Tokra Sovereign AI — Executive Brief

Sovereign from Day One. Plug-and-Prove.

Cryptographic proof. Instant control. No phone-home.

1. Executive Overview

Tokra Sovereign AI is a functional control plane for AI and other critical workloads that operates entirely within the customer's boundary. The platform is built to make policy enforcement verifiable by binding each governed action to cryptographic evidence that is exportable to existing oversight processes. Tokra runs on existing hardware, avoids mandatory cloud dependencies, and behaves deterministically—including in fully offline, air-gapped networks.

This document is a public, non-binding description for executive stakeholders. It intentionally omits implementation detail, internal architecture, and proprietary algorithms. Nothing in this brief constitutes a warranty, service commitment, or support undertaking. Any binding terms, if applicable, exist only in a separately executed agreement.

2. What Tokra Sovereign Delivers

Capabilities are framed to fit enterprise governance without forcing technology swaps:

- Verifiable control — cryptographic records for each policy decision and execution outcome; artifacts are exportable for audit and board review.
- Operational sovereignty — local custody of keys and policies; default-deny connectivity; no phone-home telemetry by design.
- Seamless adoption — on-prem or air-gapped deployment with offline parity; designed to avoid disruptive hardware changes.
- Continuous assurance — signed, immutable upgrade bundles with attributable, explainable enforcement decisions.
- Enterprise alignment — integration points for SIEM, KMS/HSM, and SSO to fit existing controls and workflows.

Framework mapping (e.g., ISO/IEC 27001, NIST 800-53, SOC 2) is available under NDA. This brief does not assert certification status.

Sector-Specific Value:

A) Banking (Financial Services)

- **Data sovereignty:** On-prem or air-gapped deployment; no phone-home; local custody of keys and policies.
- **Evidence-grade auditability:** Cryptographic artifacts for each policy-governed action, exportable to internal audit and boards.
- **Risk & compliance fit:** Default-deny posture and a clear policy-to-evidence pathway; framework mapping (ISO/IEC 27001, NIST 800-53, SOC 2) available under NDA.
- **Coexistence with core systems:** Runs alongside core banking, ERP, and payment rails without hardware swaps; interfaces for SIEM/KMS/SSO.

B) Government

- **Sovereign deployment:** Operates on national infrastructure with full offline parity; no mandatory cloud dependencies.
- **Assured operations:** Deterministic behavior and exportable evidence packs for oversight, regulators, and courts of account.
- **Policy primacy & attribution:** Runtime is bounded by declared policy; decisions are attributable to authorized roles.
- **Standards alignment:** Framework mapping available under NDA; this public brief makes no certification claims.

C) AI Training

- **Controlled training boundary:** Default-deny egress with explicit allow-lists for datasets, tools, and endpoints; zero-retention options.
- **Dataset governance & provenance:** Chain-of-custody for data and model artifacts with exportable, tamper-evident evidence.
- **Secure compute on existing hardware:** Works with current GPU/accelerator stacks; no phone-home telemetry; air-gapped parity.
- **Repeatable, explainable runs:** Signed, reproducible bundles for experiments; explainable enforcement suitable for review.

3. Principles of Control

Control is established through declared policy and proven through evidence. Tokra's operating principles are conservative and explicit:

- Governance-by-policy — organizations declare permitted behavior; Tokra enforces precisely at runtime with minimal operator burden.
- Evidence-first design — decisions and outcomes are coupled with cryptographic attestations to support accountability.
- Local custody — policy roots and keys remain under customer control; external services are optional by policy, not assumed.
- Deterministic operation — offline parity and a default-deny posture prevent unintended flows and reduce ambient risk.
- Minimal trust — reproducible, signed bundles create a verifiable chain of custody for code and configuration.

4. Evidence & Assurance

Tokra implements a policy-to-evidence pathway designed to make compliance provable rather than rhetorical. Evidence packs capture signed decisions, inputs, and outcomes for a defined policy set and can be exported to existing review, audit, and board oversight routines.

- Evidence scope — policy identifiers, decision context, execution outcomes, and verification metadata.
- Portability — evidence formatted for ingestion by common governance and audit systems.
- Attribution — decisions attributable to policy owners and authorized operators for post-incident analysis.
- Retention controls — export and lifecycle behavior are policy-defined; zero-retention defaults may be selected.

Framework mapping is available under NDA; certification claims are outside the scope of this brief.

5. Security Posture

Security assumptions emphasize containment, observability, and provenance:

- No phone-home — all connectivity is explicit, policy-controlled, and observable; hidden channels are not used.
- Isolation by design — sensitive flows are segmented; policy constrains movement to minimize blast radius and exfiltration paths.
- Signed, immutable upgrades — roll-forward under policy with verifiable provenance and change records suitable for internal review.
- Zero-retention by default — least-privilege data handling and customer-defined residency; export is policy-gated.
- Supply-chain transparency — Software Bills of Materials (SBOMs) are available under NDA.

6. Deployment Models & Interfaces

Choose the model that best matches operational risk and regulatory posture; both preserve the same functional guarantees:

- On-prem — installs alongside existing infrastructure with local key custody and policy authority.
- Air-gapped — full offline parity; all functions operate without external connectivity.

Interfaces focus on alignment with existing controls rather than introducing new dependencies:

- Identity — integrates with enterprise SSO and role-based controls to minimize operational overhead.
- Observability — SIEM export and tightly controlled evidence channels feed current security tooling.
- Key management — supports integration with KMS/HSM where policy permits; local custody remains the default.

7. Operating Model (Non-binding)

An illustrative, non-binding path from evaluation to operational use:

- Access under NDA — scope policy domains and assurance needs; review non-public materials (evidence samples, controls matrices).
- Pilot in your environment — on-prem or air-gapped; generate evidence packs and review outcomes with decision makers.
- Operationalization — proceed per your governance process; any terms, if applicable, are defined in a separate agreement.

No SLAs, response times, availability, or support commitments are stated or implied by this brief.

8. Risk & Governance Alignment

Tokra is designed to fit within existing risk programs without diluting accountability:

- Policy primacy — runtime behavior is bounded by declared policy that can be independently reviewed.
- Segregation of duties — roles for policy owners, operators, and auditors remain distinct and attributable.
- Evidence portability — artifacts can be shared with regulators, boards, and third-party auditors as required by policy.
- Regulatory posture — alignment support for common frameworks under NDA; this document does not claim certifications.

9. Differentiators

- Sovereign from day one — no mandatory cloud; designed to run on existing hardware.
- Evidence you can export — cryptographic, tamper-evident artifacts for each policy decision and execution outcome.
- Deterministic offline operation — suited to critical and regulated environments that require air-gapped resilience.
- Explainable enforcement — attributable decisions suitable for audit and post-incident review.
- Integration-ready — aligns with identity, logging, and key management investments already in place.

10. IP & Disclosure Boundary / Next Steps

This public brief does not disclose implementation detail, source code, or proprietary algorithms. Tokra may have patents filed or pending; nothing herein is a license or disclosure of trade secrets. Detailed materials are provided only within the Access Program under NDA.

- Request Access — begin a due-diligence track under NDA.
- Governance workshop — align on policy scope, evidence requirements, and deployment constraints.
- Pilot — validate outcomes in your environment; review exported evidence with stakeholders.

***Closing**: Tokra Sovereign AI — Change the game, not the hardware. Plug-and-Prove.*

Date: 1st of July 2025