

STATE MACHINE SPECIFICATION



TABLE OF CONTENTS

Purpose..... 3

What a State Machine is plainly 3

State Machine 1: Identity & Authority 4

State Machine 2: Document Lifecycle..... 5

State Machine 3: Approval Task 6

State Machine 4: Workflow Instance 7

Cross-State Machine Rules..... 8

PURPOSE

This document defines the **legal states**, **allowed transitions**, and **authority boundaries** of the system.

While events describe *what has happened*, and workflows describe *what should be coordinated*, **state machines define what is allowed to be true**.

This document exists to:

- Eliminate ambiguity
- Prevent invalid transitions
- Provide a single source of truth for correctness
- Serve as the foundation for implementation, testing, and audits

If a behavior is not allowed by a state machine defined here, it is considered a system defect.

WHAT A STATE MACHINE IS PLAINLY

A state machine defines:

- A finite set of valid states
- The events that may cause transitions
- Which transitions are allowed or forbidden
- Which subsystem has authority over the transition

A state machine does **not**:

- Decide *why* something happens (Policy does that)
- Coordinate *when* something happens (Workflow does that)
- Notify anyone (Notification does that)

A state machine only answers:

"Given the current state and an event, is this transition valid?"

.

STATE MACHINE 1: IDENTITY & AUTHORITY

Owned by: Identity & Authority Subsystem

Authority level: Absolute

Scope: Truth of a user state

Valid States

- NotAuthenticated
- Authenticated
- NotAuthorized
- Authorized

Current State	Event	Allowed	Next State	Notes
NotAuthenticated	UserAuthenticated	Yes	Authenticated	Login timestamp assigned
NotAuthenticated	AuthorizationDenied	No	Authorizaed	Cannot authorize unauthenticated user
Authenticated	AuthorizationGranted	Yes	Authorized	Authroization Timestamp assigned
Authenticated	AuthorizationDenied	Yes	NotAuthorized	Insufficient permission

Invariants

- A user must be authenticated to use the system
- Authorization must be ensured for access to any resource in the system
- No subsystem other than Identity & Authority handles user authentication and authorization

STATE MACHINE 2: DOCUMENT LIFECYCLE

Owned by: Document Lifecycle Subsystem

Authority level: Absolute

Scope: Truth of a document's state

Valid States

- Draft
- Submitted
- Approved
- Rejected
- Archived

Current State	Event	Allowed	Next State	Notes
Draft	DocumentCreated	Yes	Draft	Initial Creation
Draft	DocumentSubmitted	Yes	Submitted	Submission timestamp assigned
Draft	DocumentApproved	No	-	Cannot approve Draft
Draft	DocumentRejected	No	-	Cannot reject Draft
Submitted	DocumentApproved	Yes	Approved	Only after final approval
Submitted	DocumentRejected	Yes	Rejected	Rejection reason required
Submitted	DocumentSubmitted	No	-	Duplicate submission
Approved	DocumentArchived	Yes	Archived	Terminal transition
Rejected	DocumentArchived	Yes	Archived	Terminal transition
Archived	Any event	No	-	Archived is immutable

Invariants

- A document can only be in **one state at a time**
- State transitions are **atomic**
- No subsystem other than Document Lifecycle may change document state

Workflow completion **does not imply approval** unless this state machine allows it

STATE MACHINE 3: APPROVAL TASK

Owned by: Workflow Orchestration Subsystem

Authority level: Absolute

Scope: Truth of an individual approval task

Valid States

- Pending
- InProgress
- Completed
- Expired
- Superseded

Current State	Event	Allowed	Next State	Notes
Pending	ApprovalTaskCreated	Yes	Pending	Initial state
Pending	TaskStarted	Yes	InProgress	Optional explicit start
InProgress	ApprovalTaskCreated	Yes	Completed	Records decision
InProgress	ApprovalTimeout	Yes	Expired	Time based fact
Pending	ApprovalTimeout	Yes	Expired	Task never acted upon
Pending	TaskSuperseded	Yes	Superseded	Workflow reconfigured
InProgress	TaskSuperseded	Yes	Superseded	Escalation override
Completed	Any event	No	-	Terminal
Expired	Any event	No	-	Terminal
Superseded	Any event	No	-	Archived is immutable

Invariants

- A completed task can never expire
- An expired task can never be completed
- Superseded tasks are ignored by policy and lifecycle
- ApprovalTimeout is a fact, not a failure

STATE MACHINE 4: WORKFLOW INSTANCE

Owned by: Workflow Orchestration Subsystem

Authority level: Absolute

Scope: Truth of an approval workflow as a whole

Valid States

- **NotStarted**
- **Active**
- **Waiting**
- **Advanced**
- **Completed**
- **Stalled**

Current State	Event	Allowed	Next State	Notes
NotStarted	WorkflowStarted	Yes	Active	Triggered on submission
Active	ApprovalTaskCreated	Yes	Waiting	Awaiting action
Waiting	ApprovalTaskCompleted	Yes	Advanced	Step completed
Waiting	ApprovalTimeout	Yes	Active	Policy determines next step
Advanced	WorkflowAdvanced	Yes	Active	New task may be created
Active	WorkflowCompleted	Yes	Completed	All steps satisfied
Active	WorkflowStalled	Yes	Stalled	No valid next step
Completed	Any event	No	-	Terminal
Stalled	WorkflowResumed	Yes	Active	Manual or Policy-driven

Invariants

- A workflow cannot complete unless all required tasks are completed
- Workflow completion does not automatically imply document approval
- Workflow may advance without document state change
- Workflow state is orthogonal to document state

CROSS-STATE MACHINE RULES

These rules apply across all state machines:

1. **Events do not force transitions**
 - They are evaluated against the current state
2. **Invalid transitions must be rejected**
 - Silently ignoring them is forbidden
3. **Audit & Compliance records all attempts**
 - Including rejected transitions
4. **Notification failures never block transitions**
5. **External Integration failures never roll back state**