SerenityVault Protocol™

Infrastructure de Civilisation | v7.65 TRINITY — March 2026

WHITE PAPER
Verifiable Digital Sovereignty Architecture

Infrastructure of Civilization — TRINITY v7.65

CLASSIFICATION :	CONFIDENTIAL — STRATEGIC
VERSION :	v7.65 TRINITY — March 2026
DATE :	March 2026
DESTINATAIRES :	Sovereign States, Sovereign Funds, Critical Institutions
DOCUMENT ID :	SV-WP-EN-v7.65-TRINITY

Jacques Desrosiers — Founder & CEO

info@serenityvault.com | www.serenityvaultprotocol.org

Quebec * Dubai * Geneve * Asuncion

EXECUTIVE SUMMARY

The Civilizational Problem

The Western cybersecurity model rests on an increasingly indefensible assumption: trust in centralized third parties. This assumption is collapsing under three structural failures:

- **Jurisdictional failure** — The U.S. CLOUD Act (2018) applies extraterritorially. Geographic sovereignty is a legal illusion.
- **Technological failure** — Classical cryptographic standards (RSA, ECC) will fall to quantum computing. Data intercepted today will be decrypted tomorrow ('Harvest Now, Decrypt Later').
- **Systemic failure** — The global CrowdStrike outage (2024) demonstrated that a single faulty update can paralyze the planetary economy.

The Response: The Proof Paradigm

SerenityVault does not sell trust. SerenityVault delivers mathematical proof, physical resilience, and existential continuity. The TRINITY v7.65 architecture is built on one non-negotiable postulate: the Internet can collapse, States can fail, classical encryption is condemned. This worst-case doctrine is not pessimism — it is the foundation of SerenityVault's strategic value.

SerenityVault is not a cybersecurity solution. SerenityVault is an infrastructure of civilization.

PART I — THE FAILURE OF THE TRUST PARADIGM

1. Jurisdictional Failure: The CLOUD Act

The Clarifying Lawful Overseas Use of Data Act (2018) enables U.S. authorities to compel access to data held by any U.S.-controlled entity, regardless of physical location. Geographic sovereignty becomes a legal fiction.

2. Technological Failure: Cryptographic Obsolescence

RSA and ECC algorithms — the pillars of modern encryption — will be broken by large-scale quantum computers. Sensitive data intercepted today can be stored and decrypted within 5 to 15 years. Deferred secrecy is a myth.

3. Systemic Failure: The Fragility of Centralization

The CrowdStrike outage of July 19, 2024 simultaneously paralyzed millions of critical Windows systems worldwide — hospitals, airports, financial institutions. A single defective update created a global systemic event. Technological monoculture constitutes a civilizational vulnerability.

PART II — THE PROOF PARADIGM

SerenityVault replaces blind trust with mathematical verification. Every commitment can be proven cryptographically. Every operation is auditable. Every decision is traceable.

PILLAR	DESCRIPTION
Mathematical Proof	Post-quantum hybrid cryptography (ML-KEM + ECC Curve25519, ML-DSA). Signatures cannot be forged even by a quantum computer.
Physical Resilience	Total Wide Web (TWW) hybrid Land/Space infrastructure. Continues to operate even through Internet collapse.
Existential Continuity	Worst-case doctrine. Engineered to sustain critical operations when everything else fails.

PART III — THE TRINITY v7.65 ARCHITECTURE

The TRINITY architecture rests on three sovereign AI systems integrated into a unified infrastructure. This constitutional separation of cognitive powers structurally prevents corruption or capture.

SYSTEM	ROLE	FUNCTION
ALFRED™	Defensive Protection	Critical infrastructure security. Autonomous threat response <100ms.
ADELE™	Governance & Compliance	Deterministic constitutional engine. 12 non-bypassable prohibitions. Permanent auditability.
ALADIN 360™	Tactical Intelligence	Informational superiority (C4ISR). Resilience in degraded environments.

Separation Principle — None of the three systems can act alone. None can corrupt the others. Every critical decision requires consensus. This tripartite architecture makes compromise structurally impossible.

NOUVEAU v7.65

TEE/HSM Material Anchoring (v7.65)

ADELE's 12 constitutional prohibitions are no longer mere erasable lines of code. They are physically anchored in the silicon via Trusted Execution Environments (TEE) and dedicated Hardware Security Modules (HSM). Any physical or software intrusion attempt triggers irreversible Zeroization. Corruption is not merely prohibited by software — it is blocked by physics.

PART IV — POST-QUANTUM HYBRID CRYPTOGRAPHY v7.65

1. Definitive NIST Standards 2024/2025

NIST STANDARD	ALGORITHM	USE	LEVEL
ML-KEM (FIPS 203)	Kyber-1024	Key encapsulation	Post-quantum 256-bit
ML-DSA (FIPS 204)	Dilithium-5	Digital signatures	Military grade
ECC Curve25519	X25519	Classical hybridization	Classical 256-bit

NOUVEAU v7.65

Military-Grade Hybrid Encryption

ML-KEM layered with ECC Curve25519. Intelligence agencies (NSA, ANSSI) recommend never entrusting security to a single post-quantum algorithm alone.

Strategic consequence: To break a secret protected by SerenityVault, an adversary must simultaneously possess a functional quantum computer AND break classical elliptic-curve cryptography in real time. The 'Store Now, Decrypt Later' attack becomes entirely inoperative.

2. Secure Multi-Party Computation (MPC) — The Key That Never Exists

NOUVEAU v7.65

MPC PRINCIPLE	DESCRIPTION	RESULT
Blind decryption	Quebec / Paraguay / Dubai servers jointly compute the authorization without ever exchanging key fragments.	Zero secret transmission
Key never materialized	The master key never materializes in full — not on disk, not in RAM on any server anywhere.	Absolute Deny Value
RAM scraper immunity	Mathematically impossible to steal a key that was never physically assembled.	State-grade attack rendered useless

3. Attack Response Matrix

ATTACK VECTOR	TRINITY v7.65 RESPONSE	STATUS
Physical server access	TEE + Zeroization — immediate destruction	**ACTIVE**
Novel post-quantum flaw	ML-KEM + ECC hybridization — dual independent lock	**ACTIVE v7.65**
RAM key theft	MPC — key never assembled anywhere	**ACTIVE v7.65**
State-grade quantum computer	ML-KEM + ML-DSA — native NIST resistance	**ACTIVE v7.65**
Operator corruption	3-jurisdiction consensus + constitutional ADELE TEE	**ACTIVE**
Sovereign Hub capture	Distributed architecture — zero single point of failure	**ACTIVE**

PART V — INSTITUTIONAL GOVERNANCE: THE TRIAD

HUB	ROLE	GUARANTEE
Protocol Foundation — Quebec (Non-profit)	Guardian of the protocol and ethics. Statutory protection mandate. Incarnation of ADELE.	Cannot be acquired. Cannot be corrupted. Golden Share = cryptographic rights over root certificates.
SerenityVault Alliance — Paraguay	Sovereign operational command. Outside NATO and Five Eyes jurisdictions. Total energy independence.	If an illegal order is issued, the only response is silence.
SerenityVault DMCC — Dubai	Commercial and financial vehicle. Interface with non-Western capital and markets.	Value circulates globally while the core remains sanctuarized.

> **Sovereign Triad Principle**
>
> SerenityVault's sovereignty is non-negotiable. Its strategic alignment with partner States is desirable. A partner State does not host SerenityVault to control it. It hosts it to benefit from it — that is the fundamental distinction.

PART VI — TOTAL WIDE WEB (TWW) — GLOBAL RESILIENCE

The World Wide Web relies on vulnerable undersea cables and centralized routing points. The Total Wide Web adds an independent spatial layer, creating a hybrid Land/Space infrastructure capable of surviving the collapse of the classical network.

TERRESTRIAL LAYER	SPATIAL LAYER
Distributed Sovereign Hubs	LEO/MEO/GEO constellations
Sovereign dark fiber	Inter-satellite links
Multi-jurisdictional data centers	Orbital points of presence
ML-KEM end-to-end encrypted private networks	Total independence from terrestrial infrastructure
25G SFP28 backbone — 10km inter-site	Starlink / sovereign satellite connection

No single Hub is critical. Destroying one Hub does not affect global integrity. The TWW network is designed to survive the loss of any component.

PART VII — GOVERNED ARTIFICIAL INTELLIGENCE

PROPERTY	DESCRIPTION
LLM-Agnostic Architecture	The client selects the AI engine (Falcon, DeepSeek, Llama, Kimi K2, or proprietary model). SerenityVault provides the armored chassis.
Constitutional Separation	ALFRED (power), ADELE (ethics), ALADIN (survival) cannot act in isolation. Every critical decision requires tripartite consensus.
Auditable Transparency	Every ADELE decision is immutably logged with ML-DSA signature. Third-party audits can verify ethical compliance.
Cognitive Sovereignty	AI models hosted locally. Zero external API dependency. Zero data exfiltration.

PART VIII — SOVEREIGN AUDIT KIT (SAK) — THE GLASS BOX

The SAK transforms the TRINITY architecture into a system fully verifiable by the client's national teams, with no dependency on external third-party auditors.

LEVEL	WHAT IS VERIFIED	OUTPUT
CODE (Static)	Source transparency, integrity before compilation	SHA3-512 hash, ML-DSA manifest
BUILD (Dynamic)	Deterministic compilation, exact binary correspondence	Sovereign compilation certificate
RUNTIME (Live)	Immutable logging, operational compliance	ML-DSA signed logs, constitutional proof

"A State that cannot audit its critical cybersecurity infrastructure is not sovereign. It is a tenant."

PART IX — TECHNICAL ADDENDUM v7.65

1. Material Anchoring of Constitutional Prohibitions (TEE & Zeroization)

ADELE's 12 constitutional prohibitions are anchored in dedicated TEE and HSM modules. Even a system administrator with root access cannot read or modify ongoing operations. Any physical intrusion, abnormal voltage variation, or silicon manipulation triggers immediate Zeroization. The machine prefers self-destruction to corruption.

2. Post-Quantum Hybrid Cryptography (Definitive NIST Standards)

NOUVEAU v7.65

> **Military-Grade Double Lock**
>
> ML-KEM layered with ECC Curve25519. To break a state-level secret, an adversary must simultaneously possess a functional quantum computer AND break classical mathematics in real time.

3. MPC: The Secret That Never Exists

Through MPC, servers jointly compute the authorization without ever exchanging key fragments. The master key never materializes — not on disk, not in RAM. It is mathematically impossible for a state-grade malware to steal a key that was never assembled.

CONCLUSION — A NEW STRATEGIC CATEGORY

SerenityVault is not a cybersecurity solution. It is an infrastructure of civilization — a system engineered to sustain critical operations when everything else collapses. Its value lies not in its code, but in its capacity to prove what others can only promise.

UNIQUE PROPERTY	STATUS v7.65
Independent network (TWW)	**Operational — Land + Space**
Incorruptible governance (ADELE)	**TEE/HSM + 12 constitutional prohibitions**
Post-quantum hybrid crypto	**ML-KEM + ML-DSA + ECC Curve25519 (NIST 2024)**
Keys never assembled (MPC)	**NEW v7.65**
Deny Value architecture	**Compromise = zero result**
Offline resilience	**ALADIN/ADELE/ALFRED degraded mode**
Multi-jurisdictional neutrality	**Quebec / Paraguay / Dubai**
Sovereign audit (SAK)	**Glass box — national verification**

"SerenityVault is desirable precisely because it is free. Any attempt at control destroys the value."