonstrates contingent succession activation (primary beneficiary predeceased).

Key features:



ROOT ZERO VAULT

- Primary beneficiary: spouse (predeceased)
- Contingent beneficiaries: 3 adult children (equal shares activated)
- 3-of-5 witness requirement (one witness deceased; policy allows N-1 upon witness death)
- Asset custody: digital business, SaaS subscriptions, customer databases

Validation:

- Primary beneficiary verified as predeceased (death attestation in Journal) ✓
- Contingent beneficiaries activated per policy ✓
- Witness requirement adjusted per declared policy (4-of-5 with one deceased) ✓
- Equal distribution to three children validated ✓
- Each child receives separate CVID for their one-third share ✓

Outcome: ACCEPT (three separate acceptances). Three children each receive one-third structural authority. Distribution mathematically verifiable. Each child's claim independently provable from continuity bundle.

RootZero0240020404_GlobalDefault

Demonstrates default succession policy application (no custom rules declared).

Key features:

- Decedent died without custom succession policy
- Global default policy: statutory succession per jurisdiction of primary residence
- 2-of-3 witness minimum (family + legal counsel)
- Asset mapping: standard digital accounts

Validation:

- Default policy automatically applied ✓
- Jurisdiction identified: US (California) ✓
- Statutory succession order applied: spouse → children → parents ✓
- Witnesses confirmed jurisdiction-appropriate application ✓
- Transfer recorded per California intestacy law ✓



ROOT ZERO VAULT

Outcome: ACCEPT. Statutory succession enforced structurally. Default policy prevented contested interpretation disputes. Court verification possible without custom policy ambiguity.

RootZero0240020405_SubsetInheritance

Demonstrates partial estate succession (bounded asset subsets with separate CVIDs).

Key features:

- Subset inheritance declared: cryptocurrency → child A, intellectual property → child B, cloud infrastructure → spouse
- 3-of-4 witness requirement
- Each subset receives separate CVID commitment
- Cross-subset transfers prohibited by policy

Validation:

- Subset definitions verified against declared policy ✓
- Child A receives cryptocurrency Deed authority (subset CVID: cvid:blake3:x1...) ✓
- Child B receives IP Deed authority (subset CVID: cvid:blake3:x2...) ✓
- Spouse receives cloud infrastructure Deed authority (subset CVID: cvid:blake3:x3...) ✓
- Cross-subset transfer attempts deterministically rejected (asset scope violation) ✓

Outcome: ACCEPT (three separate subset acceptances). Each beneficiary receives bounded authority limited to their declared subset. Prevents disputes over asset interpretation. Each subset independently verifiable. Cross-subset transfers structurally prevented.

5.2 Rejection Specimens (Invalid Succession Under Bounded Policy)

RootZero0240020410_InvalidSuccessionProof

Demonstrates deterministic rejection of succession claim with insufficient witness signatures.

Scenario:



ROOT ZERO VAULT

- Succession policy requires 3-of-5 witnesses
- Claimant provides only 2 valid signatures
- Third signature cryptographically invalid (wrong public key used)

Validation:

- Witness count (2 valid) < requirement (3 minimum) X
- Validation fails deterministically (bounded predicate evaluation)

Reason code: E-AUTH (authorization condition not met)

Outcome: REJECT. Insufficient witnesses. No succession authority transferred. Claimant cannot override structural requirement through legal argument or platform cooperation. Mathematical proof of non-compliance prevents dispute ambiguity.

Legal effect: Court presented with continuity bundle showing clear rejection reason. No need to evaluate witness credibility or intent—witness count mathematically insufficient regardless of other factors.

RootZero0240020411_PostHocSubsetRedefinition_Reject

Demonstrates rejection of post-death subset boundary manipulation attempt.

Scenario:

- Decedent declared subset inheritance: cryptocurrency → child A, intellectual property → child B
- After death, child B attempts to redefine subset to include cryptocurrency
- Redefinition requested via Journal entry submission

Validation:

- Subset definitions are immutable post-issuance per L-004 (Thin Law Cannot Change) X
- Post-hoc redefinition violates structural immutability X
- Original CVID commitment binds subset definition permanently X
- New CVID (with cryptocurrency included) ≠ Original CVID X



ROOT ZERO VAULT

Reason code: E-IMMUTABILITY (policy modification attempt detected)

Outcome: REJECT. Subset boundaries remain as originally declared and committed via CVID at Deed issuance. Child B receives IP authority only (subset CVID: cvid:blake3:x2...). Cryptocurrency remains exclusively with child A (subset CVID: cvid:blake3:x1...). Post-death manipulation prevented structurally through cryptographic commitment immutability.

Legal effect: Court can verify original CVID commitment, recompute hash of claimed "modified" policy, observe mismatch, and confirm modification attempt invalid—all without evaluating intent, interpreting language, or resolving factual disputes.

RootZero0240020412_GrandchildSubsetRedefinition_Reject

Demonstrates rejection of grandchild attempting to expand inherited subset scope beyond ancestral bounds.

Scenario:

- Decedent → Child A (subset: business assets only, CVID: cvid:blake3:b1...)
- Child A → Grandchild (attempts to claim full original estate including IP subset assigned to Child B)
- Grandchild claims lineage entitles broader authority than parent received

Validation:

- Grandchild lineage traces through Child A ✓
- Child A received bounded subset (business assets only, CVID: cvid:blake3:b1...) ✓
- Subset scope constraint inherited structurally ✓
- Attempt to claim Child B's subset (IP, CVID: cvid:blake3:b2...) exceeds ancestral authority ✗
- Lineage verification: Grandchild inherits from Child A's subset only, not original estate ✓

Reason code: E-SCOPE (scope violation; beneficiary attempts action outside inherited bounds)



ROOT ZERO VAULT

Outcome: REJECT. Grandchild receives only business asset authority inherited through Child A's bounded subset. IP subset (Child B's inheritance) remains outside scope. Lineage does not override declared policy constraints. Structural enforcement prevents inter-generational scope creep where grandchildren attempt to claim siblings' inheritances by invoking descent from original decedent.

Legal effect: Court can trace lineage structurally, verify Child A's subset CVID bounds, and confirm Grandchild's claim exceeds ancestral subset—preventing common "I'm a grandchild so I inherit everything" disputes through mathematical scope enforcement.

5.3 What These Specimens Demonstrate

The canonical succession governance specimens prove that constitutional infrastructure can deterministically enforce:

Acceptance (valid under policy):

- ✓ US statutory succession with witness diversity
- ✓ UAE Sharia-compliant distribution across jurisdictions
- ✓ Contingent beneficiary activation when primary predeceases
- ✓ Default policy application when no custom rules declared
- ✓ Subset inheritance with bounded authority per beneficiary
- ✓ Offline court verification without vendor cooperation

Rejection (invalid under policy):

- ✗ Insufficient witness count (mathematical proof of non-compliance)
- ✗ Post-death policy modification (CVID immutability enforcement)
- ✗ Scope expansion across generations (ancestral subset bounds inherited)

The validation properties:

- **Bounded:** Non-Turing predicate evaluation guarantees termination
- **Deterministic:** Same succession claim → same outcome always
- **Recomputable:** Offline verification from continuity bundles years later
- **Cryptographically tamper-evident:** Hash-chained journals detect alterations



- **Jurisdictionally portable:** Same proof valid across borders

This is succession-by-structure: authority becomes mathematically verifiable rather than legally ambiguous.

6. Economic Impact, Deployment Readiness, and Adoption Strategy

6.1 Scale of Addressable Problem

Asset value: Digital assets now constitute \$2.5 trillion in global estate value, growing exponentially as individuals and businesses digitize operations. By 2030, nearly all estates will include substantial digital components.

Affected families: Millions of families annually face digital inheritance challenges:

- 2.8 million deaths annually in United States alone
- 15-20% involve cross-border assets requiring international coordination
- 60-70% of estates now include digital assets requiring platform access

Orphaned assets: Billions in digital assets become permanently inaccessible when heirs cannot prove succession authority to platforms:

- Cryptocurrency wallets with lost keys: estimated \$140 billion globally
- Cloud storage accounts terminated: millions of accounts annually
- Domain names forfeited: valuable intellectual property lost
- Business systems inaccessible: ongoing operations disrupted

Legal costs: Probate and estate administration for digital assets:

- Average probate cost: \$5,000-\$15,000 for simple estates
- Complex cross-border estates: \$50,000-\$200,000+
- Platform-specific legal disputes: \$10,000-\$50,000 per platform
- Total annual costs: \$500 million to \$2 billion in digital inheritance friction

6.2 Constitutional Governance Impact



ROOT ZERO VAULT

Friction reduction:

Vendor dependency eliminated: Families prove succession authority mathematically rather than negotiating with each platform individually. Single continuity bundle replaces dozens of platform-specific processes.

Cross-border simplification: One proof valid across all jurisdictions eliminates multiple probate proceedings. Singapore court verifies US decedent's succession to Chinese beneficiary without bilateral treaty.

Timeline acceleration: Days instead of months/years. Deterministic validation replaces lengthy evidence interpretation and vendor coordination.

Dispute resolution: Contested successions resolved through cryptographic verification rather than protracted litigation over ambiguous evidence.

Cost reduction:

Probate fees decrease: Deterministic validation reduces attorney time spent gathering evidence and coordinating with platforms. Estimated 40-60% reduction in legal fees for digital asset components.

Platform coordination eliminated: No vendor negotiation costs, no platform-specific legal proceedings, no international coordination overhead.

Cross-border costs eliminated: Single continuity bundle vs. separate probate in each jurisdiction (typical cross-border estate: \$30,000-\$100,000 savings).

Dispute costs reduced: Mathematical proof vs. evidence interpretation reduces litigation duration and expense.

Access preservation:

Orphaned assets recovered: Structural succession proof enables recovery even when platforms fail to cooperate initially. Courts can compel cooperation backed by mathematical proof.

Platform shutdown resilience: Vendor bankruptcy doesn't destroy succession legitimacy. Continuity bundle provides proof independent of vendor survival.



Long-term verifiability: Decades later, courts can still recompute succession validity. Evidence doesn't depend on corporate memory or personnel availability.

6.3 Comparison: Traditional vs. Constitutional Digital Inheritance

Dimension	Traditional Probate	Constitutional Governance (RSBIS)
Authorization	Court letters testamentary	Structural Deed + continuity bundle
Proof format	Paper documents, court orders	Cryptographic commitment, hash chains, signatures
Verification	Each platform evaluates independently	Deterministic offline recomputation
Cross-border	Separate probate per jurisdiction	Single proof valid globally
Vendor cooperation	Required; platforms may refuse	Not required; structural proof supports court enforcement
Evidence durability	Paper records, mutable platform logs	Tamper-evident journals, recomputable offline
Timeline	Months to years per jurisdiction	Days (deterministic validation)
Cost	\$5K-\$200K+ depending on complexity	Minimal (Deed issuance, witness coordination)
Platform failure	Evidence lost	Continuity bundle survives vendor bankruptcy
Cryptographic migration	No path; evidence expires	Declared signature policies enable quantum-safe migration
Dispute resolution	Evidence interpretation, witness testimony	Cryptographic verification, deterministic validation
Legal authority	Granted by court	Granted by court; supported by mathematical proof

6.4 Hybrid Deployment Strategy (Incremental Adoption)

Constitutional governance can be adopted incrementally without requiring wholesale legal reform:

Phase 1: Supplementary evidence (Immediate value)



ROOT ZERO VAULT

Current state: Traditional probate continues normally

RSBIS addition: Executors create Estate Deeds and continuity bundles

Legal effect: RSBIS provides supplementary proof accelerating platform cooperation. When executor presents both letters testamentary AND continuity bundle, platforms can verify succession cryptographically, reducing friction.

Adoption barrier: Low. No legal changes required. Pure opt-in by individuals.

Value delivered: Faster platform cooperation, portable proof across platforms, reduced disputes.

Phase 2: Preferred evidence (Court recognition)

Legal development: Courts begin formally recognizing continuity bundles as admissible evidence

Probate process: Judges accept CVID commitments as proof of policy authenticity, witness signature validation as proof of attestation

Legal effect: RSBIS proof becomes prima facie evidence of succession authority, shifting burden to challengers

Adoption barrier: Medium. Requires judicial familiarity, possibly model court rules or practice standards.

Value delivered: Accelerated probate, reduced evidentiary disputes, cross-border recognition.

Phase 3: Primary authority (Legislative recognition)

Legal development: Jurisdictions update digital asset legislation to explicitly recognize structural governance



ROOT ZERO VAULT

Statutory language: "Succession authority validated through cryptographic commitment and deterministic policy evaluation shall be deemed sufficient proof of legitimacy absent contrary evidence"

Legal effect: RSBIS structural proof becomes legally sufficient; traditional probate becomes optional fallback

Adoption barrier: Higher. Requires legislative action, model law adoption (cf. RUFADAA rollout).

Value delivered: Legal certainty, uniform cross-border treatment, platform safe harbors.

Phase 4: Integrated governance (Platform adoption)

Platform development: Digital platforms integrate RSBIS validators directly into account access workflows

Technical effect: Platforms automatically verify succession claims; structural proof enables programmatic authority transfer

Legal effect: Succession becomes nearly automatic with mathematical proof; courts handle only disputed cases

Adoption barrier: Variable. Early adopters (crypto exchanges, cloud providers) vs. legacy platforms.

Value delivered: Seamless succession, minimal executor burden, reduced platform liability.

This phased approach enables:

- Immediate value (Phase 1) without waiting for legal reform
- Progressive adoption as evidence and trust accumulate
- Backward compatibility (traditional probate always remains option)
- Risk reduction (each phase builds on previous success)

6.5 Implementation Guidance by Stakeholder



ROOT ZERO VAULT

For estate planning attorneys:

Immediate actions:

1. Familiarize with RSBIS succession governance framework
2. Identify clients with substantial digital assets (>\$100K or business-critical)
3. Offer Estate Deed creation as premium service
4. Configure witness requirements (M-of-N, geographic/role diversity)
5. Generate continuity bundles for client safekeeping

Value proposition to clients:

- Cross-border succession without multiple probate proceedings
- Platform-independent proof reducing vendor dependency
- Dispute prevention through immutable policy
- Evidence surviving decades for beneficiary verification

Competitive differentiation:

- Attorneys offering structural governance gain advantage over traditional-only practitioners
 - Clients with complex digital estates willing to pay premium for verifiable succession
 - Reduced malpractice risk (clear evidence of policy declaration)
-

For probate courts:

Immediate recognition:

1. Accept continuity bundles as supplementary evidence
2. Train judges/clerks on CVID verification (recomputing hash from canonical policy)
3. Implement offline verification procedures (cryptographic signature checking)
4. Recognize witness diversity requirements as equivalent to notarization

Medium-term adoption:

1. Develop model court rules for RSBIS evidence admissibility
2. Create standardized verification procedures



ROOT ZERO VAULT

3. Train court staff on deterministic validation concepts
4. Coordinate with other jurisdictions on cross-border recognition

Long-term integration:

1. Integrate RSBIS validators into court case management systems
 2. Enable automated succession verification for uncontested cases
 3. Reserve judicial resources for genuinely disputed matters
 4. Participate in interstate/international recognition frameworks
-

For digital platforms:

Why platforms should adopt:

Liability reduction: Mathematical proof provides clear basis for granting/denying access; reduces discretionary judgment risk

Cost reduction: Automated validation vs. manual review of probate documents; customer support burden decreased

Cross-border service: Serve international users without jurisdiction-specific legal expertise

Competitive advantage: Platforms offering RSBIS succession attract users concerned about estate planning

Implementation path:

1. Deploy RSBIS validator conforming to specification
 2. Integrate succession claim verification into account access workflows
 3. Accept continuity bundles as authorization for estate access
 4. Generate platform-specific asset mappings bound to Estate Deeds
 5. Participate in cross-platform succession standards
-

For families and beneficiaries:



ROOT ZERO VAULT

Decedent preparation (while alive):

1. Create Estate Deed declaring succession policy
2. Designate witnesses (M-of-N with diversity)
3. Map digital assets to Estate Deed
4. Store continuity bundle securely (safe deposit, with attorney, encrypted backup)
5. Inform beneficiaries of Estate Deed existence

Post-death execution:

1. Collect witness attestations (death certificates + cryptographic signatures)
2. Submit succession claim with continuity bundle
3. Present to platforms for account access
4. If platform refuses, present to court with mathematical proof
5. Court compels cooperation backed by verifiable evidence

Value received:

- Vendor-independent access to deceased relatives' digital assets
- Cross-border succession without costly international proceedings
- Reduced timeline and legal fees
- Evidence surviving platform changes and vendor bankruptcies

6.6 Broader Infrastructure Value: Cross-Problem Generality

Digital inheritance demonstrates RSBIS solving one instance of a general governance problem: **deterministic validation of high-stakes actions under declared policy with permanent, recomputable evidence.**

The same constitutional infrastructure addresses fifteen other trillion-dollar problems:

- P01 – Secret Zero:** Trust initialization becomes structural, not operational
- P02 – AI Kill Switch:** Continuity survives platform blackouts
- P04 – Provenance Collapse:** Media/model lineage becomes recomputable
- P05 – Regulatory Fragmentation:** Uniform evidence grammar across jurisdictions
- P06 – AI Governance:** Action authorization with human oversight requirements
- P07 – Legacy System Wrapping:** Incremental adoption without rip-and-replace
- P08 – Cryptographic Horizon:** Declared signature policies survive quantum transitions
- P09 – Supply Chain Opacity:** Custody chain becomes mathematically verifiable



ROOT ZERO VAULT

- P10 – Financial Inclusion:** Mathematical identity without bank-issued credentials
- P11 – Research Integrity:** Reproducibility through tamper-evident lineage
- P12 – Refugee Identity:** Property rights preservation across borders
- P13 – Environmental Crime:** Carbon credit authenticity cryptographically provable
- P14 – Healthcare Interoperability:** Clinical record continuity without vendor trust
- P15 – Trade Finance Fraud:** Document authenticity deterministically validated
- P16 – Election Integrity:** Ballot verification with preserved secrecy

All sixteen problems use:

- Same validation checklist
- Same reject code taxonomy
- Same continuity bundle format
- Same offline recomputation protocol
- Same Eight Commandments (constitutional law)

This generality proves: RSBIS is not domain-specific estate planning technology. It is domain-general constitutional infrastructure for high-stakes institutional governance.

Digital inheritance is one application demonstrating that structural trust infrastructure addresses fundamental gaps in how institutions prove authority, preserve evidence, and verify legitimacy across jurisdictions and decades.

7. Conclusion

Digital inheritance is not an estate planning problem—it is a governance problem. The multi-trillion-dollar gap between legal authority and technical capability cannot be closed through better passwords, cooperative platforms, or incremental improvements to existing probate procedures.

Traditional probate assumes physical assets with clear jurisdictional boundaries and cannot be destroyed by corporate failure. Digital assets exist across borders on platforms with arbitrary policies, can vanish when vendors fail, and often lack ownership records independent of platform attestation. Executors possess legal authority courts cannot technically enforce against uncooperative platforms, especially those operating beyond jurisdictional reach.



ROOT ZERO VAULT

Constitutional trust infrastructure solves this through structural enforcement rather than operational cooperation:

Mathematical identity through bijective mappings enables succession without vendor-issued credentials.

Immutable policy via CVID cryptographic commitments prevents post-death manipulation.

Witness diversity through M-of-N signatures with geographic and role separation prevents single-point fraud.

Offline verification via continuity bundles enables courts to recompute legitimacy without vendor cooperation.

Jurisdictional portability through shared deterministic validation enables cross-border succession without bilateral treaties.

Cryptographic agility through declared signature policies ensures recomputability survives quantum transitions.

The Recursive Stage-Based Identifier System demonstrates these properties through:

- Six canonical acceptance specimens proving valid succession (US, UAE, contingent, default, subset)
- Three canonical rejection specimens proving invalid claims (insufficient witnesses, post-hoc manipulation, scope violations)
- Complete end-to-end walkthrough from policy declaration through cross-border court verification
- Explicit scoping of what constitutional governance does and does not do

RSBIS further demonstrates that digital inheritance shares constitutional infrastructure with fifteen other trillion-dollar problems. High-stakes institutional actions across domains—AI alignment, supply chain custody, refugee identity, research integrity, environmental accountability, healthcare records, trade finance, voting—all require the same governance property: **deterministic validation of actions under declared policy with permanent, recomputable evidence.**



ROOT ZERO VAULT

The choice facing estate planning professionals, courts, platforms, and families is whether to continue depending on vendor cooperation and ambiguous legal authority, or to adopt constitutional governance that makes succession mathematically provable.

Incremental adoption is possible immediately: individuals create Estate Deeds, executors present continuity bundles as supplementary evidence, courts recognize cryptographic proof, platforms integrate validators. No wholesale legal reform required for initial value delivery.

With structural trust infrastructure, digital inheritance becomes law-by-structure, not grace-by-vendor.

What remains is adoption.

Appendix A: Complete Specimen Catalog with Canonical Identifiers

Acceptance Specimens (Valid Succession):

- RootZero0240020400_SuccessionVault_US_Example
- RootZero0240020401_SuccessionVault_UAE_Example
- RootZero0240020402_InheritanceScenarioA
- RootZero0240020403_InheritanceScenarioB
- RootZero0240020404_GlobalDefault
- RootZero0240020405_SubsetInheritance

Rejection Specimens (Invalid Succession):

- RootZero0240020410_InvalidSuccessionProof
- RootZero0240020411_PostHocSubsetRedefinition_Reject
- RootZero0240020412_GrandchildSubsetRedefinition_Reject

All specimens are normative governance definitions from RootZero_RootZeroDeed V39 constitutional specification. Complete canonical YAML available in constitutional source document.



References

Cahn, N. R. (2011). Probate law meets the digital age. *Vanderbilt Law Review*, 67(6), 1697-1754.

Carroll, E., & Romano, J. (2010). *Your Digital Afterlife: When Facebook, Flickr and Twitter Are Your Estate, What's Your Legacy?* New Riders.

Darrow, J. J., & Ferrera, G. R. (2007). Who owns a decedent's e-mails: Inheritable probate assets or property of the network? *New York University Journal of Legislation and Public Policy*, 10, 281-320.

Hopkins, J. E., & Doyle, K. B. (2016). Digital assets and estate planning: Legal and practical considerations. *ACTEC Law Journal*, 42, 151-172.

Mazzone, J. (2008). Facebook's afterlife. *North Carolina Journal of Law & Technology*, 90, 1643-1686.

Uniform Law Commission (2015). *Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA)*.

Root Zero Vault, Inc. (2025). *RSBIS Constitutional Specification* (RootZero_RootZeroDeed V39). Available at: rootzerovault.com

Correspondence: deen.saleh@rootzerovault.com