

The Sovereign Network — Concept & Architecture

A Born Between 2 Generals platform · Cyber Sentinel

Kristen@bornbetween2generals.com *Track-back, never hack-back · Zero egress by default · Local-first*

Why this exists

Today's internet is "connect first, defend later." Every site you open can run code on your machine, reach back out to servers you never chose, and attackers ride those same open doors. The whole Cyber Sentinel doctrine flips that: **nothing is trusted until it proves itself, and the system watches back instead of hacking back.**

This document brings together **two network ideas** under one roof — the ones already built into the platform for specific high-stakes situations, and the new one Kristen described: a whole clean place to live online where people are safe by default.

The two layers, side by side

	Layer A — Situation Air-Gaps (built)	Layer B — The Sovereign Mesh (new)
What it protects	The most critical systems: nuclear, grid/SCADA, records vaults, elections	Ordinary people browsing everyday sites
Posture	Truly off every network — physically/logically disconnected	Always-air-gapped <i>overlay</i> — a clean network you live on
How data moves	One-way data diode, token-gated crossing	One-way sanitizing gateway; content enters as safe static snapshots
Who's on it	A handful of operators + machines	Anyone — families, schools, businesses
The promise	"This can never be reached from the outside."	"Jump around freely and never get attacked."
Status	Prototyped: sentinel/air_gap_infra/	Prototyped: sentinel/sovereign_mesh/

They are the same doctrine at two scales. Layer A seals a reactor. Layer B gives a family a safe internet. Both assume the outside world is hostile and let nothing across without proof.

Layer A — Situation Air-Gaps (already in the platform)

Purpose-built isolation for a specific critical system.

- **True isolation** — the protected ("high") side runs with no listening sockets and no outbound capability. In real deployment it is physically disconnected; in the prototype an `assert_isolated()` self-check enforces the posture.
- **One-way data diode** — information can only cross in the intended direction, and only carrying a valid Sovereign Fabric token.
- **Air-gapped vault on the high side** — sensitive material (keys, configs, case files) lives encrypted on the isolated side and is never reachable from the low side except through the token-gated diode.
- **Multiple named zones** — e.g. `reactor-control`, `grid-scada`, `records-vault`, each with its own diode, isolation posture, and vault.
- **Breach response** — a forged token trips an instant lockdown and rotates every token.

This is the right tool when the answer is "this system should simply not be on any network."

Layer B — The Sovereign Mesh (the new "safe internet")

Kristen's vision: a brand-new network — a private, always-air-gapped internet — where ordinary people can jump between sites and never get attacked.

The mesh is a **closed-world, default-deny overlay**. Nothing exists on it unless it was admitted and signed. That single rule removes almost every way people get hurt online.

1. **Every site is admitted, signed, and content-addressed.** A site only exists on the mesh if it carries an allow-listed, signed manifest and its content matches a known hash. There is no "random link to anywhere" — the thing you open is provably the thing that was approved.
2. **The gateway is a one-way sanitizer.** The only crossing between the dirty outside internet and the clean mesh fetches outside content *once*, strips it to safe static form (no live scripts, no outbound beacons), hashes it, signs it, and publishes a snapshot. **Users never touch the live outside site** — so the live site can never touch them.
3. **Everyone carries a rotating typed token.** People (`PSN-`), sites (`SITE-`), and nodes (`NODE-`) all hold rotating identity tokens. No token, no route. A stolen or forged token fails, and a replayed old token fails after the next rotation.
4. **Safe browsing = verified hops.** Each "jump" between sites is token-checked and the destination's content-hash is re-verified before anything renders. A tampered or unknown site is refused and quarantined — **the user is never exposed**, and the attempt is logged.
5. **No outbound egress from a mesh node.** By design, a node on the mesh cannot beacon out. Even a malicious snapshot has nowhere to phone home.

6. **Tamper-evident ledger.** Every admission, crossing, refusal, and quarantine is written to a hash-chained log, so the whole network's history can be audited without trusting any operator.

The felt experience for a family: you open your safe browser, you move between sites, and nothing can run on your device, redirect you, or track you — because the network itself won't carry those things.

Layer C — Sovereign IoT & Hardware (companion, prototyping)

The same doctrine for the physical devices in a home or facility, so smart devices can't become the way in.

- **Guardian perimeter** — a default-deny gateway wraps a fleet of devices; devices talk only to the gateway, never the open internet.
- **Hardware identity** — each device carries a rotating typed hardware token (`DEV-`) bound to its hardware id; unknown or forged devices are rejected at enrollment.
- **One-way telemetry** — device data crosses to the monitoring side through a diode, never the reverse.
- **Breach response** — a forged device token or anomalous behavior quarantines the device, locks the zone, rotates tokens, and writes the event to the ledger.

Status: prototyping in `sentinel/sovereign_iot/`.

How it all connects to Cyber Sentinel

The Sovereign Network is not a separate product — it is the network layer of the same platform:

- **Sovereign Identity Fabric** issues and rotates every token used by all three layers.
- **Cyber Caller ID** screens each inbound connection against the fabric before it's allowed.
- **VigilantGuard** lures anything hostile into a sealed sandbox and analyzes a copy — never the source (track-back, never hack-back).
- **The Forensics Lab** seals every event into court-ready, tamper-evident evidence.
- **The Air-Gapped Vault** protects secrets at rest on any isolated side.

One doctrine, one console, family to nation.

Honest status

Piece	Status
Situation Air-Gaps (air_gap_infra)	Prototyped & verified
Sovereign Identity Fabric, Egress Guard	Prototyped & verified
Sovereign Mesh (safe internet)	Prototype in progress
Sovereign IoT / Hardware	Prototype in progress
Cyber Caller ID, PhishBot 3.0, VigilantGuard engine	Prototype in progress

All prototypes are **local-first simulations** that actually run and self-verify. They prove the design; a real deployment rides isolated links and one-way diodes. Nothing here hacks back, and nothing egresses by default.

A Born Between 2 Generals platform · The fortress that watches back.