Enterprise Architecture Annex

The Sovereign Pipeline & Algorithmic Accountability

Addendum to The TallySticks System Blueprint (v2.0)

Architectural Objective

To resolve the "Sovereign Gap" by establishing a mathematically enforced air-gap between non-deterministic AI processing and sovereign execution authority. This architecture ensures that accountability is enforced **pre-execution**, not audited post-event.

1 The Algorithmic Procurement Crisis

Modernization of the UK public sector and regulated financial markets relies on the deployment of Artificial Intelligence to process welfare claims, procurement contracts, and financial routing. However, deploying "Black Box" models into financial infrastructure presents a constitutional risk. Hallucinations leading to erroneous multi-million pound awards cannot be resolved by post-event auditing.

The Axiom Mandate: Accountability must be mathematically enforced at the point of intent, before capital leaves the Treasury.

2 The Tripartite Cloud Architecture

TallySticks UK utilizes a three-tier isolation model to protect the state from algorithmic error:

- **Project Alpha (The Processing Chassis):** A non-persistent environment hosting the AI agent. Termed a **"Ghost Ship"**, it possesses analytical capability but zero execution authority and no access to Personally Identifiable Information (PII).
- **Project Beta (The Sovereign Governor):** The deterministic logic layer. It houses **SPUdata** (the PII shield) and **EAVEcore** (the physical logic gate). This layer intercepts all AI-generated intents.
- **Project Gamma (The Witness Node):** An isolated cryptographic pipeline that writes the final, unalterable receipt to the public distributed ledger (an enterprise utility network, e.g., BSV).

3 Real-Time Deterministic Interception

Execution flow is governed by a sub-millisecond API boundary check:

1. **Interception:** AI intents are halted at the Project Beta boundary.
2. **Validation:** EAVEcore evaluates the intent against hardcoded *Statutory Maxims* (e.g., Public Contracts Regulations 2015).
3. **Execution/Kill:** If non-compliant, the transaction is killed and logged as a failure. If compliant, SPUdata re-attaches routing data for execution, and Gamma hashes the proof.

4 The Custodian Framework & Chain of Guardianship

The rules governing EAVEcore (*Maxims*) are not controlled by private entities. They are governed by the **Custodial Council**. To update a Maxim, a multi-signature cryptographic authorization is required. The public keys of the Custodians are linked to the Witness Node, ensuring every update to national policy is permanently hashed alongside a "Custodian's Pledge."

5 The Custodian Ceremony & The Sovereign Key

The 14-Key hierarchical protocol binds the state to the social contract through a conditional multi-sig architecture:

Key Type	Quantity	Holder
Custodian Keys	12	Decentralized Custodial Council
Sovereign Ceremony Key	1	Designated Govt Authority (e.g., HM Treasury)
Public Consensus Override	1	Decentralized Oracle / Statutory Threshold

The Constitutional Fail-Safe (The Override)

If the state attempts to capture the system or paralyze transparency by refusing to deploy the Sovereign Key, the smart contract pivots to a secondary condition:

1. **Immutable Logging:** The refusal to sign is written to the public ledger as a record of non-compliance.
2. **The Public Override:** The 12 Custodians combine their signatures with the Public Consensus Override Key to bypass the Sovereign Key and execute the necessary update.

Mathematically preventing the state from holding the public's transparency hostage.