ROOT ZERO VAULT

The Cryptographic Horizon Is a Governance Problem:

How Constitutional Infrastructure Preserves Digital Evidence Across Algorithm Transitions and Quantum Breaks

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

Every cryptographic system faces a temporal horizon: the moment when underlying algorithms break and historical evidence becomes unverifiable. Quantum computers will render RSA-2048, ECDSA, and Ed25519 signatures computationally forgeable—threatening trillions in digital contracts, property deeds, corporate authorities, and legal evidence. Current post-quantum migration strategies assume orderly transition before quantum breakthrough, but this assumption fails catastrophically if quantum computers arrive unexpectedly or if adversaries exploit the transition period to backdate forged signatures.

This paper demonstrates that the cryptographic horizon is fundamentally a governance problem requiring temporal legitimacy verification—where signatures remain legally valid under the cryptographic standards of their era, regardless of future algorithmic breaks, and where courts can distinguish legitimate historical signatures from quantum-era forgeries through declared policy rather than computational hardness.

We present the Recursive Stage-Based Identifier System (RSBIS)—a constitutional trust infrastructure addressing these requirements. RSBIS preserves evidence across cryptographic transitions through: (i) declared signature policies at issuance specifying valid algorithms and transition plans; (ii) temporal policy anchoring where verification uses era-appropriate cryptography regardless of current algorithm status; (iii) quantum backdating prevention through immutable policy declarations preventing post-hoc

algorithm substitution; (iv) multi-algorithm redundancy during transition periods reducing single-point cryptographic failure; (v) offline recomputability enabling courts to verify 50-year-old signatures under original policy declarations without trusting migration custodians.

We include normative governance specimens demonstrating deterministic acceptance of legitimate cryptographic transitions (Ed25519 → dual-mode → Dilithium3 with proper policy declarations) and deterministic rejection of cryptographic fraud (quantum backdating attempts, undeclared algorithm switches, post-hoc policy modifications). A complete end-to-end walkthrough traces corporate identity from 2024 Ed25519 issuance through 2030 dual-mode transition, 2045 quantum break, and 2074 court verification—proving 2024 signatures remain legally valid despite Ed25519 being computationally broken.

The contribution establishes that cryptographic agility is not merely technical algorithm rotation but constitutional temporal governance—courts verify legitimacy through declared historical policy, not current computational hardness. Digital evidence survives not because algorithms remain unbroken, but because governance anchors legitimacy to era-appropriate standards.

RSBIS further demonstrates that cryptographic horizon protection enables all fifteen other trillion-dollar problems—digital inheritance, supply chain custody, research integrity, healthcare records, environmental accountability—by ensuring evidence remains verifiable across the multi-decade timeframes these domains require.

---

1. Introduction: The $15+ Trillion Cryptographic Horizon Crisis

1.1 What Is the Cryptographic Horizon?

Definition: The cryptographic horizon is the temporal point when currently secure cryptographic algorithms break, rendering all historical signatures, certificates, and encrypted data unverifiable or compromised.

The threat:

Quantum computers break current cryptography:

- **Shor's algorithm** (1994): Efficiently factors large integers, breaks RSA
- **Shor's algorithm**: Solves discrete logarithm problem, breaks ECDSA (Elliptic Curve Digital Signature Algorithm), DSA, Diffie-Hellman
- **Grover's algorithm**: Weakens symmetric encryption (AES-256 → effective AES-128 security)

Current cryptographic deployment:

- **TLS certificates:** 95%+ use RSA-2048 or ECDSA (secp256r1)
- **Code signing:** Windows, macOS, Linux software signed with RSA/ECDSA
- **Digital signatures:** Contracts, legal documents, government records use RSA/ECDSA/Ed25519
- **Blockchain:** Bitcoin (ECDSA secp256k1), Ethereum (ECDSA secp256k1), most chains use quantum-vulnerable signatures
- **PKI infrastructure:** Entire certificate authority hierarchy based on RSA

Quantum timeline estimates:

- **2019:** Google claims "quantum supremacy" (disputed practical significance)
- **2023:** IBM 1,121-qubit quantum computer
- **2025-2030:** Optimistic estimates for cryptographically relevant quantum computers (CRQCs)
- **2030-2040:** Conservative estimates
- **2050+:** Skeptical estimates

Problem: We don't know when, but quantum computers WILL eventually break current crypto. Could be 5 years, could be 25 years. **Evidence must survive uncertainty.**

1.2 Scale of the Cryptographic Horizon Problem

Digital assets at risk:

Financial systems:

- **Global digital transactions:** $100+ trillion annually
- **Cryptocurrency:** $1.7 trillion market cap (Bitcoin, Ethereum—all quantum-vulnerable)
- **Digital securities:** $10+ trillion stocks, bonds, derivatives traded electronically
- **Banking records:** Every wire transfer, every account balance cryptographically signed

Legal evidence:

- **Digital contracts:** Trillions in electronically signed agreements
- **Property deeds:** Increasingly digitized (blockchain land registries in Georgia, Sweden, Honduras)
- **Corporate records:** Board resolutions, shareholder votes, M&A agreements
- **Court evidence:** Digital forensics, email authentication, document integrity

Government systems:

- **National identity:** Passports, driver's licenses, security clearances
- **Tax records:** IRS, national tax authorities store decades of signed returns
- **Military communications:** Classified documents, chain-of-command orders
- **Diplomatic cables:** International agreements, treaties

Healthcare:

- **Medical records:** HIPAA requires 30-year retention; all digitally signed
- **Prescription authenticity:** DEA-controlled substances require cryptographic verification
- **Clinical trial data:** FDA submissions, pharmaceutical R&D

Research & IP:

- **Patent applications:** USPTO requires cryptographic timestamps
- **Scientific data:** Research integrity depends on computational provenance
- **Software:** Every

open-source package, every proprietary codebase cryptographically signed

Conservative estimate: $15+ trillion in digital assets and legal evidence depend on cryptographic signatures that quantum computers will break.

1.3 Current Post-Quantum Migration Strategies and Their Failures

NIST Post-Quantum Cryptography Standardization (2016-2024):

NIST selected algorithms (2022-2024):

- **Signatures:** CRYSTALS-Dilithium (lattice-based), FALCON (lattice-based), SPHINCS+ (hash-based)
- **Key encapsulation:** CRYSTALS-Kyber (lattice-based)
- **Status:** Standardization finalized 2024; migration ongoing

Migration strategy: "Rotate keys to post-quantum before quantum computers arrive"

Why this fails:

1. The "harvest now, decrypt later" attack:

- Adversaries record encrypted traffic TODAY
- Store for years/decades
- When quantum computers available, decrypt all historical communications
- Affects: Government secrets, trade secrets, personal medical records, financial transactions

Migration timeline insufficient: Even if migration starts 2024, takes years to complete. Quantum breakthrough during migration = catastrophic failure.

2. The quantum backdating attack:

Scenario:

1. 2024: Alice signs contract with Bob using Ed25519
2. 2025: Bob breaches contract
3. 2045: Quantum computers break Ed25519
4. 2046: Bob claims contract forged—"prove signature legitimate"
5. Alice cannot prove signature predates quantum break

Even worse:

1. 2024: Alice signs contract using Ed25519
2. 2045: Quantum computer breaks Ed25519
3. 2046: **Bob forges NEW contract** with quantum computer, backdates to 2024
4. Bob presents forged contract claiming Alice agreed to unfavorable terms
5. **Court cannot distinguish legitimate 2024 signature from forged 2046 signature**

Both use same algorithm (Ed25519). Both computationally indistinguishable after quantum break.

3. The migration coordination problem:

- **Billions of systems:** Every website, every application, every device must migrate
- **Legacy systems:** 30-year-old medical devices, industrial control systems cannot update
- **Coordination impossible:** No centralized authority can force simultaneous migration

- **Partial migration = failure:** If 10% of systems stay on old crypto, adversaries target them

4. The "next horizon" problem:

- Post-quantum algorithms (Dilithium, FALCON) assumed secure against quantum computers
- But: What if new mathematical breakthrough breaks lattice-based crypto?
- What if quantum computers more powerful than expected?
- **Same problem repeats:** Evidence from 2024-2050 (post-quantum era) becomes unverifiable if post-quantum crypto breaks

1.4 Why This Is a Governance Problem, Not a Cryptography Problem

Traditional framing: "We need better quantum-resistant algorithms"

This framing fails because:

Perfect algorithms don't exist:

- Every algorithm eventually breaks (DES → 3DES → AES; MD5 → SHA-1 → SHA-256)
- Post-quantum algorithms are NEW (less battle-tested than RSA/ECDSA)
- Unknown unknowns: Mathematical breakthroughs unpredictable

Migration timing unknowable:

- Quantum timeline uncertain (5 years? 25 years?)
- Migration takes years (incomplete when breakthrough occurs)
- "Rotate before break" = **hope**, not **guarantee**

Historical evidence cannot be "fixed":

- 2024 contract signed with Ed25519 cannot be "re-signed" in 2045 (parties may be dead, hostile, bankrupt)

- Court in 2074 needs to verify 2024 signature, but Ed25519 broken
- **No amount of future cryptography helps past evidence**

The governance insight:

Don't try to prevent cryptographic algorithms from breaking. **Make legitimacy verifiable regardless of algorithm status.**

Critical scope distinction: This paper addresses **authenticity and legal legitimacy**, not **confidentiality**. Quantum computers may compromise encrypted data (revealing secrets), but constitutional governance preserves signature legitimacy (proving authority). Even if quantum computers decrypt all historical communications, they cannot forge pre-quantum policy declarations that anchor temporal verification.

Legitimate 2024 Ed25519 signature should remain LEGALLY VALID in 2074 even if Ed25519 computationally broken.

How? Through **declared temporal policy**: Court knows signature used Ed25519 in 2024 because signer DECLARED this policy at issuance. Policy declaration itself cryptographically committed (immutable). Quantum computer cannot backdate policy.

Requirements for temporal legitimacy:

1. **Signature policy declaration at issuance** – Algorithm explicitly declared; cannot be altered retroactively
2. **Temporal policy anchoring** – Verification uses era-appropriate cryptography; 2024 signature verified under 2024 standards, not 2074 standards
3. **Quantum backdating prevention** – Immutable policy declarations prevent adversaries from forging signatures and claiming they predate quantum break
4. **Multi-algorithm redundancy during transitions** – Dual-mode signing (Ed25519 + Dilithium3) reduces single-algorithm break risk
5. **Offline temporal verification** – Courts recompute legitimacy using historical policy without trusting migration custodians

6. **Constitutional continuity** – Legitimacy derives from declared policy structure, not computational hardness

---

2. The Mathematical Foundation: Temporal Legitimacy Through Declared Policy

2.1 Signature Policy Declaration at Issuance

RSBIS requires explicit cryptographic policy declaration when Deed issued:

yaml

```
deed_issuance_2024:
  identity: RootZero0892_TechCorp
  issuance_date: 2024-01-15

  signature_policy:
    mode: ed25519_only
    valid_from: 2024-01-15
    algorithm: ed25519
    public_keys:
      ceo: pubkey:ed25519:A7F3B2...
      cfo: pubkey:ed25519:9D4E1C...

    quantum_transition_plan:
      trigger: NIST_PQC_standardization_complete
      target_date: 2030-07-01
```

transition_mode: dual_mode

pqc_algorithm: dilithium3

Policy commitment:

policy_cvid: cvid:blake3:policy_2024_8f3a...

Critical property: Policy CVID is cryptographic commitment. **Cannot be altered** after issuance. Even if quantum computer breaks Ed25519, cannot modify policy CVID to claim different algorithm was used.

Legal effect: In 2074, court knows TechCorp used Ed25519 in 2024 because policy explicitly declared and cryptographically committed at issuance. Quantum computer breaking Ed25519 irrelevant—signature valid under 2024 standards.

2.2 Temporal Policy Anchoring

Verification uses era-appropriate cryptography:

Example signatures:

- Signature A: Created 2024-06-10, algorithm Ed25519
- Signature B: Created 2035-03-15, algorithm Dilithium3 (dual-mode)
- Signature C: Created 2055-11-20, algorithm Dilithium3 (PQC-only)

Year 2074 verification (Ed25519 broken by quantum computers):

Signature A verification:

Date: 2024-06-10

Declared policy at 2024: ed25519_only

Algorithm used: Ed25519

Verification approach: Ed25519 was VALID algorithm in 2024

Quantum status: Ed25519 broken in 2045 (irrelevant)

Legal validity: VALID (signature legitimate under 2024 standards)

Signature B verification:

Date: 2035-03-15

Declared policy at 2035: dual_mode (Ed25519 + Dilithium3)

Algorithms used: BOTH Ed25519 AND Dilithium3

Verification approach: Verify both signatures

Ed25519 verification: BROKEN (quantum computer)

Dilithium3 verification: VALID (post-quantum secure)

Legal validity: VALID (Dilithium3 signature holds)

Signature C verification:

Date: 2055-11-20

Declared policy at 2055: pqc_only (Dilithium3)

Algorithm used: Dilithium3 only

Verification approach: Dilithium3 verification

Legal validity: VALID (post-quantum signature)

Key insight: Signature A remains legally valid in 2074 even though Ed25519 computationally broken. **Legitimacy derives from declared policy, not current algorithm strength.**

2.3 Quantum Backdating Prevention

The attack RSBIS prevents:

Adversary's goal: Forge signature in 2045 (after quantum break), backdate to 2024 (before quantum break), claim legitimate.

Without declared policy:

1. 2024: Alice signs contract with Ed25519
2. 2045: Quantum computer breaks Ed25519
3. 2046: Bob forges signature using quantum computer, backdates to 2024
4. **Court cannot distinguish:** Both appear as "Ed25519 signatures from 2024"

With declared policy (RSBIS):

2024 legitimate signature:

yaml

```
signature_creation_2024:
  signer: Alice
  document: Contract_v1
  timestamp: 2024-06-10T10:00:00Z
  algorithm: ed25519
  signature: sig:ed25519:Alice:8F3A...

  policy_declaration:
    mode: ed25519_only
    declared_at: 2024-01-15
    policy_cvid: cvid:blake3:policy_2024_8f3a...
```

2046 forged signature attempt:

yaml

```
forged_signature_2046:
  signer: Bob_impersonating_Alice
```

document: Fraudulent_Contract

timestamp: 2024-06-10T10:00:00Z (BACKDATED)

algorithm: ed25519 (forged with quantum computer)

signature: sig:ed25519:Forged:7E2D...

policy_claim: "Used Ed25519 in 2024"

Court verification 2074:

Alice's legitimate signature:

- Policy declared 2024-01-15 (immutable CVID commitment)
- Policy CVID: cvid:blake3:policy_2024_8f3a...
- Journal entry 2024-01-15 records policy declaration
- Registry receipt 2024-01-15 provides economic finality
- **Cannot be forged:** Policy CVID committed before quantum computers existed

Bob's forged signature:

- Claims "used Ed25519 in 2024"
- But: No policy CVID from 2024
- Or: Policy CVID created 2046 (timestamp provable via Journal/Registry)
- **Forgery detected:** Policy declaration missing or backdated

Result: Court distinguishes legitimate 2024 signature (has immutable 2024 policy declaration) from forged 2046 signature (lacks pre-quantum policy commitment).

Quantum computers cannot forge policy CVIDs backdated to before quantum computers existed.

2.4 Multi-Algorithm Redundancy (Dual-Mode Signing)

During cryptographic transitions, use multiple algorithms simultaneously:

2030-2050 dual-mode period:

yaml

```
signature_policy_2030:
  mode: dual_mode
  valid_from: 2030-07-01
  algorithms: [ed25519, dilithium3]

  signing_requirement: BOTH_algorithms_required
  verification_requirement: EITHER_algorithm_sufficient
```

Signing process:

yaml

```
document_signing_2035:
  document: Corporate_Resolution_2035
  signer: CEO

  signatures:
    - algorithm: ed25519
      signature: sig:ed25519:CEO:4F7B...
    - algorithm: dilithium3
      signature: sig:dilithium3:CEO:9A2E...
```

both_required: true (signer must provide both)

Verification in 2074:

- Ed25519 signature: BROKEN (quantum computer)
- Dilithium3 signature: VALID (post-quantum secure)
- **Document remains valid:** One valid signature sufficient

Risk mitigation:

- If Dilithium3 unexpectedly breaks → Ed25519 signature still valid (under 2035 standards)
- If Ed25519 breaks (expected) → Dilithium3 signature holds
- **No single point of failure**

2.5 Offline Temporal Verification

Court in 2074 verifies 2024 signature without trusting custodians:

Continuity bundle contains:

1. **Original Deed (2024)** with signature policy declaration
2. **Journal entries** recording policy issuance, document signing
3. **Registry receipts** providing economic finality for policy and signatures
4. **Signature policy CVID** committed at issuance
5. **Public keys** (Ed25519) used in 2024

Verification steps:

1. Extract policy CVID from 2024 Deed

Policy CVID: cvid:blake3:policy_2024_8f3a...

2. Verify policy CVID committed in 2024

Journal entry: 2024-01-15 records policy issuance

Registry receipt: ADES_2024_01_15 anchors policy

3. Verify document signature under declared policy

Declared algorithm: ed25519_only

Public key: pubkey:ed25519:A7F3B2...

Signature: sig:ed25519:CEO:8F3A...

4. Apply temporal verification logic

Signature date: 2024-06-10

Algorithm status in 2024: VALID (Ed25519 secure)

Algorithm status in 2074: BROKEN (quantum computers)

Legal determination: VALID under 2024 standards

No operational dependency:

- Don't need TechCorp's cooperation (may be bankrupt)
- Don't need original servers (may be decommissioned)
- Don't need migration custodians (may be hostile)
- **Pure mathematical recomputation from continuity bundle**

---

3. End-to-End Cryptographic Transition Walkthrough

3.1 Scenario: Corporate Identity Across 50-Year Cryptographic Evolution

Timeline:

- **2024:** TechCorp issues Deed with Ed25519
- **2030:** Dual-mode transition (Ed25519 + Dilithium3)
- **2045:** Quantum computers break Ed25519
- **2050:** Full post-quantum migration (Dilithium3 only)
- **2074:** Court verifies 2024 contract

3.2 Phase 1: Initial Deed Issuance (2024 - Ed25519 Era)

TechCorp Deed creation:

yaml

```
deed_2024:
  identity: RootZero0892_TechCorp
  holder: TechCorp_Inc_Delaware
  issuance_date: 2024-01-15

  signature_policy:
    mode: ed25519_only
    valid_from: 2024-01-15
    algorithm: ed25519

    public_keys:
      ceo: pubkey:ed25519:A7F3B291...
      cfo: pubkey:ed25519:9D4E1C85...
```

required_signatures: 2-of-2 (CEO + CFO)

quantum_transition_plan:

trigger: NIST_PQC_standardization + 18_months

target_date: ~2030

transition_algorithm: dilithium3

transition_mode: dual_mode

Policy CVID commitment:

policy_cvid: cvid:blake3:techcorp_policy_2024_8f3a9d2e...

Why policy CVIDs cannot be backdated: Policy CVIDs are anchored in append-only Journals (hash-chained) with Registry receipts providing economic finality. Backdating a policy CVID would require breaking the hash chain from 2024 forward—provably impossible without altering all subsequent Journal entries. Quantum computers can forge signatures, but cannot rewrite immutable hash-chained history.

Journal entry:

yaml

journal_2024_01_15:

deed: RootZero0892

event: DEED_ISSUANCE

timestamp: 2024-01-15T10:00:00Z

signature_policy_declared: ed25519_only

policy_cvid: cvid:blake3:...8f3a...

quantum_plan: dual_mode_transition_planned_2030

entry_hash: blake3:issuance_4c2f...

Registry receipt:

yaml

registry_receipt_2024:

deed: RootZero0892

event: Initial_Deed_Issuance

economic_finality: 2024-01-15T10:00:00Z

policy_commitment: cvid:blake3:...8f3a...

receipt_id: ADES_RZ0892_20240115

Legal effect: TechCorp has cryptographically declared signature policy. Policy committed via CVID. Quantum computers cannot alter this declaration.

3.3 Phase 2: Contract Signing (2024 - Pre-Quantum)

TechCorp signs major supply contract:

yaml

contract_signing_2024:

parties: [TechCorp_Inc, SupplierCo_Ltd]

contract: 5_Year_Supply_Agreement

value: $500_million

date: 2024-06-10

techcorp_signatures:

ceo: sig:ed25519:CEO:8F3AB7...

cfo: sig:ed25519:CFO:4D2E9C...

declared_policy: ed25519_only (per Deed policy_cvid)

Journal entry:

yaml

journal_2024_06_10:

deed: RootZero0892

event: CONTRACT_EXECUTION

document_cvid: cvid:blake3:supply_contract_7e4a...

signatures: [CEO✓, CFO✓]

algorithm_used: ed25519 (per declared policy)

previous_entry_hash: blake3:issuance_4c2f...

entry_hash: blake3:contract_signed_9a3d...

Legal effect: Contract cryptographically signed with Ed25519 under declared policy. Evidence created 2024 (pre-quantum).

3.4 Phase 3: Dual-Mode Transition (2030)

NIST finalizes PQC standards; TechCorp transitions:

yaml

policy_update_2030:

deed: RootZero0892

event: CRYPTOGRAPHIC_POLICY_TRANSITION

timestamp: 2030-07-01T00:00:00Z

old_policy:

mode: ed25519_only

policy_cvid: cvid:blake3:...8f3a...

new_policy:

mode: dual_mode

algorithms: [ed25519, dilithium3]

valid_from: 2030-07-01

public_keys:

ceo_ed25519: pubkey:ed25519:A7F3B291... (SAME as 2024)

ceo_dilithium3: pubkey:dilithium3:3C8E4F... (NEW)

cfo_ed25519: pubkey:ed25519:9D4E1C85... (SAME)

cfo_dilithium3: pubkey:dilithium3:6A9B2D... (NEW)

signing_requirement: BOTH_algorithms

verification_requirement: EITHER_valid

transition_signatures:

ceo_old_key: sig:ed25519:CEO:2F7D... (signs with 2024 key)

ceo_new_key: sig:dilithium3:CEO:8A4E... (signs with 2030 key)

cfo_old_key: sig:ed25519:CFO:6C3A...

cfo_new_key: sig:dilithium3:CFO:9E1F...

Journal entry:

yaml

journal_2030_07_01:

deed: RootZero0892

event: CRYPTO_POLICY_MIGRATION

old_mode: ed25519_only

new_mode: dual_mode (ed25519 + dilithium3)

transition_signatures: 4_verified (2_algorithms × 2_signers)

policy_continuity: maintained (old policy remains valid for historical signatures)

previous_entry_hash: blake3:contract_signed_9a3d...

entry_hash: blake3:dual_mode_5e7b...

Critical property: Old policy (ed25519_only) **remains valid** for signatures created before 2030-07-01. New policy (dual_mode) applies to signatures after 2030-07-01.

Temporal policy table:

Date range | Policy mode | Verification algorithm

==========|==========|==========

2024-01-15 to 2030-06-30 | ed25519_only | Ed25519

2030-07-01 to 2050-12-31 | dual_mode | Ed25519 OR Dilithium3

2051-01-01 onward | pqc_only | Dilithium3

3.5 Phase 4: Quantum Breakthrough (2045)

Event: Quantum computer breaks Ed25519

Technical details:

- IBM announces 10,000-qubit quantum computer
- Researchers demonstrate Ed25519 signature forgery in 3 hours
- **All Ed25519 signatures computationally forgeable**

Immediate impact:

- Panic in cryptographic community
- Emergency migrations announced
- Legacy systems vulnerable
- **Historical signatures appear worthless**

RSBIS response: NONE REQUIRED

Why no panic:

- Historical Ed25519 signatures (2024-2050) remain **legally valid**
- Legitimacy determined by **declared policy**, not computational hardness
- Courts verify using **temporal policy anchoring**:
    - 2024 signature? Verify under ed25519_only policy (valid in 2024)
    - 2035 signature? Verify under dual_mode (Dilithium3 component still secure)
    - 2055 signature? Verify under pqc_only (quantum-secure)

TechCorp's 2024 contract:

- Computationally: Ed25519 signature forgeable (quantum computer)
- Legally: **STILL VALID** (signed under 2024 ed25519_only policy)

- Policy declaration: Immutable (committed 2024-01-15 via CVID)
- Quantum backdating: **IMPOSSIBLE** (policy CVID predates quantum breakthrough)

3.6 Phase 5: Full Post-Quantum Migration (2050)

TechCorp completes migration to PQC-only:

yaml

```
policy_update_2050:
  deed: RootZero0892
  event: FULL_PQC_MIGRATION
  timestamp: 2050-01-01T00:00:00Z

  old_policy: dual_mode (ed25519 + dilithium3)
  new_policy: pqc_only (dilithium3)

  ed25519_deprecation:
    effective_date: 2050-01-01
    historical_validity: PRESERVED (all pre-2050 Ed25519 signatures remain legally valid)
    new_signatures: Ed25519 no longer accepted
```

Journal entry:

yaml

```
journal_2050_01_01:
  event: ED25519_DEPRECATION
  new_mode: pqc_only
```

historical_preservation: all_pre_2050_signatures_valid_under_declared_policies

entry_hash: blake3:pqc_only_8d4f...

Legal effect: Going forward (2050+), only Dilithium3 signatures accepted. But: All historical Ed25519 signatures (2024-2050) remain legally valid under temporal policy anchoring.

3.7 Phase 6: Court Verification 50 Years Later (2074)

Legal dispute: SupplierCo claims TechCorp breached 2024 contract

Challenge:

- Original contract signed 2024-06-10 with Ed25519
- Ed25519 broken 2045 (29 years ago)
- TechCorp executives from 2024 deceased
- Original TechCorp acquired 2055, then bankrupt 2070
- Operational systems decommissioned

Traditional cryptography fails:

- Ed25519 computationally broken
- Cannot verify signature strength
- Cannot distinguish legitimate 2024 signature from quantum-forged signature
- No way to prove contract authentic

Constitutional governance succeeds:

Court obtains continuity bundle:

- 2024 Deed with signature policy declaration
- 2024-06-10 Journal entry recording contract signature
- 2024-06-10 Registry receipt (economic finality)

- Temporal policy table (ed25519_only from 2024-01-15 onward)

Verification process:

Step 1: Verify policy declaration legitimacy

Policy CVID: cvid:blake3:...8f3a...

Declared date: 2024-01-15

Journal entry: Exists, hash-chain valid

Registry receipt: ADES_RZ0892_20240115 (economic finality)

Quantum breakthrough: 2045 (21 years AFTER policy declared)

Conclusion: Policy declaration predates quantum computers ✓

Step 2: Verify contract signature under declared policy

Contract date: 2024-06-10

Declared policy at 2024-06-10: ed25519_only

Algorithm used: Ed25519

Signatures: CEO (sig:ed25519:8F3AB7...), CFO (sig:ed25519:4D2E9C...)

Public keys: Match 2024 Deed public keys ✓

Step 3: Apply temporal verification logic

Signature era: 2024 (pre-quantum)

Declared algorithm: Ed25519

Algorithm status in 2024: VALID (Ed25519 secure, quantum computers didn't exist)

Algorithm status in 2074: BROKEN (quantum computers exist)

Legal standard: Was signature valid under 2024 cryptographic standards?

Answer: YES ✓

Step 4: Check for quantum backdating

Could this signature be forged with quantum computer in 2045-2074?

Computationally: YES (Ed25519 broken)

Governance test: Does signature have pre-quantum policy declaration?

Policy CVID committed: 2024-01-15 (before quantum breakthrough)

Policy CVID alteration: IMPOSSIBLE (hash commitment immutable)

Conclusion: Signature legitimate (quantum backdating prevented) ✓

Court ruling: Contract valid. TechCorp signatures authentic. Breach enforceable.

What this demonstrates:

- ✓ Ed25519 computationally broken (2045) → irrelevant
- ✓ Signers deceased → irrelevant (no testimony needed)
- ✓ Company bankrupt → irrelevant (offline verification)
- ✓ 50-year verification → successful (temporal policy anchoring)
- ✓ Quantum backdating → prevented (immutable policy declaration)

3.8 Counterfactual: Attempt to Forge Contract with Quantum Computer

Adversary's goal: Forge contract in 2046, backdate to 2024, claim TechCorp agreed

Forgery attempt:

yaml

```
forged_contract_2046:
  parties: [TechCorp_Inc, AdversaryCo]
  contract: Fraudulent_Agreement
  claimed_date: 2024-06-10 (BACKDATED)
```

forged_signatures:

ceo: sig:ed25519:FORGED:7E2D... (created with quantum computer 2046)

cfo: sig:ed25519:FORGED:3A8F...

adversary_claim: "TechCorp signed this in 2024 with Ed25519"

Court verification 2074:

Step 1: Request policy declaration

Court: "What was TechCorp's signature policy in 2024?"

Adversary provides: Claims "ed25519_only"

Court: "Prove policy declared in 2024 with immutable commitment"

Adversary: Cannot provide policy CVID from 2024

Step 2: Check Journal/Registry for contract

Court searches TechCorp Journal for 2024-06-10

Legitimate contract: EXISTS (Journal entry blake3:contract_signed_9a3d...)

Adversary's contract: MISSING (no Journal entry from 2024)

Adversary claim: "Journal corrupted" or "entry deleted"

Court: Journal hash-chain integrity verifiable; no evidence of corruption

Step 3: Policy CVID verification

Legitimate contract references: policy_cvid:...8f3a... (from 2024-01-15)

Adversary's contract: No policy CVID reference, or references policy created 2046

Court: Policy CVID timestamp provable via Registry receipt

Conclusion: Adversary's policy declaration backdated (created after quantum breakthrough)

Court ruling: Forged contract rejected. Adversary's signatures lack pre-quantum policy commitment. Quantum backdating detected.

What this proves:

- Quantum computers CAN forge Ed25519 signatures computationally
- But: Constitutional governance DETECTS forgeries through policy declarations
- Immutable policy CVIDs cannot be backdated
- Temporal legitimacy preserved despite computational break

---

4. What Constitutional Cryptographic Agility Does NOT Do

RSBIS provides:

- ✓ Temporal legitimacy across algorithm transitions
- ✓ Quantum backdating prevention
- ✓ Offline verification 50+ years later
- ✓ Multi-algorithm redundancy during transitions
- ✓ Legal validity despite computational breaks

RSBIS does NOT provide:

- ✗ Perfect cryptographic algorithms (all algorithms eventually break)
- ✗ Prevention of "harvest now, decrypt later" attacks on CONFIDENTIALITY (signatures preserve AUTHENTICITY, not secrecy)
- ✗ Guaranteed quantum computer timeline predictions

- ✗ Automatic migration (organizations must declare policies and execute transitions)
- ✗ Protection against all side-channel attacks (implementation security separate from governance)

Proper scope: Preserves AUTHENTICITY and INTEGRITY evidence across cryptographic transitions. Does not solve CONFIDENTIALITY (encrypted data vulnerable to quantum decryption). Constitutional governance addresses "Was this signature legitimate?" not "Can this message be decrypted?"

---

5. Canonical Cryptographic Transition Specimens

Acceptance:

- RootZero0240020101_PQC_Upgrade_Path: Ed25519 → Dual-mode → Dilithium3 transition with proper policy declarations
- RootZero0240020902_Signature_Verification_Success: Multi-algorithm signature validated correctly
- RootZero0240020904_Cryptographic_Agility_Maintained: Temporal policy anchoring preserves 50-year-old signatures

Rejection:

- RootZero0240020913_Quantum_Backdating_Attempt: Forged signature lacks pre-quantum policy commitment → E-SIG
- RootZero0240020914_Undeclared_Algorithm_Switch: Signature uses algorithm not in declared policy → E-SIG
- RootZero0240020915_Post_Hoc_Policy_Modification: Attempt to alter historical policy declaration → E-IMMUTABILITY

---

6. Cryptographic Horizon Impact and Deployment

Scale: $15+ trillion digital assets and legal evidence depend on quantum-vulnerable cryptography

Impact:

- Legal evidence preserved across quantum transitions (contracts, deeds, credentials remain verifiable)
- Multi-decade verification enabled (courts verify 50-year-old signatures)
- Quantum backdating prevented (forged signatures detectable through policy declarations)
- Gradual migration supported (dual-mode reduces disruption)

Deployment:

Adoption is expected to begin in domains with longest evidence retention requirements:

- Phase 1: High-stakes legal evidence (property deeds, corporate governance, government records requiring 50+ year retention)
- Phase 2: Financial systems (contracts, securities, banking records with multi-decade dispute windows)
- Phase 3: Healthcare and research (medical records with 30-year HIPAA retention, research data integrity)
- Phase 4: General digital signatures (software signing, email authentication, certificate authorities)

Timeline depends on quantum computer development pace and institutional recognition of quantum backdating risk. Early adopters likely face litigation risk (contract disputes) or regulatory requirements (government contractors, financial services) where temporal verification provides material legal advantage.

7. Conclusion

The cryptographic horizon threatens to erase $15+ trillion in digital evidence when quantum computers break current algorithms. Traditional migration strategies assume orderly transition before quantum breakthrough—an assumption that fails catastrophically if quantum computers arrive unexpectedly or if adversaries exploit transitions to forge backdated signatures.

Constitutional trust infrastructure preserves evidence across cryptographic transitions through temporal legitimacy verification: signatures remain legally valid under their era's cryptographic standards, regardless of future algorithmic breaks. Declared signature policies prevent quantum backdating—adversaries cannot forge signatures and claim they predate quantum computers because policy declarations are immutably committed before quantum breakthrough.

RSBIS demonstrates that cryptographic agility is not merely technical algorithm rotation but constitutional temporal governance. Digital evidence survives not because algorithms remain unbroken, but because governance anchors legitimacy to era-appropriate standards.

This temporal layer enables all fifteen other trillion-dollar problems by ensuring evidence remains verifiable across the multi-decade timeframes they require.

Correspondence: deen.saleh@rootzerovault.com