IDENTITY PASSPORT

Architectural Decisions

Fifteen accepted architectural decision records

Repository HEAD revision	43b40e534a36761b72202019262bea29298c72c4
Publication tag	ip-v0.1-wd-20261113.1
Working tree status	clean
Edition source SHA-256	83ed3d841add959091e733f7216519ad887a1f3c1e92680f1cfefd210836d346
Revision date	2026-11-12
Generated	2026-11-13 (UTC)
Hugo version used	hugo v0.169.0-1da10fc44701c566b1669cdb2d12638f155138bd+extended linux/amd64 BuildDate=2026-10-27T14:52:20Z VendorInfo=gohugoio

These records preserve the accepted architectural decisions. They supplement the Identity Passport Specification v0.1 and do not replace its normative clauses.

Contents

1. IP-ADR-0001: Passport, Root, and Subordinate relationships
2. IP-ADR-0002: Multiple independent Passports and privacy
3. IP-ADR-0003: Subordinate continuity and application independence
4. IP-ADR-0004: Identity ownership and control roles
5. IP-ADR-0005: Root creation, trust, permission, and consent
6. IP-ADR-0006: Delegation, succession, and ownership transfer
7. IP-ADR-0007: Recovery Root Token and protected recovery
8. IP-ADR-0008: Orphaned objects and restricted `Inactive` state
9. IP-ADR-0009: Complete-path authorization, Revision 1
10. IP-ADR-0010: Decision and question governance
11. IP-ADR-0011: Identity Passport secure transport properties
12. IP-ADR-0012: Passport verification and trust boundaries
13. IP-ADR-0013: Identity Passport Posture Assessment and Validation
14. IP-ADR-0014: Initial Trust and Independent Acceptance
15. IP-ADR-0015: Continuous Validation and Public Standing

IP-ADR-0001: Passport, Root, and Subordinate relationships

Status: Accepted **Approval provenance:** Phase 2A-01, approved language supplied November 7, 2026.

Decision

Each Identity Passport MUST have exactly one current authoritative Root Identity.

The Root Identity is the protected source of authority for Passport identity-management and lifecycle operations. It MUST NOT be used as an ordinary consumer-facing identity or disclosed to a consumer application merely to establish a Subordinate Identity association.

A Passport MAY contain zero or more Subordinate Identities.

Root Identity creation MUST NOT automatically require or cause creation of a Subordinate Identity. Users MAY establish a Passport containing only its Root Identity.

A Passport containing only a Root Identity MAY exist for provisioning, protected management, or other non-consumer purposes. Normal consumer identity services MUST use an eligible Subordinate Identity rather than the Root.

References to Root authority describe the authorization relationship and MUST NOT be interpreted as requiring a particular cryptographic key, credential format, or storage mechanism.

Informative principle: “Root: Something to Protect. Subordinate: Something to Share.” Sharing means controlled association, not public discoverability. Root-associated authority for Passport management does not mean Root authentication is required for each ordinary consumer action.

Rationale

The Passport is an authority and management boundary. The Root is protected and distinct from identities selected for ordinary consumer use. A user can create a Passport without having to create or expose a Subordinate Identity at the same time.

Consequences

The specification must state Root and Subordinate cardinality separately from consumer identity selection. Root authority is scoped to protected Passport management and lifecycle operations. No cryptographic representation is implied by this decision.

Traceability

Related requirements: `IP-ID-01`–`IP-ID-03`, `IP-AUTH-03`. Related questions: OPEN-10, OPEN-13.

IP-ADR-0002: Multiple independent Passports and privacy

Status: Accepted **Approval provenance:** Phase 2A-02, approved language supplied November 7, 2026.

Decision

A person MAY own and control multiple independent Identity Passports.

Each Passport MUST maintain its own authoritative Root Identity and its own identity-management relationships.

Possession, ownership, or control of one Passport MUST NOT automatically establish authority over another Passport.

Implementations MUST NOT automatically disclose, correlate, or link a person's independent Passports merely because they share an owner, controller, application, authentication method, or other characteristic.

Any cross-Passport relationship or disclosure MUST satisfy the applicable explicit authorization, privacy, and consent requirements.

Rationale

Multiple Passports can support distinct identity contexts without making shared ownership or shared authentication a discovery or linking mechanism.

Consequences

Passport cardinality is independent of person cardinality. Implementations must preserve isolation across Passports and require applicable authorization, privacy and consent for cross-Passport relationships or disclosures.

Traceability

Related requirements: `IP-ID-03`, `IP-ID-05`, `IP-SEC-02`. Related question: OPEN-13.

IP-ADR-0003: Subordinate continuity and application independence

Status: Accepted **Approval provenance:** Phase 2A-03, approved language supplied November 7, 2026.

Decision

Each active Subordinate Identity MUST have exactly one current authoritative Passport relationship.

A Subordinate Identity MAY be associated with multiple independent consumer applications simultaneously.

Each application association MUST be explicitly authorized within its applicable scope and MUST be independently revocable.

An association with one application MUST NOT automatically establish an association with another application or provide access to unrelated Subordinate Identities.

A Subordinate Identity MUST retain its identity continuity independently of any particular consumer application's account, display name, or continued participation.

Changing an application's account name, changing a Subordinate Identity's presentation name, or discontinuing an application association MUST NOT by itself create a new Subordinate Identity or transfer ownership.

A trusted and appropriately authorized Passport-management application MAY facilitate management of an existing Passport, subject to the owner's applicable authorization and consent.

The application that initially facilitated Root creation MUST NOT acquire permanent exclusive management authority, ownership, or a veto over subsequent authorized management by other applications.

Leaving a consumer application MUST NOT automatically terminate the user's Passport.

Leaving Identity Passport MUST NOT automatically require termination of an otherwise independently maintained consumer-application account.

Rationale

Passport identity continuity and user ownership must not depend on one consumer application's account, naming or continued operation. Multiple applications can participate independently under explicit, scoped and revocable authorization.

Consequences

The standard distinguishes Passport identity relationships from consumer-local accounts and associations. Application trust or participation does not confer ownership, permanent control or access beyond an expressly authorized scope.

Traceability

Related requirements: `IP-ID-02`–`IP-ID-04`, `IP-LC-02`, `IP-BIND-*`. Related questions: OPEN-09, OPEN-13.

IP-ADR-0004: Identity ownership and control roles

Status: Accepted **Approval provenance:** Freshly approved Identity Ownership and Control passage, supplied November 7, 2026.

Decision

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.

The following roles MUST remain conceptually distinct:

- **Owner:** The user to whom the identity belongs.
- **Controller:** An entity explicitly authorized to exercise specified control over an identity.
- **Administrator:** An actor authorized to perform designated administrative functions.
- **Delegate:** An actor exercising explicitly granted, scoped authority.
- **Successor:** An actor designated to assume specified authority following an authorized succession event.
- **Authenticated Principal:** An actor whose identity has been established through an applicable authentication mechanism.

Authentication, administration, delegation, application trust, or control MUST NOT independently establish ownership.

Multiple controllers MAY be supported where explicitly authorized through the applicable owner-controlled process.

Granting, sharing, or transferring control MUST NOT automatically transfer ownership.

An issuing or participating application MUST NOT acquire ownership merely by creating, hosting, attesting to, or managing an identity.

Loss of contact, inactivity, absence, or inability to authenticate MUST NOT be treated as consent to ownership transfer or succession.

An identity does not become someone else's simply because its owner is no longer present.

The handling of simultaneous controllers, multiple owners, conflicting claims, revocation, and their relationship to succession and recovery remains unresolved under OPEN-13.

Rationale

Identity ownership belongs to the user and is independent from application participation and from the actors or mechanisms that authenticate, administer or exercise delegated control.

Consequences

The specification must use these roles distinctly. Control arrangements do not silently change ownership. Unresolved multi-controller and multi-owner models remain open and must not be filled in by implementation convention.

Traceability

Related requirements: `IP-ID-04`, `IP-ID-06`, `IP-AUTH-05`. Related question: OPEN-13.

IP-ADR-0005: Root creation, trust, permission, and consent

Status: Accepted **Approval provenance:** Freshly approved Root Identity Creation Requirements passage, supplied November 7, 2026.

Decision

Creation of a Root Identity MUST require all three of the following conditions:

1. The requesting application is trusted under the applicable Identity Passport application-trust mechanism.
2. The requesting application possesses Passport management-level permission.
3. The prospective identity owner explicitly opts in to Root Identity creation.

These conditions are cumulative. Satisfying them establishes eligibility to request Root creation, not automatic authorization or guaranteed acceptance.

Root Identity creation MUST NOT occur automatically as a side effect of application registration, account creation, authentication, or another unrelated operation.

The requesting application MUST NOT become the owner of the Root Identity merely because it facilitated creation.

A trusted, appropriately authorized Passport-management application MAY facilitate creation of Subordinate Identities within an existing Passport, subject to applicable Root-associated authorization and user consent.

The application that initially facilitated Root creation MUST NOT possess an inherent exclusive right to manage that Passport or prevent subsequently authorized management by another application.

Optional Initial Subordinate Creation

Root Identity creation MUST NOT require simultaneous creation of a Subordinate Identity.

An application MAY offer initial Subordinate creation alongside Root creation, but the prospective owner MUST be able to decline the Subordinate without being denied an otherwise eligible Root creation request solely for that reason.

Creation of each Subordinate Identity MUST require the applicable authorization and explicit user consent.

The application-trust bootstrap mechanism remains unresolved under OPEN-14. RFC 5280 is a candidate for evaluation, not an adopted requirement.

Rationale

Root creation is a protected, user-directed operation. Application trust and management permission establish eligibility to request it; neither replaces explicit consent or operation-specific authorization.

Consequences

Root creation is never an implicit side effect. A Root may exist without a Subordinate. The creating application acquires neither ownership nor exclusive future management rights. Trust bootstrap remains open.

Traceability

Related requirements: `IP-AUTH-01`, `IP-AUTH-05`; identity creation and lifecycle requirements. Related questions: OPEN-03, OPEN-14.

IP-ADR-0006: Delegation, succession, and ownership transfer

Status: Accepted **Approval provenance:** Freshly approved Delegation, Succession, and Ownership Transfer passage, supplied November 7, 2026.

Decision

Delegation, succession, and ownership transfer MUST remain distinct operations.

Delegation grants explicitly bounded authority without transferring ownership.

A delegate MUST NOT exercise capabilities, target scopes, or permissions exceeding the authority validly delegated to that actor.

Succession MUST require an explicitly authorized arrangement and a protected activation process.

Succession MAY transfer specified control without transferring ownership.

Absence, inactivity, loss of contact, or presumed death MUST NOT independently activate succession or constitute consent to ownership transfer.

Ownership transfer MUST be explicitly initiated by the current owner and accepted by the intended recipient through the applicable protected authorization process.

An ownership transfer MUST NOT automatically transfer unrelated identities, credentials, application accounts, or other resources.

No administrator, application, delegate, or successor MAY acquire ownership solely through their existing role or authority.

The detailed mechanisms for succession activation, disputed claims, recovery interactions, and shared ownership or control remain unresolved under the applicable OPEN questions.

Rationale

Permission to act, succession to specified control and change of ownership have different effects and safeguards. They must not be inferred from one another.

Consequences

Delegation remains scoped; succession requires prior authorization and protected activation; ownership transfer requires owner initiation and recipient acceptance. Mechanisms for disputes, recovery interactions and shared control remain unresolved.

Traceability

Related requirements: `IP-AUTH-04`, `IP-AUTH-07`–`IP-AUTH-08`; lifecycle requirements. Related questions: OPEN-11, OPEN-13.

IP-ADR-0007: Recovery Root Token and protected recovery

Status: Accepted **Approval provenance:** Recovery Root Token passage in the approved-language integration brief, supplied November 7, 2026.

Decision

An Identity Passport MAY provide an optional Recovery Root Token as a separately provisioned recovery credential associated with its existing Root Identity.

A Recovery Root Token MUST NOT constitute a second Root Identity or establish an independently active Passport authority.

A Recovery Root Token MAY provide authority equivalent to that of its associated Root Identity **solely for an explicitly authorized recovery operation**. Such authority MUST NOT be interpreted as unrestricted identity-management authority.

A Recovery Root Token MUST NOT authorize the creation of new Root Identities or Subordinate Identities.

An authorized recovery operation MAY select zero, some, or all existing Subordinate Identities for recovery into a replacement Passport governed by a new Root Identity.

When existing Subordinate Identities are recovered, their identity continuity MUST be preserved. They MUST NOT be treated as newly created identities merely because their authoritative Passport relationship changes.

A successful recovery transition MUST permanently invalidate the superseded Root authority and the consumed Recovery Root Token.

A recovered Subordinate Identity MUST NOT remain simultaneously active under conflicting Passport or Root authorities.

Possession of a Recovery Root Token MUST NOT bypass applicable authentication, authorization, lifecycle, security, or recovery-specific safeguards.

Recovery MUST NOT automatically transfer unrelated identities, credentials, application accounts, ownership rights, or other resources.

Implementations MUST NOT treat possession of a Recovery Root Token as authorization to perform ordinary identity creation, unrestricted delegation, or consumer-application operations.

Implementation details remaining unresolved

The following matters remain open and MUST NOT be treated as approved mechanisms:

- Token generation, representation, storage, and cryptographic format.
- Recovery initiation and protection against competing or fraudulent claims.
- Selection and transfer protocols for recovered Subordinate Identities.
- Recovery involving zero selected Subordinates, including token-consumption semantics.
- Recovery coordination, atomicity, and handling of interrupted transitions.
- Disputed recovery and compromised-credential procedures.

These questions remain within OPEN-11 and other applicable unresolved-question records.

Approved interpretive note: The replacement Passport and new Root are established through an authorized recovery workflow. A token is not an unrestricted Root-creation capability. Keep this consistent with IP-AUTH-04 and IP-AUTH-05.

Explanation

A Recovery Root Token is a protected continuity mechanism, not another identity. Its purpose is to allow authorized recovery when ordinary Root authority becomes unavailable or compromised, without creating additional authority that could be used for unrelated operations.

Rationale

The token provides a narrowly bounded recovery path while preserving identity continuity and preventing duplicate active control or general identity-management authority.

Consequences

The token is optional and separately provisioned. It cannot create identities. Recovery transfers selected existing Subordinates to a replacement Passport and invalidates superseded recovery authority. Token and recovery protocols remain open.

Traceability

Related requirements: IP-AUTH-04–08; recovery and lifecycle requirements. Related questions: OPEN-11, OPEN-12, OPEN-13.

IP-ADR-0008: Orphaned objects and restricted `Inactive` state

Status: Accepted **Approval provenance:** Orphaned Object Inactivity decision and `Inactive` definition approved in Phase 2A / final Phase 2B briefs, supplied November 7, 2026.

Decision

`Inactive` is a restricted lifecycle state in which an Identity Passport object is retained with its identity and continuity intact but is not eligible for ordinary operations that require the object to be active.

Being `Inactive` MUST NOT by itself mean deletion, abandonment, forfeiture, reassignment, disclosure, succession, or transfer of ownership or control. Entry into or presence in `Inactive` MUST NOT create authority for any person, application, or organization.

Reactivation or other state-changing operations MUST satisfy applicable current authorization, security, and lifecycle conditions.

An object determined to be orphaned MUST enter `Inactive` with a recorded orphan reason or condition.

The criteria for orphan detection, state propagation, retention, restoration mechanisms, and disposition remain subject to OPEN-12; no default deletion or ownership transfer is implied.

Explanation

`Inactive` retains identity and continuity while restricting ordinary active operations. It does not determine ownership or grant another party authority.

Rationale

Orphaning or lack of contact must not itself erase, reassign or expose identity, or transfer authority. A restricted existing lifecycle state provides a fail-safe holding condition pending explicitly authorized action.

Consequences

The specification must define the state and its restrictions without creating a second top-level state. Orphan detection and disposition mechanisms remain unresolved.

Traceability

Related requirements: IP-AUTH-08 and lifecycle requirements. Related questions: OPEN-11, OPEN-12, OPEN-13.

IP-ADR-0009: Complete-path authorization, Revision 1

Status: Accepted **Approval provenance:** IP-AUTH-01 through IP-AUTH-08 Revision 1, freshly approved language supplied November 7, 2026. **Editorial authorization:** Bulk Editorial Revision Authorization, November 12, 2026.

Decision

The specification's IP-AUTH-01 through IP-AUTH-08 requirements are approved as follows. Their normative clauses belong in the authored specification chapter; this ADR records their approval and rationale.

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-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-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-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-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 were satisfied under the conditions validated. 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-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-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-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.

Rationale

The requirements define complete, scoped and current authorization; distinguish authority from authentication, lifecycle and safeguards; and explicitly support protected Root management without making Root authentication a prerequisite for every ordinary consumer action.

Consequences

IP-AUTH-01–08 Revision 1 supersedes prior wording for those requirement clauses only. Other accepted requirements remain in force. Concrete storage, transaction, protocol and credential mechanisms remain implementation choices unless separately specified.

Traceability

Related specification requirements: IP-AUTH-01–08; IP-ID-04, IP-ID-06; IP-SEC-01–05. Related questions: OPEN-11–14.

IP-ADR-0010: Decision and question governance

Status: Accepted **Approval provenance:** Phase 2A-08, approved governance amendment supplied November 7, 2026.

Decision

The Phase 2A reconciliation establishes the approved identity, ownership, authorization, recovery, application-independence, and lifecycle guarantees.

Implementation mechanisms not expressly approved remain unresolved and MUST NOT be represented as accepted architectural decisions.

OPEN-01 through OPEN-10 MUST be preserved unless separately resolved or closed through the established governance process.

Questions in the canonical question register MUST retain their numeric identifiers throughout their lifecycle.

An unresolved question MUST use the designation `OPEN-nn`.

When a question is closed, its designation MUST change to `CLOSED-nn`, retaining the same numeric identifier and displaying the reference **“Formerly OPEN-nn”**.

A closure MUST record its disposition and reference the applicable resolution, accepted decision, or governance action.

Closed questions MAY be reopened through the established governance process.

The question register is responsible for tracking questions and their current disposition. Detailed change history, deliberation, and approval records MAY be maintained separately through the project’s governance mechanisms.

Question identifiers MUST NOT be recycled.

OPEN-11 through OPEN-14 MUST be incorporated into the canonical unresolved-question register, retaining their approved subject matter and distinguishing established requirements from unanswered design questions.

In particular, the following implementation details remain unresolved:

- Root trust bootstrap and evaluation of RFC 5280 or alternative mechanisms.
- Recovery authorization representation and competing-claim resolution.
- Recovery of zero Subordinate Identities and associated credential-consumption semantics.

- Orphan detection, lifecycle propagation, retention, and disposition.
- Shared ownership and control arrangements.
- Mechanisms for authoritative transfer and prevention of conflicting simultaneous control.
- Representation of explicitly authorized cross-Passport relationships.

Future implementations MAY adopt different mechanisms consistent with the approved requirements.

No implementation mechanism MAY weaken established identity ownership, application independence, authorization boundaries, recovery protections, or lifecycle safeguards.

No existing accepted architectural decision is superseded solely by this reconciliation.

Any subsequently identified conflict with an accepted decision MUST be recorded and reviewed before that decision is modified.

Rationale

Permanent question identifiers and explicit closure provenance make the status of unresolved design work auditable without turning question governance into a Passport runtime requirement.

Consequences

OPEN/CLOSED status and decision history are editorial governance. They do not define Core conformance. Existing questions remain open unless closed through the stated process.

Traceability

Related material: canonical question register, traceability register, and publication history. Related questions: OPEN-01–OPEN-14.

IP-ADR-0011: Identity Passport secure transport properties

Status: Accepted **Approval provenance:** Identity Passport Secure Transport Requirements passage in the approved-language integration brief, supplied November 7, 2026. **Editorial authorization:** Bulk Editorial Revision Authorization, November 12, 2026.

Decision

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.

Implementation details remaining unresolved

Approved protocol selection, protocol-specific profiles, trust bootstrap mechanisms, endpoint identity binding, and interoperability requirements remain subjects for further specification.

Veilid and Secure Scuttlebutt are examples of technologies that may be evaluated. Their mention does not establish approval or mandatory use.

Applicable protocol-selection questions remain unresolved under OPEN-01. Application-trust bootstrap questions remain under OPEN-14.

Explanation

Identity Passport is transport-agnostic, but it is not transport-security-optional. A participating system must protect Passport communications regardless of which approved transport technology carries them.

Rationale

Transport agnosticism should preserve protocol choice while requiring core protections for Passport data in transit.

Consequences

Confidentiality, integrity, endpoint authentication and replay protection are required properties. Protocol selection and profiles remain open.

Traceability

Related specification requirement: `IP-SEC-06`. Related questions: OPEN-01, OPEN-14.

IP-ADR-0012: Passport verification and trust boundaries

Status: Accepted **Approval provenance:** Passport Verification and Trust Boundaries passage in the approved-language integration brief, supplied November 7, 2026. **Editorial authorization:** Bulk Editorial Revision Authorization, November 12, 2026.

Decision

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.

Implementation details remaining unresolved

The following remain open to further design:

- Approved external authentication evidence formats and verification interfaces.
- The detailed trust-bootstrap mechanism for participating applications.
- Supported authentication assurance levels and their evaluation.
- Evidence freshness, binding, revocation, and replay-handling mechanisms.
- Interoperability profiles for independent Passport implementations.

No particular identity provider, authentication protocol, certification authority, or cryptographic credential format is mandated by this decision.

Explanation

An application can establish how a user authenticated and present suitable evidence to Identity Passport. Passport evaluates whether that evidence is acceptable, whether the application is appropriately trusted, and whether the requested operation is authorized. These are distinct questions. An application may help establish identity without issuing, owning, or controlling the user's Passport.

Passport determines whether evidence is acceptable for the requested operation; it does not have to manufacture every form of evidence itself.

Rationale

An application-independent Passport can accept suitable evidence from different authentication mechanisms while preserving its own decision boundary for trust, ownership and authorization.

Consequences

The standard does not require one authentication method or require Passport to implement all methods. Trust and evidence acceptance do not grant operation authority. Trust-bootstrap and interoperability mechanisms remain open.

Traceability

Related specification requirements: `IP-SEC-07`, `IP-AUTH-01`, and `IP-AUTH-05`. Related questions: OPEN-03, OPEN-14.

IP-ADR-0013: Identity Passport Posture Assessment and Validation

Status: Accepted **Amendment:** Approved November 12, 2026. **Original approval provenance:** Identity Passport Posture Assessment passage in the approved-language integration brief, supplied November 7, 2026. **Amendment approval provenance:** Owner-approved Stage 2 Integration Authorization, November 12, 2026.

Decision

Posture Assessment records an application's declarations about its behavior and practices. Declarations MUST be distinguished from facts independently established by evidence.

Posture Validation evaluates the assessed claims and applicable evidence against explicitly defined, approved Identity Passport requirements and applicable profiles, producing an attributable **PASS** or **FAIL** for a stated scope and the conditions evaluated. Assessment and Validation MAY occur within one operational process but MUST remain conceptually distinct.

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. 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.

Profiles MAY address particular domains, including Security and Privacy. Future profile types MAY be defined through the applicable specification and governance process. A Posture Assessment and Posture Validation MUST cover only approved properties and checks within the stated scope.

A successful Validation MUST indicate that the applicable checks passed under the conditions and evidence evaluated. It MUST NOT be represented as:

- A universal security certification.
- Proof that an implementation is free from vulnerabilities.
- A guarantee of production readiness.
- A permanent guarantee of continuing compliance.
- An independent grant of identity ownership, Passport authority, or permission to perform protected operations.

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.

Self-Validation and Independent Validation

Self-Validation is an application's own evaluation of its implementation. It supports finding deficiencies, remediation, and ongoing compliance work. Self-Validation MUST NOT be represented as Independent Validation.

Independent Validation is compliance evidence established independently of the evaluated application and supports the Identity Passport Zero Trust model. Self-Validation alone MUST NOT satisfy an applicable Independent Validation requirement. A passing Independent Validation establishes compliance only within the approved requirements, evidence, scope, and conditions evaluated. Whether a profile requires Independent Validation, validator qualifications, and the validation mechanism remain governed by the specification and unresolved questions.

Neither Self-Validation nor Independent Validation independently grants Management authority, Root issuance authority, identity ownership, explicit user consent, or operation-specific authorization.

Results and Disclosure

Public disclosure of detailed Posture Validation findings and evidence remains 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 the applicable specification profile. This limited duty does not require publication of detailed findings or sensitive evidence.

An implementation MAY disclose a simple result without publishing detailed findings. Where permitted by 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 findings MAY be made available to appropriately authorized viewers for testing, debugging, demonstration, governance, or interoperability evaluation where policy permits.

Disclosures MUST respect privacy, security, and information-disclosure requirements. A system MUST NOT require public disclosure of sensitive assessment evidence merely to demonstrate that validation was performed.

Evidence

Validation results MAY form part of evidence considered during implementation evaluation, interoperability review, or application-trust decisions. They MUST NOT independently replace applicable application trust, authentication, Management permission, user consent, or complete-path authorization for a protected operation.

An implementation's own Self-Validation claims MUST NOT be presented as independently established evidence. The Public Validation Ledger's independent verification of record provenance and integrity MUST NOT by itself be represented as Independent Validation of the implementation.

Terminology compatibility

Earlier accepted text, including IP-ADR-0009, used "successful Posture Assessment" to refer to a passed evaluation. For purposes of the specification terminology approved by this amendment, that result is a successful Posture Validation. The established boundary is unchanged: a passing result does not independently grant identity authority or authorization. The earlier record's approval provenance remains intact.

Rationale

The Core floor is mandatory, profiles may add but not weaken requirements, and validation claims are limited to their stated scope and evidence. Separating an application's claims from their evaluation makes the evidence basis clear while preserving the distinction between eligibility and authority.

Consequences and unresolved mechanisms

Core compliance cannot be selectively waived or offset by optional checks. Management-capable applications have a narrow approved public-disclosure duty; sensitive findings remain protected. Profiles and governance must define applicability, evidence, Independent Validation requirements and assurance. The following mechanisms remain unresolved: approved profile versioning; check identifiers, applicability, and evaluation methods; result formats and evidence requirements; validation freshness and reassessment procedures; and authorized disclosure and verification interfaces. Validator qualifications, validation mechanisms, and intervals also remain unresolved.

Traceability

Related requirements: `IP-AUTH-05`, `IP-CONF-04`–`IP-CONF-10`; related requirements in `IP-SCP-04`. Related questions: OPEN-08, OPEN-15, OPEN-17. The original November 7, 2026 approval provenance and November 12, 2026 Stage 2 amendment provenance are retained. The November 12, 2026 owner-approved preservation correction restores five provisions accepted in the historical decision; it is not a new architectural policy and does not replace or erase either approval record.

IP-ADR-0014: Initial Trust and Independent Acceptance

Status: Accepted **Approval provenance:** Owner-approved Stage 2 Integration Authorization, November 12, 2026.

Decision

Identity Passport MUST permit appropriately authorized individuals, organizations, or communities to accept initial trust relationships within their respective scopes of authority.

Identity Passport MUST NOT require one universal central authority or universally recognized trust anchor as the exclusive source of trust.

Each participant MUST be able to accept, withhold, and withdraw its own trust in an authority, subject to legitimate authorization and governance boundaries. A participant's recognition of an authority MUST NOT obligate any other participant to recognize it. One participant's distrust or withdrawal MUST NOT, solely by that act, invalidate another participant's independent trust decision, revoke identities owned by others, transfer their ownership, or extinguish their identities.

Recognition of an authority MUST NOT independently confer identity ownership, Root Identity issuance authority, Passport Management permission, or permission for any protected operation. Those operations remain subject to their separately applicable ownership, trust, permission, consent, and complete-path authorization requirements.

Rationale

Technical verification can establish whether claims follow from an accepted basis; it cannot select a participant's initial trust anchor. Trust decisions are scoped and independently made, while authority to issue or manage identities remains governed separately.

Consequences and unresolved mechanisms

This decision selects no certificate format, X.509/RFC 5280 profile, PGP/Web of Trust model, hierarchy, bootstrap-recording mechanism, revocation protocol, or federation design. How trust relationships are represented, distributed, withdrawn, and applied to dependent assertions, attestations, and authorizations remains open under OPEN-14. OPEN-02 continues to cover assertion, issuer, and key-profile details.

Traceability

Related requirements: `IP-AUTH-09`, `IP-LC-06`, `IP-SEC-06`–`IP-SEC-07`. Related questions: OPEN-02, OPEN-14.

IP-ADR-0015: Continuous Validation and Public Standing

Status: Accepted **Approval provenance:** Owner-approved Stage 2 Integration Authorization, November 12, 2026.

Decision

An application that elects to participate in an approved Identity Passport profile MUST satisfy the initial Posture Validation required by that profile before it is eligible under the profile. This decision does not require Identity Passport participation by an application instance that uses only local authentication. Continuing eligibility and good standing require current validation as specified by the applicable profile.

Applicable profiles MUST require recurring Posture Validation and reassessment after material changes or significant incidents. Profiles MUST specify the applicable cadence, evidence validity, triggers, and standing consequences. Numerical intervals, incident thresholds, grace periods, and detailed state transitions are not selected by this decision.

Where an applicable profile requires Independent Validation, Self-Validation alone MUST NOT satisfy that requirement. The validation process and public records MUST accurately identify the scope, result, and evidence/assurance level under which the standing was established.

Management-capable applications MUST make current validation standing publicly accessible. An eligible application MUST display the exact designation **“In Good Standing Since [date]”**. The date MUST be the date of the most recent successful qualifying Posture Validation, even where good standing has been uninterrupted. Each subsequent successful qualifying validation updates the date. An application that is failed, suspended, expired, overdue, or otherwise ineligible MUST NOT display that positive designation as its current status.

Identity Passport MUST provide a publicly accessible historical record of applicable validation events and standing changes. Current standing MUST link to that history through an ordinary link. History MAY be hosted separately but MUST remain publicly accessible without requiring an Identity Passport account.

The Public Validation Ledger MUST permit independent verification of the provenance and integrity of standing and validation records. The evaluated application MUST NOT exclusively control publication, alteration, suppression, or deletion of its own history. A later PASS MUST NOT erase or conceal an earlier FAIL or suspension.

Public records MUST comply with privacy and non-disclosure requirements. They MUST NOT require publication of secret credentials, protected identity information, or sensitive assessment evidence. Hosting, witnessing, verifying, or publishing ledger records MUST NOT itself confer identity ownership, Root issuance authority, or Management permission.

The current standing view SHOULD remain concise. The public history MAY provide event details beyond the current standing view, subject to approved disclosure limits. Loss of application standing MUST NOT extinguish or transfer a user-owned identity or prevent its management by another appropriately authorized application. Independent verification of record provenance and integrity is distinct from Independent Validation of the evaluated application. The architecture MUST NOT require a particular ledger technology or unnecessarily complex infrastructure.

Rationale

Continuing application eligibility depends on current, scoped compliance evidence. A simple public standing view and independently verifiable history let users inspect that status without giving the evaluated application exclusive control over its record. Public record verification and independent validation of implementation behavior are separate assurances.

Consequences and unresolved mechanisms

No numerical validation interval, evidence-expiry duration, validator qualification, third-party audit obligation, ledger protocol, cryptographic scheme, witness topology, retention duration, correction procedure, availability guarantee, or negative-status vocabulary is selected. Applicable profiles and governance must resolve the details without weakening privacy, independent verification, or the history-preservation requirement.

Illustrative interface only

The following records are fictitious examples, not validation claims:

Application	Current standing	History
Example Application A	In Good Standing Since November 12, 2026	View History
Example Application B	Validation Failed — November 12, 2026	View History
Example Application C	Validation Overdue	View History

Every example validation row below is illustrative only:

Date	Validation	Result
November 12, 2026	Routine	PASS
October 13, 2026	Routine	PASS
September 14, 2026	Revalidation	PASS
September 13, 2026	Routine	FAIL

The displayed “Since” date is the most recent successful qualifying validation, not the beginning of an uninterrupted period. “View History” is ordinary navigation, not consent to publication; the approved record remains public whether or not a reader follows the link.

Traceability

Related requirements: `IP-CONF-07`–`IP-CONF-10`. Related questions: OPEN-08, OPEN-15, OPEN-16.