

LIBERION **Digital Citizenship & Trust Protocol** Verify once. Sign & Pay everywhere.

**SNFT Passports • One-click SSO • EDC Signatures • Crypto Payments • KYC/KYB/KYP & AML • Anti-Fraud • ZK & Post-Quantum**

---

## 0. Credo

For people, for businesses, for regulators — a single trust layer that lets you **verify once**, then **sign and pay everywhere** without re-uploading documents. Only **hash + signature + timestamp** are anchored on chain (“*No PII on-chain*”); original files stay with their owner (“*originals not retained*”). Security uses a **post-quantum-ready** stack with **ChaCha20-Poly1305, ML-KEM (Kyber), ML-DSA (Dilithium) / SLH-DSA (SPHINCS+)**.

---

## 1. Executive Summary

**LIBERION** is a human-centric **Digital Citizenship & Trust Protocol**. A person (or a company) completes verification once, receives a **non-transferable SNFT Passport**, and then reuses verified **attributes** across the internet: **one-click SSO**, **legally verifiable EDC e-signatures**, and **private payments**. Businesses onboard faster with lower fraud. Regulators get provable timelines without personal data exposure.

### What you get in practice

1. **SNFT Passport (non-transferable)**. Your proof-of-personhood (PoH) + proof-of-identity (Pol) in one reusable pass.
2. **Attribute SSO**. Share only what is needed (e.g., “is 18+” or “is company director”), either as a **ZK fact** or as a **consented off-chain field**.
3. **EDC Signatures**. Every signature anchors hash, your wallet signature, and a timestamp; the file stays encrypted under your control.
4. **Marketplace & Verified**. Get a verifiable badge for companies and projects; anyone can check status via public endpoints.
5. **Payments & LCL**. Sign & Pay with **concealed amounts/balances** and selective/ZK disclosures when required.
6. **Privacy by design**. Self-custody data, encrypted capsules (Private Docs & Files), **one-click consent & revocation**.

**Baseline metrics (deployment-ready):** onboarding via SSO **30–60 s**, conversion uplift **+15–25%**, network availability **99.9%**, SDK integration **1–2 days**.

## 2. The Problem & Market → Why LIBERION is Different

### The global identity paradox

- **Web2** makes users re-upload, re-verify and spread copies of sensitive documents, creating breach-prone silos.
- **Web3** often avoids identity altogether, which invites **Sybil/bot abuse** and weakens compliance.
- **Businesses** carry legal risk by storing personal data; **users** lose time and privacy; **regulators** lack trustworthy, addressable logs that do not expose PII.

**LIBERION’s answer: one reusable passport**, attribute-level SSO, **EDC** for provable events, and a **Consent/Revocation Ledger** that records who was allowed to see what and when — without placing personal data on chain.

[Table 1 — Approaches to digital identity]

| Approach          | What it solves         | Limitations                          | How LIBERION addresses it                                                            |
|-------------------|------------------------|--------------------------------------|--------------------------------------------------------------------------------------|
| Legacy KYC SaaS   | One-time checks        | Repeats per site; vendors retain PII | <b>SNFT Passport + attribute SSO</b> ; services get <b>facts</b> , not files         |
| SSI / DID wallets | Self-sovereign control | Often lacks regulated KYC/KYB/KYP    | <b>Verification Engine</b> with LoA (levels of assurance), AML/KYT                   |
| PoH-only          | Human-necessity        | No identity/AML completeness         | <b>PoH + PoI</b> with selective/ZK attributes + consent ledger                       |
| <b>LIBERION</b>   | Full trust layer       | —                                    | <b>“No PII on-chain”, EDC, Consent/Revocation Ledger, Marketplace &amp; Verified</b> |

**Plain English:** Use identity like you use a password manager — once set up, you reuse attributes safely across apps.

## 3. Vision — Nation of Trust

**Three foundations: Privacy by Design, Identity by Consent, Trust without Exposure.** People control their data (**self-custody**). Partners request only the **minimum necessary**.

Every important event — issuance, consent, signature, revocation — leaves a **verifiable on-chain anchor** (hash + timestamp), while personal data stays encrypted off-chain.

### Outcomes

- Less friction and fewer forms for people.
- Lower fraud and compliance workload for businesses.
- Auditable, privacy-respecting trails for regulators.

---

## 4. Digital Citizenship (PoH + Pol) and LoA

A **SNFT Passport** is a **soulbound, non-transferable credential** bound to a unique living person (PoH) and their verified identity evidence (Pol). It accumulates **attributes, roles, and attestations** from trusted verifiers.

Two interaction modes:

- **Selective/ZK proof:** disclose only a fact (e.g., “18+”).
- **Consented off-chain attribute:** disclose an agreed field (e.g., company name) while anchoring the consent event on chain.

[Table 2 — Levels of Assurance (illustrative)]

|             |                                        |                                      |
|-------------|----------------------------------------|--------------------------------------|
| L<br>o<br>A | Minimum checks                         | Typical use                          |
| L<br>0      | Account + soft liveness                | Communities & low-risk sign-ups      |
| L<br>1      | Phone/email + doc scan (MRZ/ICAO)      | Airdrops with anti-bot               |
| L<br>2      | Document + liveness + sanctions screen | Crypto services with limits          |
| L<br>3      | Video-KYC + address/IBAN proof         | Fintech & P2P platforms              |
| L<br>4      | eID/QES or notarial check              | Banks & public services              |
| L<br>5      | On-site/consular + multi-attestations  | High-risk finance & corporate access |

### User story (fast track):

1. Scan QR → quick liveness + document check.
2. Passport is issued as **SNFT**.

3. New website asks: “Are you 18+?” → you approve in Wallet → site gets **yes/no proof**; no document is shared.
- 

## 5. System Architecture (**Status → Next Milestones**)

### Five layers

1. **Core / PoA validators** — anchor **hash + timestamp** of key events (SNFT issuance/revoke, EDC signatures, consent/revocations).
2. **Identity** — SNFT, attributes, roles, attestations, and status history.
3. **Privacy & ZK with full off-chain PII** — proofs/minimum disclosure on request; full fields remain off-chain.
4. **Encrypted Storage (PQC)** — content encrypted with **ChaCha20-Poly1305**; keys wrapped with **ML-KEM (Kyber)**; signatures **ML-DSA/SLH-DSA**.
5. **App layer** — Wallet/Vault, **SSO/TrustGate**, EDC, Payments, Marketplace, SDK.

[Figure 1 — Five-layer architecture]

*Alt:* PoA (hash+timestamp) → SNFT/Attributes → Privacy&ZK + full off-chain → Encrypted Storage (ChaCha20-Poly1305) → Apps (Wallet/SSO/EDC/Marketplace).

**Invariants:** “No PII on-chain”; “originals not retained.”

### **Status → Next Milestones**

**Now:** PoA anchoring; SNFT & attributes; **Consent/Revocation Ledger**; EDC-MVP; PQC-hybrid.

**Next (Q1–Q2 2026):** ZK attribute selectors; key recovery/rotation; external audits.

**Later (H2 2026):** Rollup anchoring; public validator SLA dashboards.

---

## 6. Verification Engine (+ **Unified Data Policy**)

**What it does:** combines **KYC/KYB/KYP**, liveness/anti-spoof, **AML/KYT** and risk checks. It returns signed **attestations** to the SNFT/LoA ladder; only **hash/timestamps** of events are anchored.

### **Unified Data Policy**

- **Self-custody by default.**
- Optional encrypted **capsules** (Private Docs & Files) stored where the user chooses.
- **Delegation via EDC:** time- and scope-bound access; **one-click revocation**.
- No residency promises. **RCL (Regional Compliance Layer)** is a **B2B option** governed by DPA terms.

Legal groundings (Terms of Use & Privacy Policy) define controller roles, consent, eligible users and restricted access.

---

## 7. Wallet · SSO · TrustGate (Status → Next Milestones)

**Wallet/Vault** keeps your passport, attributes, and encrypted capsules.

**SSO** works in two modes — **minimal/ZK** (proof-only) and **consented off-chain** (share an agreed field).

**TrustGate** provides PoH gating / anti-Sybil at login (human-in-the-loop when needed).

**Reusable ID** enables co-branded identity for partner ecosystems.

[Figure 2 — Wallet & SSO sequence]

*Alt:* Service requests an attribute → user sees a consent screen in Wallet → approves → service gets ZK or off-chain field → event anchored → session opens.

(UI placeholder: Wallet/Vault consent screen.)

### Status → Next Milestones

**Now:** Attribute-SSO; Consent-UI; Duress mode (alpha).

**Next (Q1 2026):** Multi-device sessions; enterprise SSO mappings; **AppTree native clients**.

**Later (H2 2026):** Offline signatures; expanded roles.

**Result:** one-click sign-in that shares only what a service truly needs.

---

## 8. EDC Signatures & Consent/Revocation Ledger

**EDC** (Electronic Document Commit) anchors **document hash + your wallet signature + timestamp** on the PoA chain; the file itself stays encrypted in your capsule. Co-signatures are supported. A **Statement-NFT** is an optional read-only extract for auditable disclosures. Every grant/revoke of access is logged as a **Consent/Revocation** event (hash/time) without exposing PII.

**eIDAS-aligned essentials (plain language):** your key is under your control, signatures are unique to you, and any post-sign change invalidates the signature.

---

## 9. Security · Privacy · Compliance → 9.(next)

### Jurisdiction-Based Access Control

**Security & privacy by default:** only event anchors go on chain; **PII remains off-chain**; content encrypted with **ChaCha20-Poly1305**; keys/signatures **ML-KEM / ML-DSA / SLH-DSA**; selective/ZK proofs; all actions addressable via EDC/Consent events.

#### 9.(next) Jurisdiction-Based Access Control (J-BAC)

- **Purpose.** Economic features (e.g., Vault locking, Citizens' Yield, Referral rewards, DAO governance) are restricted by verified jurisdiction.
  - **Eligibility.** Only **non-EU / non-US** users (and outside other restricted jurisdictions) may access economic features.
  - **Non-Eligible Users.** Identity utilities (SNFT/SSO/EDC/Marketplace) stay available; **LBR rewards are not.**
  - **Automatic restriction.** Status changes trigger automatic closure of economic features and pending state for accruals; identity utilities continue.
  - **Disclaimer.** Vault, Citizens' Yield, etc. are **not offered** to residents/citizens of restricted jurisdictions and **are not** an investment, savings or interest product. DAO allocations from the **Fee Pool are discretionary.**
- 

## 10. Privacy Relay & Secure Communication

**Privacy Relay** provides contact-aliasing and encrypted channels so that partners can reach you without learning your real email or phone. Messages and actions remain addressable via EDC/Consent events, never disclosing PII on chain.

---

## 11. Payments & LCL (Layer of Concealed Ledger) (Status → Next Milestones)

**Purpose.** **LCL = Layer of Concealed Ledger** — a payment layer with **concealed amounts and balances**; participants can reveal to designated parties using selective/ZK proofs for audits or compliance. **Do not confuse with the consent ledger.** Consents live only in **Consent/Revocation Ledger**.

**Flows.** Sign & Pay in Wallet → anchor facts on PoA; amounts/balances stay private on LCL and are visible only to participants or when selectively disclosed. PII stays off-chain; EDC proofs ensure verifiability.

### Status → Next Milestones

**Now:** Baseline payment flows + event anchoring; LCL preparation for amount/balance concealment.

**Next (H1–H2 2026):** ZK proofs for amounts/balances; donation/escrow routing; private statements.

**Later:** Public SLA for merchant gateway; expanded networks and stablecoins.

---

## 12. Marketplace & Verified (*with public endpoints*)

**Marketplace & Verified.** Companies and projects pass KYB/KYP and receive an **on-chain certificate** and a **Verified by LIBERION** badge for their site/app. Anyone can check the status — PII-free — by verifying signature/hash/timestamp.

**Public verification URL templates:**

- **Sites:** [Liberion.com/s/<token>](https://liberion.com/s/<token>)
- **Projects:** [Liberion.com/p/<token>](https://liberion.com/p/<token>)
- **Businesses:** [Liberion.com/b/<token>](https://liberion.com/b/<token>)

(UI placeholder: **Check certificate/badge** button on a company profile. Clicking opens the relevant /s/, /p/, or /b/ route.)

---

## 13. Hybrid Trust Economy (**LIBERCOIN (LBR)** — short)

**LIBERCOIN (LBR)** is the network's **native utility coin**. Supply is **fixed**; with every SNFT issuance, a portion of LBR is **permanently locked**, creating **structural deflation**. The **Fee Pool** routes value **40/30/10/10/10** across Citizens' Yield / Buyback-&-Burn / Referral / Treasury & Compliance / Ecosystem Grants. Validators are compensated via licenses/KPI grants; deposits are used only for **slashing** (penalties → burn).

**No yield promises.** See §9.(next) for jurisdictional restrictions. Detailed economics live in **Liberonomics**.

---

## 14. Roadmap **2019–2028** (tracks: **PQC / LCL / Verifier / SLA**)

- **2019–2024:** AI & KYC core.
- **Q1 2025:** PoA network live.

- **Q2 2025:** SNFT/MVP.
- **Q3–Q4 2025:** Marketplace & Consent.
- **2026:** Payments, Privacy Relay, **AppTree** clients.
- **2027–2028:** Large-scale integrations and DAO hardening.

[Figure 3 — Roadmap 2019–2028]

*Alt:* Timeline with four horizontal tracks (PQC/LCL/Verifier/SLA) and the milestones listed above.

---

## 15. Pricing & KPI/SLA · Glossary · CTA

**Pricing (baseline).** KYC **\$0 / \$0.10 / \$0.20**; KYB **\$10**; KYP **\$5**; AML/KYT — **on request**.

**KPI/SLA (baseline).** SSO **30–60 s**; conversion **+15–25%**; PoA uptime **99.9%**; SDK integration **1–2 days**.

**Glossary (short).**

**SNFT Passport** — a soulbound, non-transferable digital passport.

**EDC** — Electronic Document Commit (hash + signature + timestamp).

**Consent/Revocation Ledger** — off-chain processes with on-chain anchors for who/what/when.

**LCL** — Layer of Concealed Ledger (concealed amounts/balances; selective/ZK proofs).

**RCL** — Regional Compliance Layer (B2B option under DPA terms).

**TrustGate** — SSO/anti-Sybil gate that keeps bots out.

**CTA.** Get your Digital Passport today: **Scan QR → Sign & Pay everywhere**.

**Export.** PDF in **Light** and **Dark** modes (WCAG AA contrast), accessible alt-texts, clickable table of contents.

---

## Appendix — Legal & Compliance Notices (Plain Language)

- **Privacy by design:** No personal data is written to the blockchain; only hashes, signatures, and timestamps.
  - **Original files:** LIBERION does not retain originals; encrypted copies remain under the user’s control.
  - **Jurisdictional restrictions:** Economic features are unavailable to users in restricted jurisdictions (e.g., EU/US). Identity utilities remain available.
  - **Not an investment product:** LIBERCOIN features do not constitute savings, interest, or investment offerings. DAO allocations are discretionary.
-