Concept Paper

Title

Human-Sovereign Privacy & Security PCB (HSP-PCB)
A User-Owned Root-of-Trust Hardware Module for Present and Future Smart Devices

---

1. Executive Summary

Modern smartphones and smart devices have become compulsory interfaces to society, economy, and governance. Despite promises of privacy and consent, most devices continuously extract data, enforce persistent connectivity, and rely on opaque software and network infrastructures controlled by vendors, telecommunications companies, and states. This has resulted in widespread loss of trust, rising mental stress, financial burden (airtime and data costs), and repeated data breaches.

The **Human-Sovereign Privacy & Security PCB (HSP-PCB)** is proposed as a **small, flat, low-power, and affordable hardware module** that restores **human control at the hardware level**. It functions as a **user-owned root of trust** that enforces identity sovereignty, hardware-level consent, data minimization, and secure recovery — independent of the phone operating system, applications, network generation, or vendor policies.

The HSP-PCB is not an "anti-government" or "anti-network" device. It is a **post-surveillance, human-centered infrastructure component** designed to respect human dignity, mental well-being, environmental sustainability, and long-term digital sovereignty.

---

2. Problem Statement

2.1 Structural Failure of Digital Privacy

- Most devices collect data with or without meaningful consent.
- Consent is coerced through exclusion, urgency, and dependency.
- Software-based security is bypassable via recovery modes, firmware updates, or vendor backdoors.
- Persistent identity and continuous connectivity create permanent exposure.

2.2 Human and Social Harm

- Data leakage and resale cause reputational, financial, and psychological harm.

- Airtime and data costs disproportionately affect users in low- and middle-income regions.
- Constant notifications and connectivity contribute to anxiety and cognitive overload.
- Device theft leads to irreversible loss of personal and life-critical data.

2.3 Trust Collapse

Users increasingly distrust: - Phone manufacturers - App developers - Cloud providers - Telecommunication companies - Long-term data promises

This trust collapse cannot be fixed with better apps or policies alone.

---

3. Design Philosophy

The HSP-PCB is built on four non-negotiable principles:

1. **Human First** – The human, not the device or network, is the authority.
2. **Hardware-Enforced Consent** – Physical and cryptographic controls override software.
3. **Data Minimization by Design** – Prevent unnecessary data from existing.
4. **Dignified Failure** – Loss, theft, or coercion does not become catastrophe.

The system assumes that operating systems, networks, and even chip supply chains may eventually be compromised.

---

4. Core Concept

The HSP-PCB is best understood as:

> **A Secure Enclave + Hardware Firewall + Network Controller + Identity Vault on a PCB**

It operates as an independent control plane that: - Owns cryptographic identity and keys - Gates access to sensors, data, and networks - Enforces user consent in hardware - Remains functional across current and future network generations

---

5. Threat Model

The system assumes the following adversaries are possible: - Compromised phone OS or firmware - Malicious or coerced telecom infrastructure - IMSI catchers and traffic

correlation - Supply-chain attacks - Physical theft or confiscation - Advanced nation-state technical capabilities

The system does **not** attempt to defeat lawful physical coercion or global RF surveillance. Instead, it ensures **no silent or remote compromise** is possible without the human.

---

6. Architecture Overview

6.1 Hardware Root of Trust

- Secure element for identity and key storage
- Secure MCU for policy enforcement
- Debug interfaces permanently disabled
- Tamper detection (voltage, clock, physical)

6.2 Identity Sovereignty

- No factory-set identity
- On-device key generation
- Support for rotating and multi-persona identities
- Offline-capable verification

6.3 Hardware Consent Engine

- Multi-factor authentication (liveness, biometric, PIN)
- Physical consent enforcement
- Cryptographic permission tokens
- Time-bounded and context-aware access

6.4 Independent Network Control

- Network-agnostic design
- Own radios or mediated access to host radios
- Burst-based, offline-first communication
- Traffic timing and metadata minimization

---

7. Lock, Quarantine, and Recovery Model

7.1 Key Hierarchy

- **DEK (Data Encryption Key):** Encrypts all user data
- **KEK (Key Encryption Key):** Wraps DEK
- **HUK (Human Unlock Key):** Derived only after successful authentication

Data is never wiped by default. Access is controlled.

7.2 Operational States

Phase 0 – Normal

- Owner authenticated
- Data accessible
- Full functionality

Phase 1 – Soft Lock

- Triggered by loss or anomaly
- Keys sealed
- Data unreadable
- Fully recoverable

Phase 2 – Quarantine

- Triggered by tampering or repeated failures
- Device becomes silent and useless
- No recovery modes
- Still recoverable by owner or recovery policy

Phase 3 – Final Cryptographic Lock (Optional)

- User-predefined trigger
- KEK destroyed
- Data mathematically unrecoverable
- Device enters inert state

---

8. Controlled Recovery Paths (No Backdoors)

All recovery mechanisms are: - Opt-in - User-defined - Transparent - Revocable

8.1 Delayed Unlock

- 30–90 day delay
- Offline countdown
- Tamper-aware

8.2 Multi-Party Recovery

- Threshold-based trusted contacts
- Sharded secrets
- No single point of compromise

8.3 Legal Escrow (Optional)

- User-chosen legal entity
- Requires due process and time delay
- Disabled by default

8.4 Inheritance Mode

- Time-based release after death
- Prevents permanent data loss

---

9. Physical & Environmental Constraints

9.1 Form Factor

- Credit-card slice
- < 2.5 mm thickness
- < 20 g

9.2 Power

- Ultra-low-power design
- Event-driven operation
- No always-on radios

9.3 Sustainability

- Long lifecycle (10–15 years)
- Modular radios
- Repairable design
- Minimal e-waste

---

10. Ethical Commitments

The HSP-PCB will: - Contain no master keys - Enforce no region-based restrictions - Avoid telemetry and analytics - Support independent audits - Remain transparent in governance

---

11. User Promise (Truthful and Limited)

The system promises: - Without the owner, data cannot be accessed. - Stolen devices become silent and unusable. - Recovery is possible only if the user pre-authorizes it. - Final lock is permanent and irreversible.

The system does **not** promise anonymity, invisibility, or immunity from lawful coercion.

12. Conclusion

The Human-Sovereign Privacy & Security PCB represents a shift from surveillance mitigation to **human dignity by design**. By enforcing consent, minimizing data generation, and providing graceful failure and recovery, it offers a realistic, ethical, and future-proof foundation for smartphones and smart devices.

This is not a product for attention extraction. It is infrastructure for trust.

Appendix A: Formal System Architecture Specification

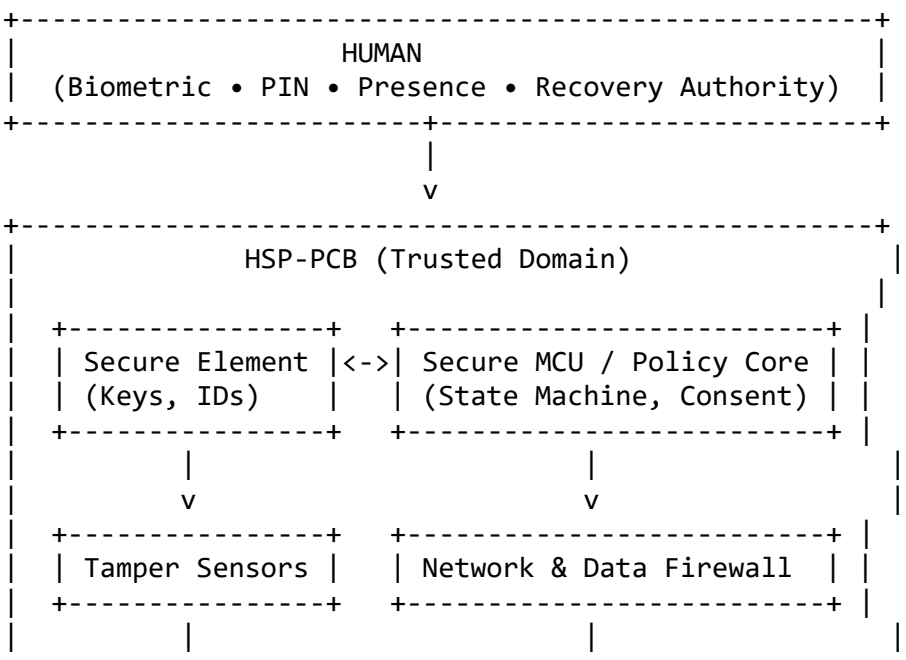
A1. System Overview

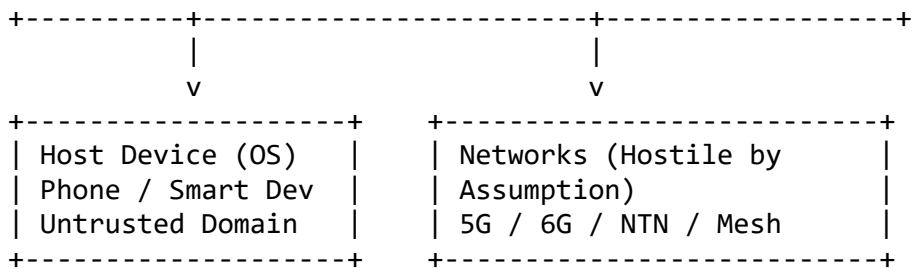
The Human-Sovereign Privacy & Security PCB (HSP-PCB) is an independent, user-owned **hardware root-of-trust and policy enforcement module** that operates alongside (but never depends on) the host device operating system, firmware, or network infrastructure.

The architecture is designed to: - Survive OS, firmware, and network compromise - Enforce human consent at the hardware level - Remain network-generation agnostic (4G, 5G, 6G, NTN) - Support long-term deployment with minimal power and material footprint

---

A2. High-Level System Block Diagram





A3. Trust Boundary Definition

Trusted Domain

- Secure Element (SE)
- Secure MCU
- Cryptographic state machine
- Consent and recovery logic

Untrusted Domain

- Phone operating system
- Device firmware and bootloaders
- Applications
- Telecom and internet infrastructure

No data, identity, or policy decision is trusted if originating from the untrusted domain.

A4. Hardware Components

A4.1 Secure Element (SE)

Responsibilities: - Root key storage - Identity generation (DID support) - KEK / DEK wrapping - Anti-tamper response

Properties: - No debug access - Side-channel and fault resistance - Secure non-volatile memory

---

A4.2 Secure MCU (Policy Core)

Responsibilities: - Enforce state machine - Authenticate user factors - Manage recovery workflows - Gate all data and network access

Properties: - TrustZone or equivalent isolation - Secure boot from ROM - Firmware update only in unlocked state

---

A4.3 Authentication Interfaces

- Liveness detection (camera / sensor mediated)
- Fingerprint sensor (template never leaves SE)
- PIN / passphrase input (rate-limited)

All authentication results resolve to a **binary hardware decision**: allow or deny.

A4.4 Tamper Detection Subsystem

- Voltage and clock anomaly sensors
- Physical enclosure sensors
- Debug interface fuses

Tamper events feed directly into the state machine.

A4.5 Network & Data Firewall

Responsibilities: - Mediate all data entering or leaving the host - Enforce offline-first behavior - Shape traffic timing and volume

Key rule: No direct host-to-network path bypasses the PCB.

A5. Cryptographic Architecture

A5.1 Key Hierarchy

```
[ Human Authentication ]
          |
          v
        [ HUK ]
          |
          v
        [ KEK ] ----wraps----> [ DEK ] ---> Encrypts Data
```

- DEK never leaves encrypted form
- KEK never leaves secure element
- HUK exists only ephemerally after authentication

A6. Operational State Machine (Formal)

```
STATE_0: NORMAL
  - Owner authenticated
  - DEK accessible

STATE_1: SOFT_LOCK
  - Trigger: anomaly / loss
  - DEK sealed
  - Recoverable

STATE_2: QUARANTINE
  - Trigger: tamper / repeated failure
  - KEK sealed
  - No external interfaces

STATE_3: FINAL_CRYPTO_LOCK (Optional)
  - Trigger: user-defined condition
  - KEK destroyed

STATE_4: INERT
  - Terminal state
```

Transitions are irreversible except where explicitly allowed by recovery policy.

A7. Recovery Architecture (No Backdoors)

Recovery Inputs

- Time-delayed unlock counters
- Multi-party secret shards
- Legal escrow shards

Enforcement Rules

- All recovery paths are evaluated inside the SE
- Host OS cannot accelerate, delay, or observe recovery

A8. Power and Form-Factor Constraints

- Credit-card slice PCB
- < 2.5 mm thickness
- Event-driven power model
- Deep sleep default state
- No always-on radios

A9. Security Guarantees (What the Architecture Enforces)

- No silent data extraction
- No OS-level bypass
- No vendor or government master keys
- No remote unlock capability

A10. Explicit Non-Guarantees

- No protection against physical coercion
- No guarantee of anonymity
- No immunity from lawful seizure

A11. Deployment Contexts

- Smartphones
- Wearables
- Vehicles
- Medical devices
- Drones and IoT endpoints

A12. Architectural Summary

The HSP-PCB architecture establishes a **human-centered trust anchor** that remains valid even as operating systems, networks, and geopolitical environments evolve. By grounding control in hardware-enforced consent and cryptographic dignity, it provides a stable foundation for long-term digital sovereignty.

Appendix B: Threat → Mitigation Matrix

Threat Category	Attack Vector	Mitigation Layer	Failure Outcome
OS Compromise	Root / malware	Hardware consent gate	Data inaccessible
Firmware Exploit	Recovery / flashing	PCB ignores boot state	No access
Baseband Attack	IMSI catcher	Offline-first + traffic	Metadata minimized

Threat Category	Attack Vector	Mitigation Layer	Failure Outcome
		shaping	
Physical Theft	Device seizure	Soft Lock → Quarantine	Device useless
Brute Force	PIN / biometric	Rate-limited SE auth	Lock escalation
Reverse Engineering	Chip probing	Tamper detection + fuses	Key sealing
Supply Chain	Backdoored OS	Independent trust root	No privilege
Network Coercion	Forced connectivity	User-owned network policy	Silence enforced
Legal Overreach	Vendor unlock demand	No master keys	Impossible
Quantum Threat	Future crypto breaks	Algorithm agility	Re-keyable

Appendix C: DFM / BOM-Level Reference Design

C1. Chip Class Selection (Non-Vendor-Specific)

- Secure Element: CC EAL5+ class, tamper-resistant
- Secure MCU: Low-power ARM TrustZone-M or RISC-V PMP
- Power Management IC: Ultra-low quiescent current
- Sensors: Minimal biometric + tamper sensors
- Connectivity: Optional modular radio interface

C2. Power Budget (Target)

Mode	Consumption
Deep Sleep	<10 µA
Authentication Event	<20 mA (short burst)
Active Policy Eval	<5 mA
Network Mediation	Event-driven only

C3. Physical Design for Manufacture

- Credit-card slice PCB
- 4–6 layer board
- <2.5 mm thickness
- Conformal coating
- No exposed debug pads

Appendix D: Manufacturer-Ready Logical Diagrams

D1. Logical Integration Diagram

```
[ Sensors ] --> [ HSP-PCB ] --> [ Host SoC ] --> [ Display / Input ]
                      |
                      +--> [ Network Interfaces ]
```

D2. Data Flow Control

```
User Action
   |
   v
HSP-PCB Policy Check --> Allow / Deny --> Host OS
```

Appendix E: Whitepaper Summary for Funders & Policymakers

E1. Problem

Digital infrastructure extracts value from people while offering limited accountability or resilience.

E2. Solution

HSP-PCB introduces a human-owned hardware control plane enforcing consent, recovery, and dignity.

E3. Impact

- Reduced surveillance abuse
- Lower data and airtime costs
- Improved mental well-being
- Climate-aligned long-life hardware

E4. Policy Alignment

- Data protection by design
- Human rights–aligned security
- National digital sovereignty without fragmentation

Appendix F: Android and Future Device Integration Paths

F1. Android Integration

- HSP-PCB exposes secure API
- Android treats PCB as external trust authority
- Sensors and network access mediated through PCB

F2. Future Device Integration

- Embedded on device motherboard
- Modular attachment for wearables
- Vehicle and IoT secure enclave role

Appendix G: End-to-End HSP-PCB Solution Overview

The complete HSP-PCB solution spans:

1. Hardware root-of-trust PCB
2. Formal cryptographic state machine
3. User-defined recovery governance
4. Host integration APIs
5. Manufacturing and sustainability model
6. Ethical and legal positioning

Together, these elements deliver a **deployable, auditable, and future-proof human sovereignty infrastructure**.