

## Commit Tenant Flow Sequence Diagram - Context

---

✅ This diagram fully captures:

### 1. Full PEC evaluation pipeline

- Schema → provenance → tenant → policy
  - Constraints → invariants → HITL → decision
- 

### 2. All decision outcomes

- REJECT → REJECTED
  - PENDING\_HITL → PENDING\_HITL
  - ACCEPT → AUTHORIZED
- 

### 3. HITL branch

- Invalid cosign → remains PENDING\_HITL
  - Partial quorum → remains PENDING\_HITL
  - Quorum satisfied → AUTHORIZED
- 

### 4. Commit / binding validation outcomes

Includes all **critical commit paths**:

- PENDING\_HITL → reject
  - REJECTED → reject
  - EXECUTED → reject (replay)
  - AUTHORIZED + fail → stays AUTHORIZED
  - AUTHORIZED + success → EXECUTED
- 

⚠️ **What is *not explicitly represented***

These are **not errors**, but **omissions / compressions**:

---

## 1. Pre-PEC hard failures short-circuiting

These are *implicitly* included, but not explicitly:

- Schema failure → immediate REJECT
- Provenance failure → immediate REJECT
- Tenant not ACTIVE → immediate REJECT
- Policy not found → immediate REJECT

Right now, the diagram shows the pipeline but not **early exits**.

---

## 2. Constraint / invariant failure precedence

Not explicitly shown:

- Constraint FAIL → REJECT
- Hard invariant FAIL → REJECT (overrides everything)

This is logically inside PEC, but not visually branched.

---

## 3. HITL → REJECT path

Spec allows:

PENDING\_HITL → REJECTED

Via:

- expiration
- cancellation
- governance revocation

The diagram currently only shows:

- remain PENDING\_HITL
- or → AUTHORIZED

So this path is not shown in the diagram.

---

## 4. Idempotency behavior

Not shown (which is fine for this diagram):

- replay of submit → no new ledger entries
  - idempotency conflict → rejection without mutation
- 

## 5. Cross-tenant / scope violations

Also intentionally omitted, but not represented:

- TENANT\_SCOPE\_VIOLATION paths
- 

 **This diagram correctly represents state transitions + commit gating.**

Especially:

AUTHORIZED → (binding fail) → stays AUTHORIZED

PENDING\_HITL → (commit attempt) → stays PENDING\_HITL

That is the core of AGCP's execution model.

---

## Final assessment

✓ **What it is:**

- A **complete execution-path diagram** for:
  - PEC decision
  - HITL handling
  - commit binding validation

! **What it is not:**

- A **fully exhaustive conformance / error-path diagram**
-