Passport Alliance

Governing Charter | Version 1.0

An Open, Multi-Stakeholder Governing Body for Agent Identity Standards

Founded by: Cory M. Gibson | AetherPro Technologies LLC

Root Key Ceremony: 2026-02-21 | Charter Effective: May 2026

Preamble

The proliferation of autonomous AI agents operating across organizational boundaries, jurisdictions, and agentic frameworks has created a legal and technical vacuum: no universal standard exists for agent identity, accountability, or authority delegation.

The Passport Alliance exists to fill that vacuum with an open, cryptographically grounded, legally defensible standard — one that any framework, any organization, and any operator can implement without proprietary dependency or centralized control.

The Alliance does not exist to serve AetherPro Technologies LLC exclusively. It exists because the problem is real, the solution is needed, and no one had formalized it. AetherPro is the founding organization and custodian of the root key — but the Alliance is governed collectively, its standards are freely implementable, and its membership is open to any organization meeting the admission criteria defined herein.

This is how all foundational internet protocols were built. SMTP, DNS, TLS, and OAuth all began with small groups of engineers who identified a problem and wrote the spec. The Passport Alliance follows that tradition.

Article I — Name, Purpose, and Structure

1.1 Name

This organization shall be known as the Passport Alliance (the "Alliance").

1.2 Mission

The Alliance exists to:

- Publish and maintain the APIS (Agent Passport Issuance Standard) specification as a free, open standard
- Operate the root trust anchor for the APIS credential chain
- Admit and audit Realm Issuers who wish to issue APIS-compliant Agent Passports
- Operate the shared public infrastructure: agents.passportalliance.org namespace, alliance-root.jwk publication, and APIS Direct Registration for domain-less principals
- Advance the legal and technical recognition of Agent Passports as a valid form of non-human identity

1.3 Governance Model

The Alliance is governed as an open, multi-stakeholder body. Governance mirrors the structure of established internet standards bodies:

Alliance Role	Analogy	Responsibility
Alliance Steering Committee	IANA / ICANN Board	Sets policy, holds root key, admits Realm Issuers
Realm Issuers	Intermediate Certificate Authorities	Issue Agent Passports within their registered realm
Principal Operators	Domain Registrants	Register machines and agents, hold custodial authority
Contributing Members	IETF Working Group Participants	Propose spec amendments, implement tooling, review standards

Article II — The Root Key

2.1 Root Key Record

The Passport Alliance Root Key was generated on 2026-02-21 by Cory M. Gibson, founder and CEO of AetherPro Technologies LLC, in an air-gapped environment with no network connectivity. The ceremony was conducted on an offline machine with the storage medium physically disconnected from all networked infrastructure.

The root key ceremony is the functional and legal equivalent of a WebTrust-audited Certificate Authority root key ceremony. It establishes the cryptographic anchor from which all APIS trust is derived.

Root Key Parameter	Value
Ceremony Date	2026-02-21
Ceremony Conductor	Cory M. Gibson, AetherPro Technologies LLC
Key Algorithm	ECDSA P-384 (FIPS 186-4 compliant)
Key Storage	Air-gapped hardware security module
Public Key Publication	https://aetherpro.us/.well-known/alliance-root.jwk
Zenodo DOI	https://doi.org/10.5281/zenodo.18820877
Key Usage	Signs Realm Issuer certificates only — never signs Agent Passports directly
Renewal Policy	Root key ceremony repeated every 5 years or upon compromise suspicion

2.2 Root Key Custodianship

The root key is held exclusively by the Alliance Steering Committee. The founding custodian is AetherPro Technologies LLC. As the Alliance matures and additional Steering Committee members are admitted, root key custodianship shall be distributed across a minimum of three geographically separate keyholders using Shamir's Secret Sharing (minimum 2-of-3 threshold).

2.3 Root Key Compromise Protocol

In the event of confirmed or suspected root key compromise:

1. All Realm Issuer certificates are immediately revoked
2. A public notice is published within 24 hours at passportalliance.org
3. A new root key ceremony is convened within 72 hours
4. All Realm Issuers must re-certify against the new root

5. All Agent Passports issued under the prior root are revoked and must be re-issued

Article III — Realm Issuers

3.1 Definition

A Realm Issuer is an organization that has met Alliance admission standards and is authorized to issue APIS-compliant Agent Passports within one or more registered realms (domains). Realm Issuers operate as intermediate certificate authorities in the APIS trust chain.

3.2 Admission Requirements

Any organization may apply for Realm Issuer status by satisfying the following requirements:

Requirement	Description
Legal Entity	Applicant must be a registered legal entity (LLC, Corp, Partnership, or equivalent) in any jurisdiction.
Domain Control	Applicant must demonstrate control of the realm domain(s) they intend to operate via DNS challenge.
Technical Compliance	Applicant must operate an APIS-APP compliant issuance endpoint, revocation endpoint, and public JWKS endpoint.
FIPS Cryptography	All issued certificates must use FIPS 186-4 compliant key generation (ECDSA P-256 minimum, RSA-2048 minimum).
Audit Logging	Applicant must maintain tamper-evident audit logs of all Passport issuance and revocation events for a minimum of 3 years.
Revocation SLA	Applicant must commit to processing revocation requests within 4 hours of receipt.
APIS Agreement	Applicant must sign the Realm Issuer Agreement accepting the APIS standard terms and the Alliance governance authority.

3.3 Admission Process

6. Applicant submits Realm Issuer Application via passportalliance.org/apply
7. Alliance Steering Committee reviews application within 30 days
8. Technical compliance audit conducted by Alliance or designated auditor
9. Upon approval, Alliance issues a Realm Issuer Certificate signed by the Alliance Root Key
10. Realm Issuer Certificate is valid for 2 years, renewable upon re-audit

3.4 Realm Issuer Obligations

- Publish JWKS at [realm-domain]/.well-known/apis-jwks.json

- Maintain public revocation endpoint at [realm-domain]/.well-known/apis-revocation
- Report any suspected compromise to the Alliance Steering Committee within 4 hours
- Comply with all APIS specification amendments within 90 days of ratification
- Accept and process Alliance-directed emergency revocation orders immediately

Article IV — Open Standard Commitment

4.1 Free and Open Implementation

The APIS specification is a free, open standard. Any individual, organization, or framework may implement APIS without license, royalty, or permission from the Alliance. Attribution is appreciated but not required for implementation.

4.2 Patent Non-Assertion

AetherPro Technologies LLC and all Alliance Steering Committee members commit to a patent non-assertion pledge covering all claims reading on the APIS specification. No member of the Alliance will assert patents against any party implementing the APIS standard in good faith.

4.3 Trademark

The terms "Passport Alliance," "Agent Passport," and "APIS" as used in this governance context are trademarks of AetherPro Technologies LLC. Use of these marks in implementations that comply with the APIS specification is permitted without prior authorization. Misleading use of these marks to imply Alliance endorsement of non-compliant implementations is prohibited.

Article V — Spec Amendment Process

5.1 Proposal

Any Contributing Member or Realm Issuer may propose a specification amendment by submitting a written proposal to the Alliance Steering Committee. Proposals must include a problem statement, proposed solution, impact assessment for existing implementations, and a 90-day migration path.

5.2 Review and Ratification

Proposals are published publicly for a 30-day comment period. The Steering Committee votes on ratification. A two-thirds supermajority is required for amendments that affect the core credential structure (Sections 3-8 of the APIS specification). Simple majority is sufficient for clarifications and additions.

5.3 Backward Compatibility

All ratified amendments must maintain backward compatibility with Passports issued under prior specification versions for a minimum of 18 months following ratification.

Article VI — Public Infrastructure

The Alliance operates the following public infrastructure, funded by Realm Issuer fees and voluntary contributions:

Service	URL	Purpose
Root Key Publication	aetherpro.us/.well-known/alliance-root.jwk	Public JWKS for root key — verifiable by anyone without an Alliance account
Alliance Registry	passportalliance.org/registry	Public directory of active Realm Issuers and their JWKS endpoints
Shared Namespace	agents.passportalliance.org	Free subdomain delegation for domain-less principals
Direct Registration	passportalliance.org/register	APIS Direct Registration for entities without any domain
Spec Publication	passportalliance.org/spec	Canonical published APIS specification — all versions
Status Page	status.passportalliance.org	Real-time operational status of Alliance infrastructure

Founding Attestation

This Charter is established by the founding organization of the Passport Alliance:

Founding Organization: AetherPro Technologies LLC
Founder and CEO: Cory M. Gibson
CAGE Code: 174V7 | SAM.gov Registered
Charter Date: May 2026

Root Key Ceremony Conducted: 2026-02-21
Zenodo DOI: https://doi.org/10.5281/zenodo.18820877