

Glossary

Use this glossary to resolve terms used across the AIP 1.0 protocol, the reviewed Rust implementation, and connector-fleet operations. It is for developers, operators, evaluators, and reviewers who need to distinguish similar concepts before

SECTION	API Reference
TYPE	Reference
PROTOCOL	AIP 1.0
SOURCE	docs/reference/glossary.md

Implementation terms describe source revision [97be86e9efedf07ecf1783b03800f683f107fb04](#). Normative protocol meaning belongs to the AIP 1.0 specification and JSON Schemas. A glossary definition does not by itself establish that a deployment implements, conforms to, or has qualified the described behavior.

Distinctions that matter

Do not confuse	Distinction
Protocol, implementation, and deployment	The protocol defines interoperable meaning. An implementation realizes some or all of that contract. A deployment configures and runs exact implementation artifacts under its own trust and operating controls.
Participant, principal, and actor	A participant sends or receives AIP messages. A principal is a represented identity. The actor is the transport-authenticated principal performing the current operation.
Capability, handler, and connector	A capability is the advertised operation contract. A handler is executable code admitted for that capability. A connector maps one external product boundary to one or more capabilities.
Connector type, version, instance, replica, and host	A type names an implementation family; a version identifies one immutable release; an instance is one tenant-owned configured installation; a replica is one routable process identity; the host is the process boundary running that replica.
Profile binding and capability binding	A profile binding describes how a capability appears through a compatibility profile. A capability binding is tenant policy that selects a configured connector instance.
Capability binding and route assignment	A binding is reusable tenant policy. A route assignment is the immutable action-specific target selected from that policy before an external side effect.
Action, session, and transaction	An action requests one capability invocation. A session groups related work between principals. A transaction governs plan, commit, reconciliation, and compensation around one or more effects.
Approval and escalation	Approval is a policy-bound authorization decision for frozen governed input. Escalation asks for human input, takeover, or exception handling and may not authorize execution.
Implemented, conformant, qualified, and live verified	Source presence, protocol test results, exact-artifact topology results, and bounded observation against a real external system are separate evidence levels.

Alphabetical glossary

Term	Meaning
Action	A request to invoke one capability with a stable action ID, structured input, and optional execution context. The current runtime records its lifecycle separately from the request object.
Action result	The protocol object carrying an action status, output, messages, usage, receipt reference, or error. A result that requires approval or human input does not necessarily mean the durable action lifecycle is terminal.
Actor	The transport-authenticated principal supplied to trusted identity and authorization logic for the current operation. Payload identity claims do not replace the actor.
Admission package	A signed declarative connector release unit containing one type and version plus bounded policies, instances, replicas, bindings, and the complete signed evidence set.
Admission policy	A hard capacity and circuit-breaker policy referenced by a capability binding and pinned into each new route assignment.
AIP facade tool	A stable MCP-visible tool that exposes native AIP discovery or lifecycle behavior without generating one MCP tool name for every capability.
AIP version	The version of the normative AIP wire contract. It is independent of a workspace package version, connector version, image tag, or documentation revision.
Approval	A durable request and decision governing frozen action input and policy context. Approval records authorization evidence; they do not authenticate the actor or prove the provider effect occurred.
Approval authority	A deployment-owned resolver that returns current tenant, role, group, external-system, and delegated-authority membership for an approval actor. Policy evaluation retains the resulting authority path for audit.
Artifact attestation	Registry record of immutable artifact, schema, software bill of materials, provenance, conformance, scan, signer, and policy-check identities derived from verified admission evidence.
Audit event	Structured record containing an actor, audit action, timestamp, optional identity context, and optional data. It supports review but is not automatically a cryptographic receipt.
Callback	Asynchronous action-result delivery to an allowed destination. The reviewed runtime records delivery through a durable outbox and retry lifecycle.
Capability	A callable operation advertised by a participant with a stable ID, input schema, optional output schema, and optional risk and execution contract.
Capability binding	Tenant policy that makes one capability available through one configured connector instance, with priority and revision-fenced policy references.
Capability catalog	Tenant-scoped discovery view of callable capabilities derived from admitted definitions, active versions, enabled bindings, and eligible instances.
Capability contract	Declaration of side effects, idempotency, execution, data, credentials, approval, scheduling, transaction, and compensation behavior for a capability.
Catalog revision	Monotonic revision of the published connector-fleet catalog used to paginate consistently and pin routing evidence.
Compatibility profile	Versioned mapping between another protocol, such as MCP or A2A, and native AIP semantics. It exposes only the correspondence defined by that profile.
Compensation	A new governed action intended to offset an earlier committed effect. It is not deletion of history and does not guarantee that the original effect is reversible.
Conformant	Having passed a declared protocol or profile conformance scope. The claim applies only to the identified implementation or artifact and test scope.
Connector	Product-boundary implementation that maps external APIs or events to AIP capabilities while the external product remains the domain authority.
Connector host	Standalone process boundary that runs a frozen connector, owns provider credentials and durable connector runtime state, and participates in signed fleet lifecycle control.
Connector-host lease	Sequence and expiry granted by the trusted lifecycle control plane after registration or heartbeat. An expired lease makes the replica ineligible for new routing.

Term	Meaning
Connector instance	Logical tenant-owned installation of a connector type, selecting an admitted version, non-secret configuration revision, and opaque secret-provider reference.
Connector replica	One pre-provisioned or running connector-host process identity for an instance, pinned to an exact version, peer identity, endpoint, topology, capacity, health revision, and expiring lease.
Connector type	Stable identity of one connector implementation family, independent of release versions, tenant installations, and running processes.
Connector version	One immutable connector release record with an exact manifest, manifest digest, artifact evidence, implementation-support map, and candidate, admitted, active, or revoked lifecycle status.
Correlation ID	Opaque identifier that groups related messages or workflow activity without replacing action, session, transaction, or delegation identity.
Credential handle	Opaque, scope- and tenant-aware reference to deployment-owned credential material. Connectors resolve short-lived material at the final boundary; the handle does not expose the secret.
Cursor	Opaque continuation position for an authorized list, event, stream, or reconciliation query. A cursor is scoped to the surface that issued it.
Dead letter	Durable work parked after automatic execution or recovery cannot continue under its current policy. It requires inspection and a bounded operator decision.
Delegate	Authenticated participant selected to execute a delegated child action.
Delegation	Governed parent-child action relationship across a participant boundary, carrying bounded authority, depth, expiration, and result linkage.
Deployment intent	Operator-reviewed desired connector-instance state with a monotonic generation, exact admitted package identity, desired replica set, and rollout limits.
Durable	Persisted under the configured storage contract so state is not owned only by one request, connection, task, or process lifetime. Durability strength still depends on the selected backend and deployment.
Envelope	Native AIP message wrapper carrying protocol version, message type, sender, recipient, correlation, optional security metadata, and exactly one message body.
Error category	Stable class that describes the nature of a protocol failure. It informs handling but does not authorize retry without the capability and outcome context.
Escalation	Request for human input, takeover, or policy-exception handling. It is broader than approval and may leave execution unauthorized.
Evidence	Retained protocol, provider, source, test, artifact, or deployment facts used to support a bounded claim. Its strength depends on identity, scope, procedure, and limitations.
Evidence statement	Independently signed admission record binding one evidence family and document digest to an exact artifact and manifest for a bounded validity period.
External account	Product-side tenant, workspace, organization, or account mapped to a verified AIP tenant at the trusted identity boundary.
Fencing	Monotonic token, revision, generation, digest, or lease rule that prevents a stale owner or plan from mutating current state.
Frozen connector SDK	Stable connector execution contract that requires implementations to declare capability support and provides typed hooks for failures, reconciliation, cancellation, streaming, and events to the shared host.
Gateway	Boundary that applies configured protocol validation and authentication, resolves trusted identity and policy, and dispatches work to the runtime and admitted handlers.
Generation	Monotonic desired-state revision for one connector instance. A newer observed generation fences an older orchestration intent or plan.
Governed input	Exact action data plus identity and policy context bound by hash or snapshot to an approval, transaction plan, or signed orchestration decision.
Handler	Executable implementation registered or admitted for a callable capability. Publishing a capability without compatible executable support is invalid.

Term	Meaning
Idempotency key	Caller-supplied value used within a defined scope to recognize replay of the same business intent. It does not make an unsafe provider operation exactly once.
Implemented	Present in the identified source revision or artifact. This claim alone says nothing about conformance, deployment configuration, qualification, or live behavior.
Isolated-live qualification	Evidence from an exact connector build exercised against an identified real external product in a controlled, connector-isolated topology.
Lease	Time-bounded ownership record for queued work, recovery work, or a connector-host replica. Completion or renewal requires the matching fence so a stale owner cannot act.
Live verified	Observed in a bounded procedure against an identified real external system. The claim is time-, environment-, and scenario-specific.
Manifest	Participant discovery document containing identity, supported profiles, capabilities, resources, and declared operational or security metadata.
MCP projection	Representation of AIP-backed behavior as MCP tools, resources, prompts, tasks, notifications, or metadata. The projection is not a second native AIP wire model.
Native AIP	The AIP envelope, message, lifecycle, and evidence model used without translation through a compatibility profile.
Operational read model	Authorized durable view used to inspect actions, approvals, transactions, callbacks, events, receipts, resources, or related runtime state.
Orchestration plan	Deterministic platform-neutral batch derived from a verified admission package, desired intent, and exact observed replica snapshot. A separate trusted signature authorizes execution.
Outcome unknown	Transaction state in which an external effect may have committed but no definitive result is available. Blind retry is unsafe; reconciliation must establish provider state.
Participant	Logical protocol endpoint or system that sends or receives native AIP messages. A participant may represent one or more principals.
Principal	A represented human, agent, service, tenant, customer, contact, or system identity with a stable AIP principal ID and optional trust metadata.
Production readiness	Deployment-owned acceptance decision covering exact artifacts, configuration, dependencies, controls, evidence, recovery, and operating responsibility. It is not an AIP protocol status.
Profile binding	Metadata on a capability that identifies the compatibility profile and profile-specific representation for that capability.
Profile state	Versioned durable state owned by a compatibility profile for projections or bindings that cannot be reconstructed from native action state. Raw credentials do not belong in it.
Protocol	Versioned interoperable rules for message meaning, fields, state, errors, and extension boundaries. A protocol does not prescribe one process topology.
Qualification	Procedure and evidence showing that an exact artifact and declared topology satisfy a bounded operational or integration scope.
Qualified	Having passed an identified qualification procedure with exact artifact, topology, dependency, and result identities. The claim does not extend beyond that scope.
Receipt	Hash-linked protocol evidence of a decision or state transition. A receipt supports integrity and ordering claims within its chain, not correctness of every external fact.
Reconciliation	Provider lookup that resolves an uncertain external outcome before retry, compensation, or terminal settlement.
Replay	Duplicate delivery of a message, action intent, event, callback, decision, or lifecycle request. Each surface defines its own replay identity and retention window.
Resource	Discoverable readable object advertised by a participant, optionally owned by a capability and constrained by tenant and access policy.
Route assignment	Immutable action-specific execution target selected before an external effect, pinning tenant, instance, replica, version, endpoint, peer identity, catalog and policy revisions, credential reference, admission reservation, and fence token.

Term	Meaning
Runtime	Durable owner of action, session, approval, transaction, event, callback, queue, lease, retry, reconciliation, and retention lifecycles.
Session	Durable relationship grouping related protocol work between an initiating and responding principal under one lifecycle.
Side effect	Declared consequence a caller must assume, such as reading, writing, deleting, sending a message, changing financial or identity state, or using an external service.
Stream chunk	Ordered partial output, progress, tool event, error marker, or completion marker associated with one action.
Tenant	Administrative data and policy boundary established from trusted identity and used to scope discovery, routing, storage, and authorization.
Transaction	Governed execution context for dry run, plan, prepare, commit, reconciliation, compensation, or terminal settlement around external effects.
Transaction plan	Durable protocol-visible plan binding exact action input, capability, identity, policy, predicted effects, and expiration for a later commit.
Transport binding	Rules for carrying native AIP messages over a delivery mechanism such as HTTP, NATS, SSE, or WebSocket without changing message meaning.
Trust domain	Administrative boundary that owns identities, signing relationships, policy, and accepted capability or connector authorities.

Terminology authority

Use this glossary for concise human meaning. Use the specification and schemas for normative wire fields and enum values, and use the dedicated reference page for exact routes, flags, variables, errors, and metrics. Connector-local documentation owns provider names and product-specific operation terms.

When source and prose differ, first identify whether each statement describes the protocol, the pinned implementation, a deployment, or retained evidence. Then apply the source-of-truth order defined by the documentation home page.

Related pages

- [AIP 1.0 specification](#)
- [JSON Schemas](#)
- [How AIP works](#)
- [Profiles, transports, and connectors](#)
- [Connector fleet architecture](#)