🛡️ ZK-Proof of Sensing (ZK-PoS): Especificação Técnica v1.0

A **Prova de Sensoriamento (ZK-PoS)** é o mecanismo criptográfico que ancora o rótulo MEASUREMENT à realidade física, eliminando a possibilidade de injeção de dados sintéticos sem a posse física do hardware homologado.

1. O Problema: O "Man-in-the-Middle" Epistêmico

Sem ZK-PoS, um atacante pode emular a API de um sensor perfeitamente. O sistema recebe um Golden Vector que parece uma medição, mas é um output de um modelo generativo (Ghost Model).

2. Invariantes de Hardware e Criptografia

INV-HWD-01: Identidade Siliciosa Única

Cada sensor homologado deve possuir uma **PUF (Physical Unclonable Function)** ou uma chave privada gravada em um enclave seguro (TEE) no momento da fabricação.

- **Ameaça:** Clonagem de identidade de sensores.
- **Mitigação:** A chave privada nunca deixa o silício; assinaturas são geradas internamente.

INV-HWD-02: Acoplamento Espaço-Temporal

Toda prova de sensoriamento deve incluir um *nonce* derivado do estado atual da rede (ex: hash do último bloco) e um timestamp assinado.

- **Ameaça:** Ataques de rebatimento (replay attacks) de medições antigas.
- **Violação:** Se violado, dados históricos podem ser usados para forjar o presente.

3. Fluxo de Geração da Prova (The "Chain of Truth")

1. **Captura:** O transdutor físico converte sinal analógico em digital.
2. **Binding:** O controlador do sensor anexa o Current_Block_Hash e o Internal_Clock_Tick.
3. **ZK-Generation:** O enclave (ou um chip auxiliar de baixo consumo) gera uma prova de conhecimento zero (ex: Groth16 ou STARK) atestando que:
    - O valor V foi lido pelo sensor ID_{sensor}.
    - ID_{sensor} possui a assinatura válida da autoridade de homologação.
    - O cálculo não foi adulterado entre a captura e a saída.
4. **Publicação:** O Golden Vector é emitido contendo o dado bruto e o zk_proof.

4. O Verificador (On-Chain/Node-Level)

O nó receptor não precisa conhecer os segredos do sensor. Ele apenas executa a função de

verificação:
$Verify(Proof, Public\_Input, Hardware\_Root\_Key) \rightarrow \{True, False\}$
Se $False$, o vetor é sumariamente rejeitado e o nó emissor entra no protocolo de **Detecção de Fraude Epistêmica**.

5. Matriz de Confiabilidade (Hardware Tiers)

Nem todo hardware suporta ZK-STARKs complexos. Definimos níveis de certeza:

Nível	Tecnologia	Descrição	Confiança
L3 (Max)	**Full ZK-Sensing**	Prova ZK gerada no próprio chip do sensor.	Absoluta (Matemática)
L2 (Mid)	**TEE Binding**	Dado capturado e assinado dentro de um Secure Enclave (ex: SGX/TrustZone).	Alta (Segurança de Hardware)
L1 (Low)	**Signed Metadata**	Apenas assinatura digital simples baseada em chave de fabricante.	Média (Auditável)
L0 (None)	**Unattested**	Dado sem prova de hardware.	Nula (Tratado como HUMAN_ATTESTED)

6. Análise de Falhas e Mitigações

- **Ameaça de "Side-Channel":** Atacante estimula o sensor físico com estímulos artificiais (ex: laser em câmera).
  - **Mitigação:** Heurísticas de coerência cruzada (Semantic Ghosting) do protocolo de fraude. O ZK prova que o sensor leu algo, a coerência prova que o que ele leu faz sentido.
- **Degradação de Hardware:** PUFs podem mudar com o tempo.
  - **Mitigação:** Protocolo de recalibração periódica e renovação de certificados de hardware.

Status: PROPOSTA / EM DEFINIÇÃO
Próximo Passo: Formalização matemática dos circuitos de prova para sensores de baixa

potência.