IDENTITY PASSPORT

Identity Passport Specification v0.1 — Working Draft for Public Comment

Working Draft for Public Comment

A semantic specification for user-owned identity across independent applications.

Version	v0.1
Status	Working Draft for Public Comment
Revision date	2026-11-12
Hugo version used	hugo v0.169.0-1da10fc44701c566b1669cdb2d12638f155138bd+extended linux/amd64 BuildDate=2026-10-27T14:52:20Z VendorInfo=gohugoio
Working tree status	clean
Repository HEAD revision	43b40e534a36761b72202019262bea29298c72c4
Publication tag	ip-v0.1-wd-20261113.1
Edition source SHA-256	8f1c657401df31ca7c3a7222c3a448a30da2b482a8cef88cf008363a3f00616c
Identity Passport source baseline	3eb40b409cd9ef2c151a2b6afa4f6836381e291a
Generated	2026-11-13 (UTC)

This is an abstract semantic specification. It does not define a complete wire protocol, certification scheme, or production deployment profile. OPEN-01 through OPEN-17 remain unresolved.

For current public-comment and security-reporting instructions, visit the Identity Passport project website.

Original specification text is offered under CC BY-SA 4.0. Individual figures may carry separate license terms; see their captions.

Contents

Specification overview

1. Scope and maturity

2. Terminology and identity relationships

3. Authority and non-inference

4. Lifecycle and privacy

5. Resolve One Subordinate

6. Binding and provisioning

7. Security and privacy considerations

8. Conformance

Profiles

ipa1 assertion profile candidate

Glossary

OPEN-01 through OPEN-17

Implementation evidence status

Identity Passport Specification v0.1 — Working Draft for Public Comment

Identity Passport Specification v0.1 — Working Draft for Public Comment

Revision dated 2026-11-12.

This specification defines an abstract identity and authority model plus one protected read operation: Resolve One Subordinate. Clauses with `IP-*` identifiers are candidate normative requirements for public review. They derive from accepted Architecture Decision Records (ADRs) and canonical contracts cited in each chapter. ADR references identify accepted architectural decisions; this publication does not alter the canonical records.

The specification does **not** define a universal request encoding, transport, assertion wire profile, public error schema, or independent certification scheme. Those decisions remain open. A profile can add wire details without changing the abstract authority rules.

Chapters

1. Scope and maturity
2. Terminology and identity relationships
3. Authority and non-inference
4. Lifecycle and privacy
5. Resolve One Subordinate
6. Binding and provisioning
7. Security and privacy considerations
8. Conformance and profiles

Requirement and decision traceability

The following index maps the current normative candidate requirements to their chapters. Their accepted-decision mappings are summarized below; the detailed clause-level matrix is maintained in the non-published review-artifact traceability register. ADRs record accepted architectural decisions. Open Questions record unresolved mechanisms or policy choices. Legacy reference-implementation material is supporting evidence only and does not establish or replace accepted decisions.

Requirement identifiers	Specification chapter
IP-SCP-01–IP-SCP-04	Scope and maturity
IP-ID-01–IP-ID-11	Terminology and identity relationships
IP-AUTH-01–IP-AUTH-09	Authority and non-inference
IP-LC-01–IP-LC-11	Lifecycle and privacy
IP-RES-01–IP-RES-09	Resolve One Subordinate
IP-BIND-01–IP-BIND-08	Binding and provisioning
IP-SEC-01–IP-SEC-08	Security and privacy
IP-CONF-01–IP-CONF-10	Conformance and profiles

Accepted ADR index

Accepted ADR	Normative requirement mapping	Related unresolved questions
IP-ADR-0001	IP-ID-01–IP-ID-03, IP-AUTH-01, IP-AUTH-03, IP-LC-01, IP-LC-07, IP-RES-01	OPEN-10
IP-ADR-0002	IP-ID-03, IP-ID-05, IP-ID-07, IP-AUTH-03, IP-LC-03–IP-LC-04, IP-SEC-02	OPEN-13
IP-ADR-0003	IP-ID-02, IP-ID-08–IP-ID-09, IP-AUTH-03, IP-LC-01–IP-LC-02, IP-LC-06, IP-RES-01, IP-BIND-01, IP-BIND-03, IP-BIND-06, IP-SEC-07	OPEN-09, OPEN-13
IP-ADR-0004	IP-ID-04, IP-ID-06, IP-ID-09–IP-ID-11, IP-AUTH-04–IP-AUTH-05, IP-LC-08, IP-SEC-05	OPEN-13
IP-ADR-0005	IP-AUTH-01, IP-AUTH-05, IP-LC-06–IP-LC-07, IP-BIND-02, IP-SEC-07	OPEN-03, OPEN-14
IP-ADR-0006	IP-ID-10, IP-AUTH-04, IP-AUTH-07, IP-LC-08	OPEN-11, OPEN-13
IP-ADR-0007	IP-AUTH-04, IP-AUTH-06–IP-AUTH-07, IP-LC-01, IP-LC-09, IP-LC-11	OPEN-11
IP-ADR-0008	IP-AUTH-04, IP-AUTH-07–IP-AUTH-08, IP-LC-10, IP-SEC-05	OPEN-12
IP-ADR-0009	IP-AUTH-01–IP-AUTH-08; related authorization clauses throughout identity, lifecycle, resolve, binding, and security chapters	OPEN-11–OPEN-14
IP-ADR-0010	IP-ID-11, IP-LC-11, IP-SCP-03–IP-SCP-04, IP-CONF-01–IP-CONF-03; question lifecycle convention	OPEN-01–OPEN-14

Accepted ADR	Normative requirement mapping	Related unresolved questions
IP-ADR-0011	`IP-SEC-06`; related transport/profile boundaries in `IP-SCP-03`, `IP-RES-09`, `IP-CONF-02`	OPEN-01, OPEN-05
IP-ADR-0012	`IP-ID-04`, `IP-ID-06`, `IP-AUTH-01`, `IP-AUTH-05`, `IP-SEC-07`, `IP-BIND-02`–`IP-BIND-04`	OPEN-02–OPEN-04, OPEN-14
IP-ADR-0013	`IP-AUTH-05`, `IP-CONF-04`–`IP-CONF-08`; related scope/evidence claims in `IP-SCP-04`, `IP-CONF-01`–`IP-CONF-03`	OPEN-08, OPEN-15, OPEN-17
IP-ADR-0014	`IP-AUTH-09`; related application-trust boundary in `IP-LC-06`, `IP-SEC-06`–`IP-SEC-07`	OPEN-02, OPEN-14
IP-ADR-0015	`IP-CONF-07`–`IP-CONF-10`	OPEN-08, OPEN-15, OPEN-16

Open-question cross-reference

These are unresolved matters, not accepted ADRs or additional normative requirements. See the canonical Open Questions register for current wording and status. OPEN-01 through OPEN-10 retain their legacy RFC-01 through RFC-10 mappings; OPEN-11 through OPEN-17 have no historical RFC mappings.

Open question	Primary affected clauses or topic	Relevant chapters
OPEN-01	`IP-SEC-06`; transport selection, versioning, serialization	Scope, Security, Profile
OPEN-02	`IP-SCP-03`, `IP-CONF-02`; assertion and trust profile	Scope, Binding, Profile
OPEN-03	`IP-AUTH-05`, `IP-BIND-02`; fresh Principal authentication	Authority, Binding, Security
OPEN-04	`IP-RES-02`, `IP-BIND-02`; Account/Principal association freshness	Resolve, Binding
OPEN-05	`IP-RES-09`; denial, response, and timing policy	Scope, Resolve, Security
OPEN-06	`IP-BIND-05`–`IP-BIND-08`, `IP-LC-11`; acceptance and recovery edge cases	Binding, Lifecycle
OPEN-07	`IP-SEC-04`, `IP-RES-09`; deadlines and resource-bound profiles	Resolve, Security

Open question	Primary affected clauses or topic	Relevant chapters
OPEN-08	`IP-CONF-01`–`IP-CONF-10`; semantic minimum, validation evidence/assurance, independent-validation applicability and validator qualifications, and profile extensions	Conformance, Profile
OPEN-09	`IP-ID-08`, `IP-LC-02`, `IP-BIND-01`; consumer registration and isolation	Identity, Lifecycle, Binding
OPEN-10	`IP-ID-01`–`IP-ID-11`, `IP-AUTH-08`, `IP-LC-10`; remaining model terminology ambiguity	Identity, Authority, Lifecycle
OPEN-11	`IP-AUTH-04`, `IP-AUTH-06`–`IP-AUTH-07`, `IP-LC-09`, `IP-LC-11`; Root recovery mechanisms	Authority, Lifecycle
OPEN-12	`IP-AUTH-08`, `IP-LC-10`; orphan detection and disposition	Authority, Lifecycle
OPEN-13	`IP-ID-10`–`IP-ID-11`, `IP-LC-08`; shared control and ownership	Identity, Lifecycle
OPEN-14	`IP-AUTH-09`, `IP-LC-06`, `IP-SEC-06`–`IP-SEC-07`; application trust bootstrap	Authority, Lifecycle, Security
OPEN-15	`IP-CONF-08`–`IP-CONF-09`; recurring validation and standing lifecycle	Conformance
OPEN-16	`IP-CONF-10`; Public Validation Ledger governance and records	Conformance
OPEN-17	`IP-CONF-05`; Management application disclosure	Conformance

Scope and maturity

Purpose

Identity Passport Specification v0.1 is a **Working Draft for Public Comment**. It specifies candidate identity and authority semantics and the observable behavior of resolving exactly one Subordinate Identity. It does not claim complete wire interoperability, independent implementation certification, or production deployment readiness.

IP-SCP-01 — Scope. A consumer may request current authorization for one exact Subordinate target. The operation does not create, select, grant, cache, or transfer authority. [ADRs 7D, 8C, 8G; canonical resolver contract, Purpose and Exact read capability.] [IP-ADR-0001, IP-ADR-0003, IP-ADR-0009.]

IP-SCP-02 — Semantic boundary. Implementations must preserve the abstract entities, authority rules, exact-target behavior, privacy boundary, and consistency result defined here, regardless of storage or transport. [ADRs 8A–8H; domain model and resolver contract.] [IP-ADR-0001, IP-ADR-0002, IP-ADR-0003, IP-ADR-0004, IP-ADR-0009, IP-ADR-0012.]

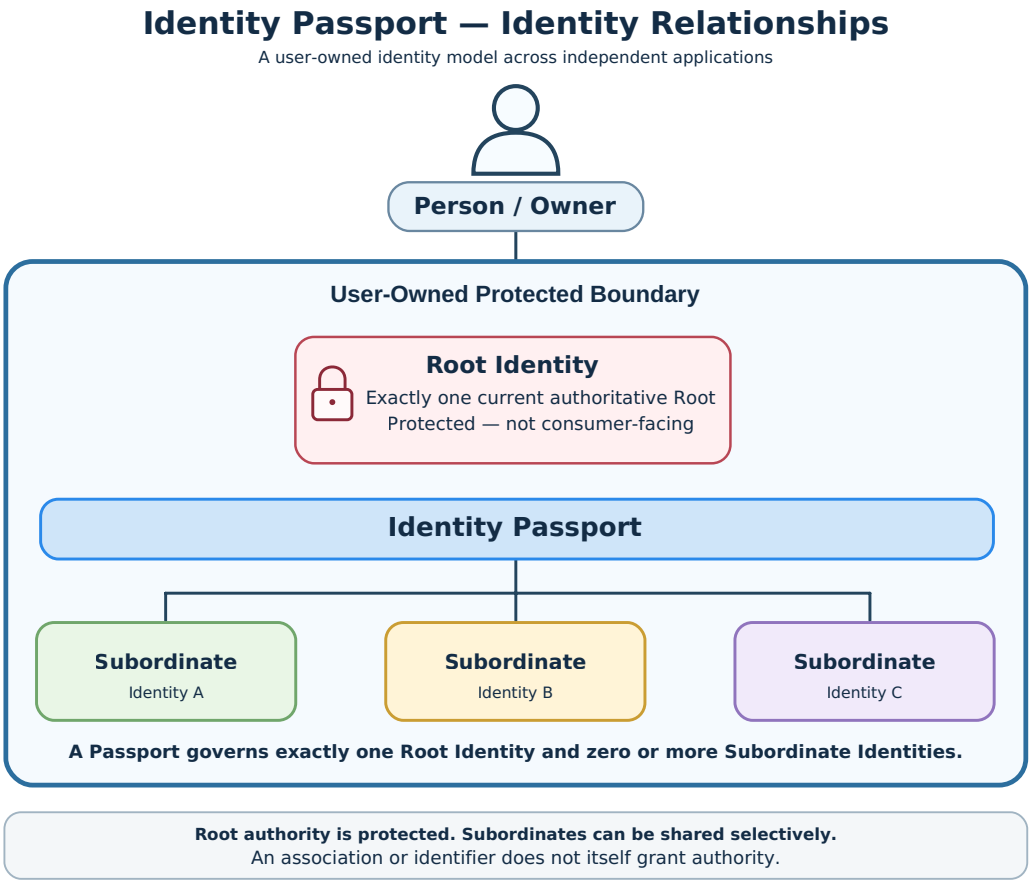
IP-SCP-03 — No interoperability claim. This draft does not define complete transport, serialization, issuer trust distribution, public error wire schema, or vectors. A compatible wire implementation cannot be inferred from semantic conformance. See OPEN-01, OPEN-02, OPEN-05, and OPEN-08. [IP-ADR-0010, IP-ADR-0011, IP-ADR-0012.]

IP-SCP-04 — Evidence boundary. Implementation tests and deployment reports are evidence about a named revision/profile; they do not define protocol semantics or establish production readiness by themselves. [ADR register; canonical validation plan and resolver contract.] [IP-ADR-0010, IP-ADR-0013.]

Examples and implementation notes are informative unless a clause explicitly marks an observable requirement.

Terminology and identity relationships

Use these terms consistently. An identifier or association is not authority. The public glossary defines roles and non-inferences.



Informative illustration of Passport ownership and identity organization. Licensed CC BY-SA 4.0.

Open the identity relationships diagram at full size (SVG)

IP-ID-01 — Entity separation and Root cardinality. A Passport and its Root Identity are distinct. Each Passport MUST have exactly one current authoritative Root Identity. The Root is protected and MUST NOT be used as an ordinary consumer-facing identity or disclosed to a consumer merely to establish a Subordinate association. [IP-ADR-0001.]

IP-ID-02 — Identity cardinality. A Passport MAY contain zero or more Subordinate Identities. Root creation MUST NOT require or cause Subordinate creation. An active Subordinate MUST have exactly one current authoritative Passport relationship. Ordinary consumer identity services MUST use an eligible Subordinate, not the Root. [IP-ADR-0001, IP-ADR-0003.]

IP-ID-03 — Account relationships. Account-to-Passport authorization relationships are explicit and MAY be many-to-many. Shared Account access MUST NOT create identity linkage. [IP-ADR-0001–IP-ADR-0002.]

IP-ID-04 — Authentication separation. Authentication identifies an Authenticated Principal in a trusted context. Account association, identity mapping, identity verification, and operation authorization are distinct facts. [IP-ADR-0004, IP-ADR-0012.]

IP-ID-05 — Identifier privacy. Internal continuity identifiers MUST NOT become unavoidable public correlation identifiers; context-facing bindings and their rotation preserve private continuity while limiting cross-context linkage. [IP-ADR-0002, IP-ADR-0003.]

IP-ID-06 — Non-inference. Authentication, Account association, mapping, identifier possession, and resolution output are separate facts. None creates a grant or authority beyond the exact current request. [IP-ADR-0004, IP-ADR-0009, IP-ADR-0012.]

IP-ID-07 — Independent Passports. A person MAY own and control multiple independent Passports. Each MUST maintain its own authoritative Root and identity-management relationships. Ownership or control of one MUST NOT automatically establish authority over another. Implementations MUST NOT automatically disclose, correlate, or link independent Passports because they share an owner, controller, application, authentication method, or other characteristic. Any cross-Passport relationship or disclosure MUST satisfy applicable explicit authorization, privacy, and consent requirements. [IP-ADR-0002.]

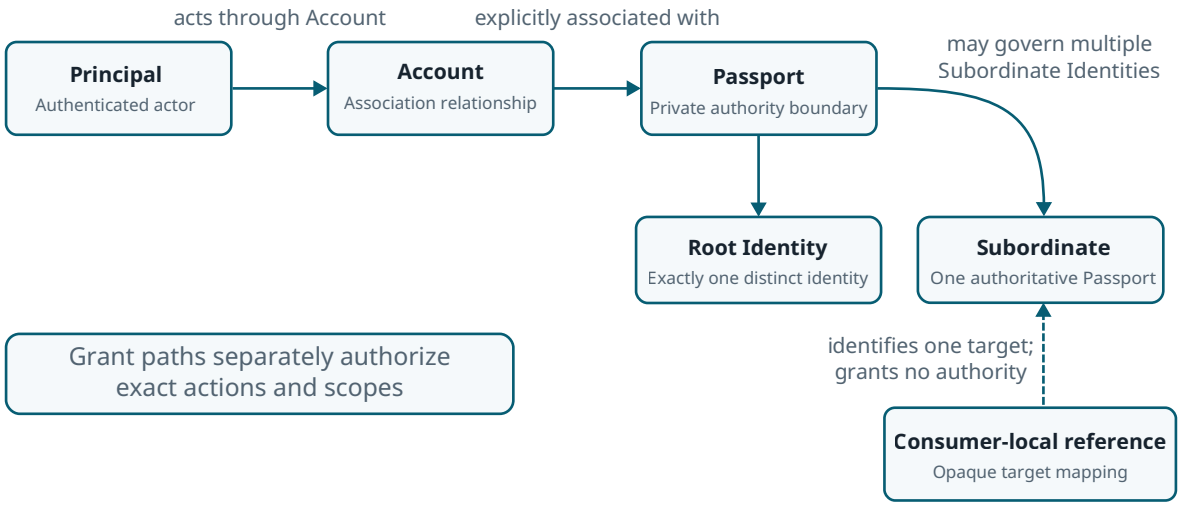
IP-ID-08 — Subordinate continuity and application independence. A Subordinate MAY be associated with multiple independent consumer applications simultaneously. Each application association MUST be explicitly authorized within applicable scope and independently revocable. One association MUST NOT establish another or expose unrelated Subordinates. Subordinate identity continuity MUST be independent of application accounts, display names, and continued application participation. Changes to account or presentation names, or discontinuation of an association, MUST NOT alone create a new Subordinate or transfer ownership. [IP-ADR-0003.]

IP-ID-09 — User ownership. Identity ownership MUST remain with the identity's user and MUST NOT be inferred from application issuance, hosting, authentication, administration, or possession of identity records. An issuing or participating application MUST NOT acquire ownership by creating, hosting, attesting to, or managing an identity. [IP-ADR-0003–IP-ADR-0004.]

IP-ID-10 — Distinct roles. Owner, Controller, Administrator, Delegate, Successor, and Authenticated Principal MUST remain conceptually distinct as defined in the glossary. Authentication, administration, delegation, application trust, or control MUST NOT

independently establish ownership. Granting, sharing, or transferring control MUST NOT automatically transfer ownership. [IP-ADR-0004, IP-ADR-0006.]

IP-ID-11 — Unresolved shared control. The specification does not establish a multiple-owner model or resolve simultaneous controllers, conflicting claims, or the relationship of shared control to succession and recovery; these remain open under OPEN-13. Implementations MUST NOT treat an unspecified mechanism as an accepted requirement. [IP-ADR-0004, IP-ADR-0010.]



Informative illustration; cardinalities and non-inference rules above are normative. Creator: Banjo Fox. Licensed CC BY-SA 4.0.

Open the relationship diagram at full size (SVG)

Authority and non-inference

Protected Passport management and ordinary consumer operations

Protected Passport identity-management and lifecycle operations require Root-associated authority through a complete path. This includes applicable delegation, recovery, succession, and ownership-transfer operations. This does not require the Root Identity or its owner to authenticate separately for each ordinary consumer-application action. Ordinary consumer operations may rely on the application's own permissions and applicable Passport identity-resolution authorization. [IP-ADR-0001, IP-ADR-0005, IP-ADR-0009.]

IP-AUTH-01 — Complete-Path Authorization.

Every protected Identity Passport operation MUST be authorized through at least one complete, current authority path.

The path MUST authorize the requesting actor, the requested capability, the intended target, and the applicable scope.

Authorization MUST evaluate all relevant conditions, including provenance, grant status, validity periods, lifecycle eligibility, security restrictions, and other applicable constraints.

Root-associated authority MUST be established for protected Passport identity-management and lifecycle operations, including applicable delegation, recovery, succession, and ownership-transfer operations.

This requirement does not mean that the Root Identity or its owner must authenticate separately for every ordinary consumer-application action.

Ordinary consumer-application operations MAY be authorized through the application's own permissions and applicable Passport identity-resolution authorization, without treating those operations as Root-management requests.

Where a delegate is expressly authorized to exercise scoped Root-derived management authority, that delegate MAY act within the valid delegated scope without requiring the owner to authenticate for each operation.

No actor, application, role, credential, or previous authorization result MAY bypass the complete-path requirement.

[IP-ADR-0001, IP-ADR-0005, IP-ADR-0009, IP-ADR-0012.]

The applicable workflow MUST assign a minimum security class for each protected operation. The caller MUST NOT select or lower that floor. Class safeguards and proof requirements are specified in IP-SEC-08. [8W-A; IP-ADR-0009.]

Minimum class	Protected operations
1 — Routine	Resolve One Subordinate. This floor applies only to that lookup.
2 — Administrative	Enrollment creation; grant issue, delegation, and revocation; external-work dispatch/ reconciliation; authorized security-audit read.
3 — Sensitive	Enrollment activation; authentication-credential rotation; recovery add/rotation; identifier rotation.
4 — Critical	Final-recovery disablement; Root ownership-transfer proposal, acceptance, and commit; Subordinate transfer proposal, acceptance, and commit; succession configuration, trigger, challenge, dispute resolution, and commit; Passport/Root retirement request/commit; Passport/ Root deletion request; deletion commit; hold placement and release.
5 — Emergency	Recovery initiation and completion; restore reconciliation and activation.

The Class 4 floor applies to Passport/Root retirement request and commit, Passport/Root deletion requests, and deletion commits at the scopes in the approved matrix. Floors are minimums and do not replace operation-specific authority, scope, proof binding, lifecycle, or commit checks. [8W-A.]

IP-AUTH-02 — No Pooled Partial Grants.

An implementation MUST NOT combine separately incomplete grants, sibling scopes, or unrelated constraints to synthesize authority.

Each authorized operation MUST be supported by at least one independently complete, current authority path satisfying all applicable requirements.

Multiple independently complete authority paths MAY exist. Any such path MAY authorize an operation when it independently satisfies the required capability, target, scope, conditions, and restrictions.

[IP-ADR-0009.]

IP-AUTH-03 — Scope Does Not Promote.

A grant scoped to a Subordinate Identity MUST NOT automatically extend to another Subordinate Identity, its Root Identity, or its governing Passport.

A Passport-scoped grant MAY cover a Subordinate Identity only when current authoritative membership and all applicable authorization requirements confirm that coverage.

Authorization established for one consumer application MUST NOT automatically confer authority upon another consumer application, even when both are associated with the same Subordinate Identity.

An application association MUST NOT independently establish Passport management authority, ownership, or permission to access unrelated identities.

Root-associated management authority MUST remain subject to its explicitly authorized capabilities, target scopes, and restrictions.

[IP-ADR-0001, IP-ADR-0002, IP-ADR-0003, IP-ADR-0009.]

IP-AUTH-04 — Capabilities, Delegation, and Recovery Authority.

`Use`, `Issue`, and `Delegate` MUST remain distinct authorization capabilities.

Grants MUST be non-delegable by default.

Delegated authority MUST NOT exceed the valid delegable authority of its issuer and MUST remain subject to the applicable target, scope, conditions, restrictions, and lifecycle requirements.

Delegation MUST NOT independently transfer identity ownership.

Recovery, succession, and ownership transfer MUST be treated as distinct protected operations and MUST NOT be inferred from ordinary `Use`, `Issue`, or `Delegate` permissions.

A Recovery Root Token MAY possess authority equivalent to its associated Root Identity for the explicitly authorized purpose of recovery.

Such equivalent authority MUST NOT extend beyond the recovery operation’s permitted scope.

A Recovery Root Token MUST NOT authorize creation of new Root Identities or Subordinate Identities, ordinary identity management unrelated to recovery, or unrestricted delegation.

Successful recovery MUST permanently invalidate the superseded Root authority and the consumed Recovery Root Token.

No delegated or recovery authority MAY bypass an object’s applicable lifecycle restrictions, including the restricted `Inactive` state of orphaned objects.

[IP-ADR-0004, IP-ADR-0006, IP-ADR-0007, IP-ADR-0008, IP-ADR-0009.]

IP-AUTH-05 — Safeguards Do Not Create Authority.

Authentication strength, credential possession, security classifications, application trust, Passport management permissions, successful Posture Validation, consumer roles, recovery eligibility, administrative status, reconciliation status, or possession of identity identifiers MUST NOT independently establish identity authority.

These safeguards and qualifications MUST NOT replace a complete, current authorization path satisfying the requested operation's capability, target, scope, lifecycle, and security requirements.

A trusted application MUST NOT assume authority over an identity merely because its trust relationship is valid.

An application possessing Passport management-level permission MUST NOT exercise that permission without satisfying the applicable operation-specific authorization and user-consent requirements.

Successful Posture Validation establishes only that the specified checks passed within the scope, evidence, and conditions evaluated. It MUST NOT independently grant authorization to access or manage an identity.

Authentication establishes the actor's identity for an operation. It MUST NOT independently establish ownership or permission to perform that operation.

[IP-ADR-0004, IP-ADR-0005, IP-ADR-0009, IP-ADR-0012, IP-ADR-0013.]

IP-AUTH-09 — Trust Acceptance Is Independent and Scoped.

An appropriately authorized individual, organization, or community MAY independently accept, withhold, or withdraw trust in an authority within its legitimate scope. Recognition by one participant MUST NOT require recognition by another. No universal central authority or trust anchor is required.

One participant's withholding or withdrawal of trust MUST NOT, solely by that act, invalidate another participant's trust decision or revoke, extinguish, or transfer an identity owned by another user. Recognition of trust MUST NOT independently grant identity ownership, Root issuance authority, Passport Management permission, or operation-specific authorization.

The mechanisms for recording, representing, distributing, and withdrawing trust and the effects on dependent attestations remain open under OPEN-14. [IP-ADR-0014.]

This operation’s authority

Resolve One Subordinate uses the reference capability `IdentityResolve` (`identity.resolve`), grant mode `Use`, exact `SubordinateIdentity(target)` scope, and the `Routine` floor for this lookup only. `Routine` requires an authenticated assurance; `Unspecified` is denied. The consumer cannot select or lower this floor. This rule does not set floors for binding or lifecycle operations. [IP-ADR-0009; related IP-ADR-0001 and IP-ADR-0012.]

Current state, not a lease

IP-AUTH-06 — Current Authority, Not a Permanent Lease.

A successful identity resolution, binding, assertion acceptance, or authorization decision MUST NOT establish permanent or reusable authority for subsequent protected operations.

Each subsequent protected operation MUST independently evaluate its current authorization requirements.

Changes to grants, application associations, controlling authority, credentials, lifecycle state, or relevant security conditions MUST be respected by subsequent authorization decisions.

An application MUST NOT treat a previously successful identity resolution as continuing permission to access or manage that identity.

Following successful Recovery Root Token activation and completion of the applicable recovery transition, superseded Root authority and consumed recovery credentials MUST remain permanently invalidated.

[IP-ADR-0007, IP-ADR-0009.]

IP-AUTH-07 — Revalidate Protected Mutations.

Protected identity-management and lifecycle mutations MUST revalidate all commit-relevant authorization and security conditions before the mutation is committed.

This validation MUST include applicable authority paths, target and scope, lifecycle eligibility, authoritative membership, credential and recovery state, controlling authority, and relevant security generations or versions.

Recovery, ownership transfer, delegation, succession, and Subordinate Identity reassignment MUST NOT succeed using authorization invalidated by an intervening relevant change.

When transferring recovered Subordinate Identities to a replacement Passport, the authoritative transition MUST prevent simultaneous active control through conflicting Passport or Root authorities.

An uncertain, failed, or aborted validation commit MUST NOT be treated as successful authorization.

Implementations MUST preserve these guarantees without requiring a particular database engine, transaction mechanism, or storage architecture.

[IP-ADR-0006, IP-ADR-0007, IP-ADR-0008, IP-ADR-0009.]

IP-AUTH-08 — Authority and Lifecycle Are Separate.

Authorization decisions MUST NOT independently change an identity's lifecycle state.

An identity's lifecycle eligibility MUST NOT independently establish authority to perform an operation.

Any Identity Passport object determined to be orphaned MUST enter the existing restricted `Inactive` lifecycle state with an explicit orphaned reason or condition.

An orphaned object MUST NOT continue ordinary identity operations or exercise authority that depends upon an unavailable or invalid controlling relationship.

Restoring an orphaned object from `Inactive` MUST require an explicitly authorized recovery, reconciliation, or other approved lifecycle operation.

Absence, inactivity, silence, or loss of contact MUST NOT be interpreted as consent to recovery, reassignment, ownership transfer, or succession.

An inactive or orphaned identity MUST NOT become available for unauthorized management merely because its previous owner cannot be contacted.

[IP-ADR-0008, IP-ADR-0009.]

Lifecycle and privacy

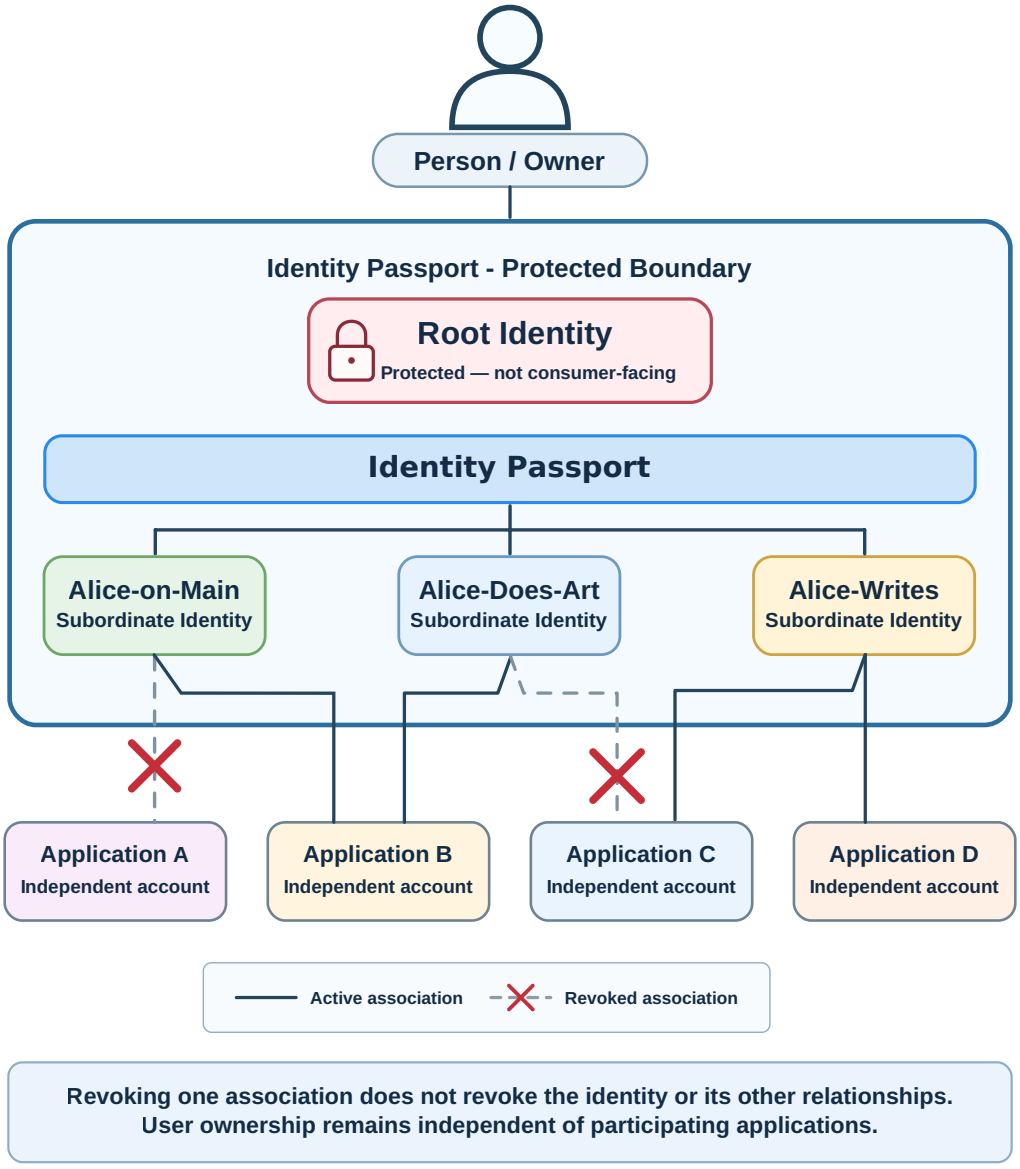
This chapter states approved lifecycle requirements at the semantic level. Recovery, succession, and orphan-handling mechanisms that remain open are not specified here.

IP-LC-01 — One current membership. A committed Subordinate membership change leaves exactly one authoritative Passport for an active Subordinate; conflicting work cannot create dual control or an active orphan. [IP-ADR-0001, IP-ADR-0003, IP-ADR-0007.]

IP-LC-02 — Binding is not a grant. A consumer mapping identifies one candidate Subordinate; it is not a Passport authorization record. Revoking or replacing the mapping affects the local binding, not Passport grants. [IP-ADR-0003, IP-ADR-0009.]

Identity Passport — Associations and Revocation

One subordinate may be associated with multiple independent applications



Informative illustration of independent application associations and selective revocation. Association is not authority; applicable grants and policy still govern each operation. Licensed CC BY-SA 4.0.

Open the application associations and revocation diagram at full size (SVG)

IP-LC-03 — Privacy-minimized output. A one-target resolve operation returns only the opaque consumer reference. It does not disclose Root continuity, siblings, Passport IDs, grant paths, unrelated Accounts, or private binding history. [IP-ADR-0002, IP-ADR-0009.]

IP-LC-04 — Privacy across failures. After consumer authentication, hidden target existence and authority relationships are not disclosed by denial, lookup, retry exhaustion, or operational failure. Telemetry and restricted diagnostics MUST NOT include identity keys. [IP-ADR-0002, IP-ADR-0009.]

IP-LC-05 — Retirement and deletion are distinct. Voluntary retirement and privacy-first deletion are separate lifecycle actions. Detailed disposition, retention, deletion-accounting, and external reconciliation requirements remain subject to reconciliation with the accepted historical decisions and applicable unresolved questions.

IP-LC-06 — Trusted, consented creation. Root Identity creation MUST require a requesting application trusted under the applicable application-trust mechanism, Passport management-level permission, and the prospective owner's explicit opt-in. These cumulative conditions establish eligibility to request creation, not automatic authorization or guaranteed acceptance. Creation MUST NOT occur as a side effect of registration, account creation, authentication, or an unrelated operation. The facilitating application MUST NOT thereby become owner or acquire exclusive future management authority. [IP-ADR-0003, IP-ADR-0005.]

IP-LC-07 — Optional initial Subordinate. Root creation MUST NOT require simultaneous Subordinate creation. An application MAY offer initial Subordinate creation with Root creation, but the prospective owner MUST be able to decline it without losing an otherwise eligible Root creation request solely for that reason. Each Subordinate creation MUST require applicable authorization and explicit user consent. [IP-ADR-0001, IP-ADR-0005.]

IP-LC-08 — Delegation, succession, and ownership transfer. Delegation MUST grant bounded authority without transferring ownership, and the delegate MUST NOT exceed that grant. Succession MUST require an explicitly authorized arrangement and protected activation; it MAY transfer specified control without ownership. Absence, inactivity, loss of contact, or presumed death MUST NOT alone activate succession or consent to ownership transfer. Ownership transfer MUST be initiated by the current owner and accepted by the intended recipient through the applicable protected authorization process. It MUST NOT automatically transfer unrelated identities, credentials, application accounts, or resources. An administrator, application, delegate, or successor MUST NOT acquire ownership solely through an existing role. [IP-ADR-0004, IP-ADR-0006.]

IP-LC-09 — Default recovery and restricted recovery authority. An Identity Passport MUST have at least one viable recovery path by default. The owner MAY explicitly elect a no-recovery configuration only through the protected Class 4 Critical process. Ordinary administration MUST NOT remove or disable the final viable recovery path. Security-class safeguards do not replace the required owner authority. This default does not require a Recovery Root Token or prescribe a recovery mechanism; recovery mechanisms and procedures remain subject to OPEN-11. A Passport MAY provide an optional Recovery Root Token as a separately

provisioned recovery credential associated with its existing Root. It MUST NOT be a second Root or independently active Passport authority. It MAY authorize only an explicitly authorized recovery operation and MUST NOT authorize new Root or Subordinate creation. Authorized recovery MAY select zero, some, or all existing Subordinates for a replacement Passport under a new Root; recovered Subordinates MUST retain identity continuity. A successful recovery transition MUST permanently invalidate superseded Root authority and the consumed token and MUST NOT leave a recovered Subordinate active under conflicting Passport or Root authorities. Token possession MUST NOT bypass applicable safeguards or authorize ordinary creation, unrelated management, unrestricted delegation, or consumer operations. Recovery MUST NOT transfer unrelated identities, credentials, accounts, ownership rights, or resources. [7H; IP-ADR-0007, IP-ADR-0009; OPEN-11.]

IP-LC-10 — Inactive and orphaned objects. `Inactive` is a restricted state that retains an object's identity and continuity while making it ineligible for ordinary operations requiring an active object. It does not mean deletion, abandonment, forfeiture, reassignment, disclosure, succession, or transfer of ownership or control, and creates no authority. An object determined to be orphaned MUST enter `Inactive` with a recorded orphan reason or condition. State-changing operations MUST satisfy applicable current authorization, security, and lifecycle conditions. Orphan detection criteria, state propagation, retention, restoration mechanisms, and disposition remain open under OPEN-12. [IP-ADR-0008–IP-ADR-0009.]

IP-LC-11 — Recovery replacement constraints. The replacement Passport and new Root are established through an authorized recovery workflow; a Recovery Root Token is not an unrestricted Root-creation capability. Recovery initiation, competing-claim protection, selection and transfer protocol, zero-Subordinate token-consumption semantics, coordination, and disputed or compromised-credential procedures remain unresolved and MUST NOT be inferred here. [IP-ADR-0007, IP-ADR-0010.]

Resolve One Subordinate

Request meaning

IP-RES-01 — One target. A resolve request concerns exactly one Subordinate Identity selected from a trusted consumer-side binding. It uses `identity.resolve`, `Use`, exact target scope, and `Routine` class for this operation only. [ADR 8C, 8G; canonical resolver contract, Exact read capability and scope.] [IP-ADR-0001, IP-ADR-0003, IP-ADR-0009.]

IP-RES-02 — Trusted context. The consumer instance, Principal, separately mapped Account, target, and opaque consumer reference come from trusted server-side context. An untrusted browser-supplied Passport ID or caller-selected assurance is not authority. Missing, mismatched, inactive, or unspecified association denies. [ADRs 8B, 8G, 8S-A; resolver contract, Contract.] [IP-ADR-0002, IP-ADR-0009, IP-ADR-0012.]

Result and resolution point

IP-RES-03 — Opaque result. Success returns only the exact `ConsumerIdentityRef`; it does not serialize Passport IDs, Root IDs, Subordinate IDs, grant data, version vectors, or reusable authorization claims. [ADRs 7P, 8D, 8G; resolver contract, Contract.] [IP-ADR-0002, IP-ADR-0009.]

IP-RES-04 — Current coherent view. Authorization evaluates a coherent view of target membership, grants/provenance, restrictions, lifecycle/continuity, association, security generation, and authoritative time. [ADRs 8G–8H, 8J-A, 8L-A–8M-A, 8S-A–8U-A.] [IP-ADR-0009, IP-ADR-0012.]

IP-RES-05 — Linearized result. A concurrent relevant mutation is either reflected in the decision or ordered after the resolution point. The point is the authoritative-time sample only when Passport validation commits successfully and the consumer's local mapping/session snapshots bracketing it agree. [ADR 8H; resolver contract, Cross-database resolution protocol and linearization point.] [IP-ADR-0009.]

IP-RES-06 — Uncertain commit fails closed. Failed, aborted, or uncertain validation commit establishes no successful resolution point and returns no success. Stale state restarts the complete attempt within a bounded internally configured retry limit. Exhaustion returns generic `IdentityUnavailable`. [ADRs 8H, 8K-A, 8L-A.] [IP-ADR-0009.]

IP-RES-07 — Local bracketing. The consumer re-reads its Account/Principal mapping, target binding, consumer context, and session/security generation after Passport validation. A

changed version or inactive mapping discards the result and restarts within bounded retry. The two databases are not one transaction. [ADRs 8H, 9F-A; resolver contract, Cross-database resolution protocol.] [IP-ADR-0003, IP-ADR-0009.]

IP-RES-08 — No stale cache. A cached result may be used only with equivalent proof of current local mapping and Passport state and a fresh authorization evaluation; the initial reference slice does not cache resolve outcomes. [ADR 8G; resolver contract, cache rule.] [IP-ADR-0009.]

Observable failures

IP-RES-09 — Failure privacy. For authenticated consumers, unknown/unbound/revoked references, denied authority, stale state, database/adapter failure, overload after admission, and retry exhaustion share one transport-safe generic failure shape. Do not expose target-specific detail. Unauthenticated requests may receive the ordinary authentication-required response before lookup. Immediate admission rejection occurs before target lookup and uses a generic response; a scheduler cannot promise exact packet arrival time. [Resolver contract, Denial and failure privacy / Bounded asynchronous scheduling.] [ADR 8G; resolver contract, Denial and failure privacy and Bounded asynchronous scheduling.] [IP-ADR-0009, IP-ADR-0011.]

The exact public status code, response schema, timing profile, transport, and operation versioning remain open questions. See OPEN-01, OPEN-05, and OPEN-07.

Binding and provisioning lifecycle

Binding establishes a consumer-local association through a protected ceremony. It does not grant ongoing Passport authority.

Challenge and assertion

IP-BIND-01 — One-time challenge. The consumer creates an unpredictable challenge tied to its current Account/session generation, consumer instance, purpose, expected mapping version, and (for a Subordinate binding) exact reference and target. It expires and is consumed at most once. [Resolver contract, Challenge and assertion issuance; ADR 9F-A.] [IP-ADR-0003, IP-ADR-0009, IP-ADR-0010.]

IP-BIND-02 — Trusted issue. Only a trusted Passport issuer creates binding evidence after fresh Principal authentication and current Account/Principal association validation. A Subordinate bind also evaluates complete current exact-target `IdentityResolve` Use authority. [ADRs 8K-A, 8L-A, 8S-A, 8T-A.] [IP-ADR-0005, IP-ADR-0009, IP-ADR-0012.]

IP-BIND-03 — Bound claims. Evidence binds issuer, audience/consumer instance, purpose, challenge/assertion ID, issue/expiry, distinct Account and Principal, relevant security/association generations, and exact consumer reference/target when applicable. Cryptographic encoding is profile-specific. [Resolver contract, Challenge and assertion issuance; ADRs 8S-A, 9F-A.] [IP-ADR-0003, IP-ADR-0012.]

Live acceptance and local installation

IP-BIND-04 — Live acceptance. Signature verification alone is insufficient. Passport rechecks current issuer trust/status, audience, purpose, challenge, exact claims, expiry, replay/revocation state, current Account/Principal association and security generation, and exact-target authority before accepting. Acceptance is single-use and records an opaque receipt. [ADRs 8K-A–8M-A, 8S-A, 8T-A, 9F-A.] [IP-ADR-0009, IP-ADR-0012.]

IP-BIND-05 — Stable retry. Repeating the same acceptance operation ID returns the same receipt idempotently. Re-presenting an accepted assertion with a different operation ID is replay and is rejected. [ADR 9F-A; resolver contract, Live Passport acceptance contract.] [IP-ADR-0009.]

IP-BIND-06 — Separate commits. Passport acceptance and consumer mapping installation are distinct committed facts in separate databases. The receipt proves Passport acceptance only. The consumer revalidates challenge/session/context/mapping versions and performs local

mapping update plus audit atomically under compare-and-swap. [ADRs 8H, 9F-A.] [IP-ADR-0003, IP-ADR-0009.]

IP-BIND-07 — No implied authority. Neither an assertion, receipt, nor local mapping grants a later resolve or protected action. Each later operation evaluates current authority. [ADRs 8G–8H.] [IP-ADR-0009.]

IP-BIND-08 — Uncertain local result. If the local commit is uncertain, check the local idempotency record; report installation only when mapping and audit are known committed. Retry only the same local operation with the same Passport receipt. If challenge or expected version changed, require fresh proof. A post-acceptance revocation does not erase the acceptance record, but cannot authorize future resolve. [Resolver contract, Local installation and cross-database behavior; ADR 9F-A.] [IP-ADR-0009.]

The Passport acceptance commit is not by itself the complete local provisioning result. Do not describe the two stores as distributed-atomic.

Security and privacy considerations

IP-SEC-01 — Fail closed. Missing trusted association, invalid proof, stale or unavailable authoritative state, expired/revoked evidence, or uncertain validation commit cannot produce success. A bounded version conflict may retry; missing authority or uncertainty is not converted to permit. [ADRs 8G–8H, 8K-A–8M-A, 8S-A–8U-A.] [IP-ADR-0009.]

IP-SEC-02 — Limit disclosure. Return only the exact opaque consumer reference after successful resolve. Keep response and telemetry from revealing hidden targets, Root/sibling relationships, account links, grant paths, or identity keys. [ADRs 7P, 8D–8G, 8R-A.] [IP-ADR-0002, IP-ADR-0009.]

IP-SEC-03 — Resist replay. Bind evidence to audience, purpose, challenge, actor, operation, target, state/generation, and authoritative expiry; enforce one-time acceptance and context-bound idempotency. [ADRs 8S-A, 9F-A.] [IP-ADR-0009.]

IP-SEC-04 — Bound work. Admission, asynchronous waiting, blocking execution, connections, deadlines, retries, and cancellation must be bounded so timed-out work remains accounted for until safely stopped. Numeric limits and runtime mechanisms are deployment/profile choices. [Resolver contract, Bounded asynchronous scheduling and execution; ADR 8H.] [IP-ADR-0009.]

IP-SEC-05 — Identity and data ownership. System-of-record stewardship, hosting, administration, or technical custody MUST NOT independently confer ownership of a user’s identity or user-owned identity data.

Identity Passport MUST preserve the user’s ownership of their identity and control over their identity data, subject to the applicable ownership, authorization, privacy, and lifecycle requirements. This does not imply ownership of unrelated third-party information. Ownership, control, authentication, administration, and authorization remain distinct. [IP-ADR-0004, IP-ADR-0008.]

IP-SEC-06 — Secure transport properties. All Identity Passport data transmitted between participating systems MUST use an approved secure transport protocol appropriate to the applicable communication and trust context.

An approved transport MUST provide:

- **Confidentiality:** Protection against unauthorized disclosure of Identity Passport data in transit.
- **Integrity:** Protection against undetected alteration of transmitted data.
- **Endpoint authentication:** A means of verifying the identity or authorized identity context of communicating endpoints.

- **Replay protection:** Effective safeguards against unauthorized reuse of previously valid messages or protocol exchanges.

Implementations MUST NOT assume that use of a secure transport protocol independently establishes application trust, identity ownership, or authorization to perform a requested operation.

Transport security MUST remain separate from the Passport application-trust bootstrap and the authorization decisions governing identity operations.

The standard MUST NOT require a particular transport technology where alternative protocols satisfy the approved security and interoperability requirements.

Transport approval MUST evaluate the required security properties in the context of the protocol's actual threat model and deployment conditions.

An implementation MUST NOT weaken these transport protections merely because the communicating systems share an operator, network, hosting environment, or participating application. [IP-ADR-0011.]

IP-SEC-07 — Passport verification and trust boundaries. Identity Passport MUST maintain an application-independent identity verification and authorization boundary.

Participating applications MAY serve as entry points through which users authenticate, present identity evidence, or request authorized Identity Passport operations.

Identity Passport MUST NOT require every participating application to use the same authentication method.

Identity Passport MUST NOT be required to implement every authentication method used by participating applications.

A participating application MAY present evidence established through an external authentication mechanism, provided the evidence is acceptable under the applicable Passport verification and trust policies.

Identity Passport MUST evaluate the evidence and applicable authority requirements before accepting it for a protected Passport operation.

Evidence supplied by an application MUST NOT independently establish identity ownership, Root authority, Passport management authority, or permission to perform a requested operation.

Acceptance of authentication evidence MUST remain distinct from authorization of a particular operation.

A trusted application MUST NOT be treated as having unrestricted authority over identities merely because Passport recognizes its trust relationship.

Applications facilitating Passport management MUST satisfy applicable application-trust, management-permission, user-consent, and complete-path authorization requirements.

The application that facilitates identity verification or Root creation MUST NOT thereby acquire ownership of the identity or exclusive authority over its future management.

Identity Passport MUST preserve the independence of its identity relationships from the applications through which users authenticate or manage those identities. [IP-ADR-0012.]

IP-SEC-08 — Operation security classes and proof requirements. Security classes select safeguards for a protected operation; they MUST NOT independently grant a capability or replace complete-path authorization. The applicable workflow MUST assign its minimum class. A caller MUST NOT select or lower that floor. [7F, 8S-A, 8W-A; IP-ADR-0009.]

Class	Name	Required safeguards
1	Routine	Active valid session, authenticated context, and explicit capability.
2	Administrative	Fresh authentication, scope evaluation, and audit.
3	Sensitive	Fresh authentication, explicit confirmation, notification, audit, and operation-bound Class 3 proof.
4	Critical	Strong authentication, ownership and continuity checks, impact preview, operation-bound Class 4 proof, and delayed/cancellable execution where appropriate.
5	Emergency	Restricted recovery or compromise procedures, narrowly defined authority, enhanced audit, and operation-bound Class 5 proof.

Evidence used to satisfy a security-class floor MUST be bound to the actor, operation, exact target, relevant versions, purpose, and authoritative expiration. Classes 3–5 require operation-bound proof of the corresponding class. Class satisfaction supplements all actual authorization and other applicable conditions. [8S-A.]

Issuer compromise, trust-anchor/key rotation, independently auditable fresh authentication, public error/timing policy, and deployment integration remain open questions. These gaps block production and interop claims; they do not silently alter the candidate semantic rules.

Conformance boundary

This page is a proposal for public review, not a certification or evidence of implementation compliance.

IP-CONF-01 — Bounded claim. A semantic conformance statement identifies the exact candidate clauses and profiles tested; it must not imply independent certification or wire interoperability. See OPEN-08. [IP-ADR-0009, IP-ADR-0010, IP-ADR-0013.]

Semantic candidate

A semantic implementation claim should identify the clauses tested and demonstrate at least:

1. Exact-target `Use` authorization and denial for expired, restricted, out-of-scope, non-member, and incomplete-path cases (`IP-AUTH-01`, `IP-AUTH-03`, `IP-RES-01`).
2. No path pooling, scope promotion, or authority from identity references or security class (`IP-AUTH-02`–`IP-AUTH-05`, `IP-ID-06`).
3. Opaque one-target output and privacy-preserving failures, including telemetry constraints (`IP-RES-03`, `IP-RES-09`, `IP-LC-03`–`IP-LC-04`).
4. A coherent resolution point under concurrent association, grant, restriction, membership, lifecycle, and generation changes (`IP-RES-04`–`IP-RES-06`).
5. No success after failed or uncertain validation commit; bounded retry and generic exhaustion (`IP-RES-06`).
6. No stale local mapping/session generation across the Passport resolution point (`IP-RES-07`).
7. No lease semantics: later protected operations reauthorize (`IP-AUTH-06`).
8. Single-use binding acceptance, same-operation receipt recovery, different-operation replay rejection, and distinct local CAS installation (`IP-BIND-04`–`IP-BIND-06`).
9. Uncertain local commit recovery through local idempotency state without duplicate installation (`IP-BIND-08`).
10. Bounded admission/execution/cancellation behavior for any implementation claiming the resolver resource-bound profile (`IP-SEC-04`).

These are candidate semantic obligations. Their exact test harness, mandatory subset, error transport, and timing tolerances remain subject to OPEN-05, OPEN-07, and OPEN-08.

Named profiles

IP-CONF-02 — Named profile claim. A profile names specific assertion encoding, issuer trust, transport, key lifecycle, error behavior, and test vectors. `ipa1` is a candidate optional profile only. A profile-level claim must identify its version and pass its own published vectors. See OPEN-02 and OPEN-08, plus the profile page. [IP-ADR-0010, IP-ADR-0011, IP-ADR-0012.]

Implementation evidence

IP-CONF-03 — Evidence provenance. PostgreSQL lock tests, Rust test counts, Aardwolf session behavior, operational runbooks, and deployment settings support claims about a pinned implementation revision. They do not establish universal interoperability or production readiness. [ADR 8H; canonical validation plan and resolver contract.] No implementation evidence is independently reproduced or approved for publication with this site. See evidence status. [IP-ADR-0010.]

IP-CONF-04 — Core conformance floor. Identity Passport conformance MUST be evaluated against explicitly defined, approved requirements and applicable profiles. An implementation claiming Identity Passport Core conformance MUST satisfy all applicable mandatory Core requirements.

Core requirements constitute the minimum mandatory conformance baseline. Implementations MUST NOT claim Core conformance by selectively excluding, waiving, or substituting mandatory Core requirements.

Assessment profiles MAY extend the Core baseline with additional checks, but MUST NOT weaken or replace mandatory Core requirements.

Assessment requirements and guidance MAY be classified using established categories, including:

- **Core:** Mandatory requirements for implementations claiming Core conformance.
- **Best Practice:** Recommended practices that are not themselves mandatory Core requirements.
- **Optional:** Capabilities or profiles that implementations may elect to support.

Assessment profiles MAY address particular domains, including Security and Privacy. Future profile types MAY be defined through the applicable specification and governance process.

Validation Results and Disclosure

Public disclosure of detailed Posture Validation findings and evidence MUST be optional unless an independently applicable, explicitly approved policy establishes a disclosure obligation. Management-capable applications MUST make the public disclosures, current standing, and history access required by this specification. This limited duty does not require publication of detailed findings or sensitive evidence.

An implementation MAY disclose a simple validation status without publishing detailed findings.

Where permitted by the applicable policy, an implementation MAY disclose a numerical result, such as the number of applicable checks passed.

Numerical results MUST NOT imply that mandatory Core failures can be offset by passing optional checks.

Detailed assessment findings MAY be made available to appropriately authorized viewers for testing, debugging, demonstration, governance, or interoperability evaluation.

Assessment and Validation disclosures MUST respect applicable privacy, security, and information-disclosure restrictions.

A system MUST NOT require public disclosure of sensitive assessment or validation evidence merely to demonstrate that validation was performed.

Assessment Evidence

Posture Validation results MAY form part of the evidence considered during implementation evaluation, interoperability review, or application-trust decisions.

Such evidence MUST NOT independently replace the application-trust, authentication, Management-permission, explicit user-consent, or complete-path authorization requirements applicable to a protected operation. [IP-ADR-0013.]

IP-CONF-05 — Management application transparency. An application seeking or exercising Passport Management permissions MUST openly disclose what Passport-related identity information it collects, stores, processes, and transmits; how it protects that information and the user’s ownership; and which Management operations it seeks or performs. Disclosures MUST be accessible without requiring publication of protected identity information, credentials, secrets, or confidential security details. [IP-ADR-0013; OPEN-17.]

IP-CONF-06 — Assessment and Validation are distinct. Posture Assessment MUST record the application’s declarations about its behavior and practices. Claims MUST be distinguished from facts established by evidence. Posture Validation MUST evaluate those claims and

applicable evidence against approved requirements and the applicable profile, producing an attributable PASS or FAIL for a stated scope and conditions. Assessment and Validation MAY occur within one operational process but MUST remain conceptually distinct. A declaration-only check MUST NOT be represented as proof of implemented behavior. A successful Validation MUST NOT be represented as universal security certification, proof that an implementation is vulnerability-free, production readiness, a permanent guarantee of continuing compliance, or an independent grant of identity ownership, Passport authority, or permission to perform protected operations. [IP-ADR-0013; OPEN-08.]

IP-CONF-07 — Validation evidence and eligibility. Profiles MUST state the evidence and assurance level required for their validation results and whether Independent Validation is required. Self-Validation is an application's evaluation of its own implementation for finding deficiencies, remediation, and ongoing compliance. Independent Validation is compliance evidence established independently of the evaluated application. Self-Validation MUST NOT be represented as Independent Validation and MUST NOT satisfy an applicable Independent Validation requirement. A passing Independent Validation establishes compliance only within the approved requirements, evidence, scope, and conditions evaluated. Passing an applicable Posture Validation MAY establish eligibility to participate in a Passport trust or interoperability arrangement where that arrangement requires such validation. Eligibility MUST NOT be confused with trust or authorization. Neither process independently grants Management authority, Root issuance authority, identity ownership, explicit consent, or operation-specific authorization. [IP-ADR-0013; OPEN-08.]

IP-CONF-08 — Initial and continuing Validation. An application that elects to participate in an approved Identity Passport profile MUST pass the initial Posture Validation required by that profile before eligibility under it. This requirement does not make Identity Passport participation mandatory for an application instance using only local authentication. A participating application MUST maintain current validation to remain in good standing and continue exercising permissions that require that status. Applicable profiles MUST require recurring validation and reassessment following material changes or significant incidents. They MUST specify maximum validation intervals, evidence validity, triggers, and standing consequences. No numerical interval or grace period is set by this requirement. Loss of application standing MUST NOT extinguish or transfer a user-owned identity or prevent its management by another appropriately authorized application. [IP-ADR-0013, IP-ADR-0015; OPEN-15.]

IP-CONF-09 — Public current standing. A Management-capable application MUST make its current validation standing publicly accessible without requiring an Identity Passport account. When eligible and current, it MUST display the exact wording **"In Good Standing Since [date]"**. The date MUST be the date of its most recent successful qualifying Posture Validation, even if good standing has been uninterrupted; each later successful qualifying validation updates the date. A failed, suspended, expired, overdue, or otherwise ineligible application

MUST NOT display that positive designation as its current status. Exact negative-state wording remains open. [IP-ADR-0015; OPEN-15.]

IP-CONF-10 — Public Validation Ledger. Identity Passport MUST provide publicly accessible current standing and historical validation events and standing changes for applications covered by the applicable profile. Current standing MUST link through an ordinary link to the publicly accessible history; the history MAY be hosted separately. Readers MUST be able to verify record provenance and integrity independently of the evaluated application's assertions. The evaluated application MUST NOT exclusively control publication, alteration, suppression, or deletion of its history; later PASS results MUST NOT erase or conceal earlier failures or suspensions. Independent verification of record provenance and integrity MUST NOT be represented as Independent Validation of the application. Public records MUST comply with privacy and non-disclosure requirements and MUST NOT require publication of credentials, protected identity information, or sensitive evidence. Ledger publication, hosting, witnessing, or verification MUST NOT confer ownership or Management authority. No particular ledger technology is required. [IP-ADR-0015; OPEN-16.]

No conformance mark or interoperability statement is justified by this draft alone.

Named profiles

Profiles may define specific wire encodings or implementation requirements without changing the semantic core. A profile is not mandatory for every v0.1 semantic implementation unless separately approved.

ipa1 assertion profile candidate

Status: candidate optional profile; not a universal v0.1 requirement. The canonical Resolve One Subordinate contract records that Slice B uses an `ipa1` envelope and Ed25519 signing. That is implementation evidence and a concrete profile proposal, not by itself approval of a public interoperable standard.

The described Slice B form includes a profile marker, key ID, encoded payload, and signature. Its payload binds purpose, assertion and issuer identifiers, audience, challenge, distinct Account and Principal identifiers, Passport/security generations, optional consumer reference and Subordinate target, and issue/expiry values. The implementation uses an issuer/key allowlist and fails closed on malformed or untrusted assertions. Exact payload encoding and behavior are defined in the source contract at the pinned baseline, not restated here as universal requirements.

A future profile approval must settle the complete byte-level grammar, parser rejection rules, issuer identity and trust-anchor distribution, key rotation/revocation, lifetime/clock policy, privacy/logging rules, and positive/negative interoperability vectors. No one may infer algorithm agility, production key custody, or universal applicability from the `ipa1` name.

A conforming semantic implementation may use another separately specified mechanism. An implementation claiming `ipa1` profile compatibility must implement the approved profile exactly once it is frozen.

Glossary

This glossary defines the terms used in the semantic draft. The relationship rules and cardinalities are stated in Identity relationships.

Term	Definition	Does not imply
Account	Authentication/access relationship through which a Principal may act.	Ownership or a grant.
Administrator	Actor authorized to perform designated administrative functions.	Ownership or unrestricted authority.
Acceptance receipt	Recoverable record that Passport accepted one assertion operation.	Local installation, distributed atomicity, or later authority.
Authenticated Principal	Actor whose identity has been established through an applicable authentication mechanism.	Ownership or permission to perform an operation.
Binding assertion	Time-limited evidence for a particular association/ binding ceremony.	A standing grant or proof that state remains current.
Consumer	Registered relying application with its own local references and mapping lifecycle.	Permission to bypass Passport authorization.
ConsumerIdentityRef	Opaque, random, consumer-instance-scoped reference to one bound target.	Passport ID, Root-derived value, or transferable authority token.
Controller	Entity explicitly authorized to exercise specified control over an identity.	Ownership; control MUST NOT itself transfer ownership.
Delegate	Actor exercising explicitly granted, scoped authority.	Authority beyond the grant or ownership.
Grant	Bounded authority with issuer, grantee, capability, scope, provenance, constraints, lifetime, and state.	Authority outside its complete valid path.
Inactive	Restricted lifecycle state retaining identity and continuity while excluding ordinary operations requiring an active object.	Deletion, abandonment, forfeiture, reassignment, succession, transfer, or authority for another actor.
Owner	The user to whom an identity belongs.	Administrative, delegated, or application control by others.
Independent Validation	Posture Validation evidence established independently of the evaluated application.	Universal certification, proof beyond the evaluated scope/conditions, or authority over an identity.
Passport	Private authority and security container, distinct from governed identities.	An identity or consumer-visible identifier.

Term	Definition	Does not imply
Posture Assessment	An application's declarations about its behavior and claimed practices.	Independent proof that the implementation behaves as declared.
Posture Validation	Evaluation of assessed claims and applicable evidence against approved requirements and an applicable profile, producing PASS or FAIL for a stated scope and conditions.	A universal security certification, identity ownership, trust, Management permission, or operation authorization.
Principal	Actor evaluated for an operation; not necessarily an identity holder.	Ownership of every related identity.
Public Validation Ledger	Public current-standing information and historical validation records whose provenance and integrity can be independently verified.	A required blockchain, independent validation of application behavior, or authority to manage identities.
Recovery Root Token	Optional, separately provisioned recovery credential associated with an existing Root, limited to explicitly authorized recovery.	A second Root, unrestricted management, or identity-creation authority.
Resolution result	Evidence that one reference was authorized at one consistency point.	A lease or permission for a later operation.
Self-Validation	An application's evaluation of its own implementation to find deficiencies, remediate, and maintain compliance.	Independent Validation or independently established compliance evidence.
Root Identity	A governed identity distinct from its Passport. Every Passport has exactly one Root Identity.	Consumer visibility or implicit scope.
Successor	Actor designated to assume specified authority following an authorized succession event.	Ownership or activated authority before protected succession activation.
Subordinate Identity	Identity governed by a Passport; an active Subordinate has exactly one authoritative Passport at a time.	Authority over Root or sibling identities.

The normative non-inference requirement appears as `IP-ID-06` in Identity relationships.

Open Questions

These are open design questions, not normative requirements. OPEN-01 through OPEN-10 retain the order and subjects of the ten questions in the earlier working draft. OPEN-11 through OPEN-17 are additional permanent identifiers with no historical RFC mapping. Accepted architectural decisions are recorded in Architecture Decision Records (ADRs).

Question lifecycle

This issue-tracker-style convention governs question records and is not a Core implementation-conformance requirement.

`PUB-01` remains a separate publication-readiness tracker item and is outside the seventeen-question architectural `OPEN-nn` sequence.

- An open question is designated `OPEN-nn`.
- A closed question is designated `CLOSED-nn`, retains its numeric identifier, and displays **Formerly OPEN-nn**.
- Numeric identifiers are permanent and MUST NOT be recycled.
- Closure records MUST state the disposition and cite the supporting resolution, accepted decision, or governance action.
- A closed question MAY be reopened through the established governance process; its status returns to `OPEN-nn` with the original numeric identifier, and the reopening action is recorded.
- The register records current status; detailed deliberation and approval history MAY remain in separate governance records.

OPEN-01

Select transport, operation versioning, and request/response serialization?

Publication impact: Required for wire interoperability.

OPEN-02

Approve assertion format, issuer authentication, trust anchors, and key rotation? Is `ipa1` optional or mandatory for a named profile?

Publication impact: Required for assertion-profile interoperability and deployment trust.

OPEN-03

Define independently auditable fresh Principal authentication?

Publication impact: Required for trustworthy issuance.

OPEN-04

Define linearizable Account/Principal association semantics across authentication providers and reviewed equivalents to the reference epoch design?

Publication impact: Required for stale-association resistance.

OPEN-05

Define public denial/error codes, response shape, unauthenticated behavior, and timing guidance?

Publication impact: Required for transport-level privacy conformance.

OPEN-06

Freeze assertion acceptance receipts, operation identity, expiry/revocation races, and recovery vectors?

Publication impact: Required for cross-database provisioning interoperability.

OPEN-07

Define cancellation, deadlines, retry budgets, and resource-bound profiles?

Publication impact: Required for comparable availability/resource claims.

OPEN-08

Define the semantic minimum and profile extensions, including profile-specific evidence and assurance levels, when Independent Validation is required, and applicable validator qualifications?

Publication impact: Required for meaningful conformance claims.

OPEN-09

Define consumer registration, isolation, and portable consumer-instance identity?

Publication impact: Required for interoperable consumer lifecycle.

OPEN-10

Are any Root/authority lifecycle terms still ambiguous after alignment to the current canonical model?

Publication impact: Close by source alignment unless a specific conflict is found.

OPEN-11 — Root Recovery

How should recovery proceed when Root authority is lost, stolen, unavailable, or compromised? Define the unresolved recovery-initiation, competing-claim, fraud-safeguard, and recovery-protocol questions while preserving the approved restrictions on Recovery Root Token authority, identity continuity, and invalidation of superseded authority. No recovery mechanism is selected here.

OPEN-12 — Orphaned Object Lifecycle

How should orphaned Passport-related objects be detected, have restricted `Inactive` state propagated, retained, restored, and ultimately disposed of? The approved safeguards for `Inactive` remain in force; the lifecycle mechanisms remain unresolved.

OPEN-13 — Shared Ownership and Control

How should multiple controllers or owners, conflicting authority, control revocation, succession, and interactions with recovery be handled? The specification does not establish a multiple-owner model or resolve shared-control mechanisms.

OPEN-14 — Application Trust Bootstrap

How should participating application trust be represented, established, evaluated, distributed, and withdrawn? Appropriately authorized individuals, organizations, and communities may independently accept, withhold, or withdraw trust within their legitimate scopes; no universal trust anchor is required, and one participant's choice does not compel another's. How do withdrawal and distrust affect dependent assertions, attestations, and authorizations without revoking another participant's trust or user-owned identity? How should trust domains interoperate, and how is trust kept separate from Root issuance and Management permission? RFC 5280 and alternatives remain evaluation candidates only; no trust-bootstrap mechanism is adopted. See also OPEN-02 for assertion format, issuer authentication, trust anchors, and key lifecycle.

OPEN-15 — Recurring Validation and Standing Lifecycle

What maximum validation intervals, evidence-validity periods, material-change and incident triggers, overdue/grace conditions, and failure, suspension, remediation, restoration, contestation, and unavailable-result consequences should applicable profiles define? What effects, if any, apply to existing permissions while validation is not current? No numerical interval or response state is selected here. See OPEN-08 for profile scope and evidence/assurance levels.

OPEN-16 — Public Validation Ledger Governance

What record fields, publisher/validator roles, independent verification assurances, preservation/retention expectations, correction-without-erasure procedures, availability, and interoperability are required for the public validation history? The evaluated application cannot have exclusive control of its history. No ledger technology, cryptographic method, witness topology, or validator governance is selected here.

OPEN-17 — Management Application Disclosure

What precise public disclosures are required of applications seeking or exercising Management permissions about collection, storage, processing, transmission, protection of Passport-related data, requested Management operations, and user ownership safeguards? How should disclosures avoid exposing protected identity information, credentials, secrets, or confidential security details?

PUB-01 — Publication readiness

Who owns the website, source pin/update process, versioning, and public comment endpoint? This must be resolved before public publication; the site remains separate from the service.

Proposals

Future design submissions may be called **Proposals**. No formal proposal numbering system is established yet.

The semantic draft can be reviewed before these questions are resolved, but it must remain explicit that transport interoperability and production trust are not specified.

Implementation evidence status

No implementation evidence has been independently reviewed and approved for publication with this draft. These semantic pages make no claim of implementation readiness, production readiness, or independent certification.

A future evidence release should identify the exact source revision, invariant and requirement IDs, test command, tool/environment versions, reproducible result artifact, adversarial conditions, limitations, and reviewer. Test counts without this provenance do not establish a protocol requirement or a production claim.

The project-reported test counts supplied with the initial draft remain in the non-published review artifacts until they are independently checked and approved for publication.