Identity Continuity Under Interruption — Procurement Language

For inclusion in SOWs, RFIs, RFPs, and technical evaluations. This language is intended to support architectural evaluation and requirements definition, not to mandate specific implementation techniques.

Variant A — Minimal (1 Paragraph)

The system shall preserve identity continuity under interruption conditions, including degraded, delayed, reordered, or unavailable telemetry. Loss of observation alone shall not result in identity reinitialization, duplication, or state divergence. The system shall maintain internal identity representations that remain authoritative across interruption and shall perform validated re-association upon recovery.

Variant B — Medium (Bulleted Requirements)

The proposed system shall:

- Preserve identity authority across interruption without requiring reinitialization.
- Maintain persistent internal state for tracked entities independent of continuous observation.
- Prevent downstream subsystems from creating new or duplicate identities during interruption.
- Perform validated re-association before resuming identity authority after telemetry restoration.
- Ensure identity continuity across distributed and heterogeneous execution environments.

Variant C — Strict (Verification-Oriented)

Offerors shall describe how the proposed system:

1. Preserves identity authority during periods of degraded or unavailable telemetry, including how authority is retained and not implicitly revoked.
2. Maintains persistent internal representations of entities independent of continuous observation.

3. Prevents identity duplication, drift, or parallel instantiation across distributed subsystems during interruption.
4. Validates re-association of restored telemetry before resuming identity authority.
5. Avoids reset cascades or unintended identity reinitialization during recovery, including how re-association is gated and controlled.
6. Produces machine-readable artifacts, if any, indicating whether available system-maintained evidence is sufficient or insufficient to assert identity continuity under declared interruption conditions.

Responses shall focus on architectural behaviors rather than specific implementation techniques.

Notes to Procurement

- No specific inference methods, algorithms, sensor modalities, or control architectures are required.
- Deterministic, probabilistic, hybrid, or heuristic approaches are acceptable.
- Centralized or decentralized architectures may satisfy these requirements.

Related Reference Material

SISMIQ Continuity Requirements (SCR)
Canonical architectural requirements for identity continuity under interruption.

Identity Failure Chain Under Interruption
Explanatory overview of common identity failure modes in interruption-prone systems.

Architectural Note: Identity Continuity Under Interruption
Contextual discussion of architectural implications and design tradeoffs.

Continuity Compliance Checklist
Self-assessment tool mapping system behavior to continuity requirements.

For architecture or specification clarification:

contact@sismiq.io