TECHNICAL ARCHITECTURE

The cryptographic core that powers sovereign identity, private communication, the anonymous bank layer, and the ENTIFY meshnet.

ENTIFY is a unified sovereign operating system. Behind the simple user experience lies a layered, modular cryptographic architecture designed to be maximally secure, decentralised, and legally compliant — while preserving the user's anonymity, autonomy, and rights.

This page explains how ENTIFY works under the hood:
the data flows, the components, the cryptographic layers, and the integration pathways with Solana, Reticulum Meshnet, Elerium hardware, and the Internal Private Clearing (IPC) banking layer.

1. Identity Layer — The Sovereign Identity Vault

At the foundation of ENTIFY is the Identity Vault: a cryptographically sealed Solana-based identity container that holds:

- Biometric hash bundle (voiceprint, faceprint, signature, gait, optional DNA key)
- Affidavit identity record
- Legal KYC bundle (encrypted, user-controlled)
- Assigned sovereign identity DID
- Private trust metadata
- Elerium keypair (hardware-rooted private keys)

The Vault is built on a hybrid architecture:

1.1 Solana + Elerium Hardware Keypair

- The private keys for the identity vault are generated inside the Elerium Secure Element (on Enticard, Entifone, or Entitag).
- Keys never leave hardware.
- Solana is used for:
    - State persistence
    - Timestamping
    - Identity proofs

- Token rails
- Secure programmatic execution

This creates a triple-proof identity:

1. Life-affirmation affidavit
2. Biometric cryptographic binding
3. Hardware-rooted private key control

1.2 Zero-Knowledge Biometrics

ENTIFY never stores raw biometrics.
Only irreversible ZK-biometric hashes are stored.
Biometrics can prove who you are without ever revealing your data.

1.3 KYC-in-the-Vault

A global first:

- ENTIFY stores KYC encrypted inside the user's own vault.
- IPC verifies KYC but cannot access it.
- Regulators receive proofs-on-request, never identity dumps.

2. Sovereign Trust Layer — The Private Trust Engine

Every identity vault automatically generates a self-sovereign digital trust structure:

- The user becomes the living grantor and beneficiary.
- The vault identity becomes the trustee authority.
- IPC becomes the public-facing administrator.
- All assets held by the user (digital or physical) become allodially owned trust property.

This system creates:

- A non-seizable identity
- A non-forfeitable property structure
- A legal firewall between the user and external jurisdictions

It meets requirements of:

- Trust law
- Property law
- Contract law
- Digital asset frameworks
- International private law

3. Communication Layer — Reticulum Mesh + Identity Vault

ENTIFY integrates Reticulum Meshnet, enhanced with identity-anchored routing and sovereign cryptography.

3.1 Proofless Routing

- No blockchain consensus needed for message passing
- Instead uses identity-bound routing signatures
- Reduces latency, increases privacy, removes dependency on internet

3.2 Cross-Layer Encryption

Every message is secured by:

1. Hardware keypair (Elerium)
2. Vault keypair (Solana)
3. Application ephemeral keypair

This creates a 3-layer quantum-resistant tunnel.

3.3 Anti-Coercion Mode

If the user is forced to unlock the device:

- A “decoy vault” opens
- True identity and communications stay hidden
- Meshnet triggers emergency broadcast with:
    - Location triangulation
    - Audio/video evidence
    - Timestamped chain proof

4. Financial Layer — The Internal Private Clearing (IPC)

Anonymous, legal, compliant finance.

ENTIFY uses a three-tier privacy architecture:

4.1 Layer 1 — Public (IPC Ltd)

- A normal UK-registered admin company
- Holds standard bank accounts
- Provides VISA/Mastercard integration
- Has compliance officers and AML processes

4.2 Layer 2 — Private (Allodial Reserve Trust)

- A private administrative trust
- Holds aggregate balances
- Contains no personal data
- Exists purely as a clearing entity

4.3 Layer 3 — Sovereign Identity Vault

- Stores user KYC and identity
- Controls user's actual ownership
- Is anonymous to the banking partner
- Issues ZK-payment authorisations

This creates the world's first legal anonymous bank account, compliant yet sovereign.

5. Device Layer — Enticard, Entifone, Entitag

5.1 ENTICARD

- NFC cryptographic card
- Contains Elerium Secure Element
- Stores identity private keys

- Used for authentication, asset-tagging, IPC payments
- Functions offline

5.2 ENTIFONE

(Phase 2 hardware)

- Hardened AOSP or VollaOS
- Reticulum mesh integration
- Native identity vault
- Hardware offline mode
- Direct mesh communication
- Child-safety proximity features
- Secure element integration

5.3 ENTITAG

- Tiny hardware token
- Tags physical assets
- Enables proof-of-ownership
- Supports allodial asset logging
- Can be added to vehicles, safes, gold, land deeds

6. Blockchain Layer — Solana Integration

ENTIFY uses Solana as the state backbone for:

- Identity vault indexing
- Timestamping affidavits
- Asset proofs
- IPC payment authorisations
- ENToken issuance circuitry
- Trust metadata
- ZK challenge-response proofs

- Meshnet root-of-truth anchoring

Why Solana?

- Extremely fast
- Extremely cheap
- High throughput
- Durable state
- Proven infrastructure
- Enterprise partnerships
- Growing ecosystem

ZK-Solana Bridge

ENTIFY generates:

- Zero-knowledge identity proofs
- Zero-knowledge asset proofs
- Zero-knowledge KYC confirmation

These enable:

- Anonymous payments
- Legal compliance
- Trusted interactions between sovereign users

7. Storage Layer — Entinet Decentralised Storage

ENTIFY devices create an alternative decentralised internet:

- User devices pool storage into Entinet
- Works like IPFS + meshnet + identity signing
- Data is sharded, encrypted, and backed by hardware identity
- Supports:
    - Backups

- Documents
- Media
- Affidavits
- Evidence in emergencies
- Community data

Over time Entinet becomes a self-owned global information layer, independent of Big Tech infrastructure.

8. Protection Layer — Sovereign Defence System

ENTIFY embeds the world's first cryptographically-verified personal protection network:

- Real-time mesh triangulation
- Emergency broadcast to trusted nodes
- Automatic evidence recording
- Tamper-proof chain anchoring
- Trust-law and affidavit-based rights protection
- Anti-coercion vault
- Court-ready data packets

This creates a civil rights shield, backed by cryptography rather than government permission.

9. Governance Layer — ENTLAND (Future)

A living digital nation emerging from cryptographic trust.

ENTIFY lays the foundations for ENTLAND — a voluntary, distributed, sovereign digital jurisdiction.

Features include:

- Self-issued identity
- Self-administered trust structure
- Community-based justice

- Mesh-anchored communication
- A gold-anchored stable currency
- A voluntary opt-in governance model
- Digital passports
- Land trusts
- Home jurisdictions
- Inter-jurisdictional interoperability

10. Architecture Summary Diagram (Text Version)

[User]
  ↓ (affidavit + biometrics)
[Identity Vault — Solana + Elerium SE]
  ↓
[Private Trust Engine]
  ↓
[Communication Layer — Reticulum Mesh]
  ↓
[Financial Layer — IPC + Allodial Reserve]
  ↓
[Device Layer — Enticard / Entifone / Entitag]
  ↓
[Storage Layer — Entinet Decentralised Storage]
  ↓
[Governance Layer — ENTLAND (future)]

Conclusion

ENTIFY is not simply an app. It is an integrated operating system built from first principles: identity, trust, communication, finance, asset-ownership, and protection — unified into a single sovereign architecture.
A system that does not depend on any one company, government, or server.
A system secured by mathematics, bound by trust law, and owned by its users.