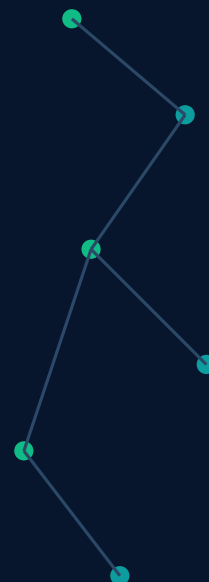


ECZ-ID Agent Passport Overview and Customer Guide

Persistent identity for AI and software agents across changing models, endpoints, runtimes, providers, versions and toolchains.



AGENT PASSPORT · OVERVIEW

PRIMARY READER

Buyer, technical evaluator, business owner, security architect, product or platform owner.

SECONDARY READER

Enterprise architect, procurement, operations, governance and developer stakeholders.

WHEN TO READ THIS

You are deciding whether Agent Passport is relevant to an agent estate and what value it adds.

RELEASE

2026.10 · 15 October 2026

WHAT YOU WILL KNOW AFTER READING

You can explain the Agent object, customer value, responsibility, state, bindings, evidence, authority boundaries and independent re-check.

WHAT THIS DOCUMENT DOES NOT ESTABLISH

A Passport does not by itself establish safety, certification, blanket authority or claims that are absent from the published record.

NEXT

Read the AWS Getting Started Guide when you are ready to acquire and activate the free Passport.

EXECUTIVE EXPLANATION

A durable identity anchor for software actors that keep changing

Agent Passport separates the identity of the agent from the changing infrastructure around it.

One identity across changing agent infrastructure

The surrounding implementation can change while the canonical Agent ECZ-ID remains referenceable.



WHY THIS MATTERS

An endpoint, API key or runtime role can identify where something is running now. Agent Passport is designed to keep a persistent ECZ-ID referenceable as those surfaces change.

What stays durable

The Agent ECZ-ID for the intended logical agent.

What can change

Bindings, published state, evidence, model, endpoint, provider and version context.

What is re-checked

Current Resolver proof when freshness or consequence requires it.

AGENT PASSPORT IN ONE VIEW

Identity in the centre; bounded, re-checkable context around it

The Passport can connect a persistent Agent ECZ-ID to responsibility, supported authority/delegation, state, bindings and evidence where present.

What an Agent Passport can represent

Persistent identity at the centre; bounded context around it; Resolver for independent re-check.



INTERPRETATION BOUNDARY

Identity is not blanket authority. Responsibility does not automatically mean every underlying assertion has been independently verified.

Resolver

Public, read-only proof that a human or machine can re-check.

Dashboard

Authenticated customer control plane for permitted estate actions.

CUSTOMER VALUE

Four high-value situations where persistent agent identity matters

The value is not “another agent ID.” It is a stable identity that can remain useful while technical context changes.

Production agents

Keep one referenceable identity while models, endpoints or versions change.

External counterparties

Let another party re-check the organisation claiming responsibility and the current published context.

Cross-platform agents

Maintain continuity across provider, runtime or toolchain change without treating the provider ID as the authority root.

High-consequence interactions

Evaluate identity, responsibility, bindings, evidence and supported authority separately before action.

CUSTOMER OUTCOME

Counterparties can refer to the same Agent ECZ-ID and inspect the current bounded record instead of treating a transient endpoint or self-assertion as the identity.

RESPONSIBILITY

Who claims responsibility for this agent?

Agent Passport can publish the relevant Parent or organisation relationship where supported; interpret the relationship together with the actual state and evidence present.

Parent / organisation

The organisation or Parent relationship provides responsibility context for the agent record where supported.

What this does not imply

A published relationship is not automatically proof that every declaration or external claim has been independently verified.



READER RULE

Read responsibility as a bounded relationship in the current record. Do not turn it into a universal assurance statement.

AUTHORITY AT THE DECISION BOUNDARY

Identity answers “who or what?”; authority answers “may this actor do this action?”

Agent Passport can carry supported authority or delegation context where present, but the decision remains action-specific and policy-driven.

Use identity as input to the decision - not as the decision itself

Resolve the Agent, evaluate the action-specific context you need, then apply local policy.

**BOUNDARY**

Agent Passport can support the decision; it does not automatically grant permission to spend, call APIs or invoke tools.

Identity can support

Who or what the agent is, the current published state and relevant relationships.

Identity cannot replace

Authentication, runtime controls, local policy or action-specific authority evaluation.

CRITICAL BOUNDARY

Agent Passport does not automatically permit spending, API calls, tool invocation or any other consequential action.

STATE, BINDINGS AND EVIDENCE

The context around identity is expected to change

Bindings connect the persistent ECZ-ID to changing external surfaces; evidence supports bounded claims; state is point-in-time and should be re-checked when freshness matters.

CURRENT STATE

Published point-in-time state for the Agent record. Re-resolve when the consequence requires current proof.

BINDINGS

A2A Agent Card or manifest, MCP-related surface, API/endpoint, repository/package reference or other supported machine surfaces.

EVIDENCE

References that support identity, relationship, state, binding or authority claims according to source, scope and freshness.

BINDING LAW

A provider-native identifier, endpoint or manifest is context associated with the Agent ECZ-ID. It does not replace ECZ-ID as the canonical identity root.

What can change safely

Endpoint, model, provider, version and supported evidence can change while the same logical Agent ECZ-ID remains referenceable.

When to challenge

If a required binding, evidence item or authority context is absent or stale for the decision you are making, treat it as not established and obtain fresh proof.

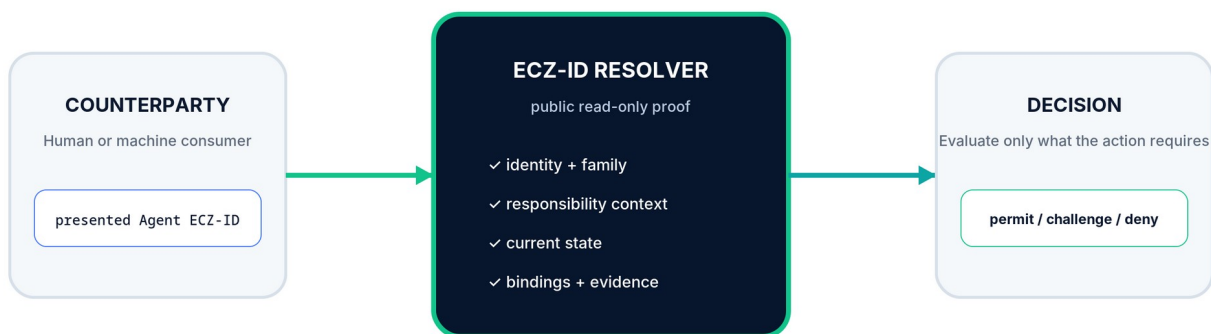
RESOLVER PROOF

Independent re-check before the interaction matters

Resolver is the public, read-only ECZ-ID proof surface. It is intentionally separate from the authenticated control plane.

Independent re-check when freshness matters

Human and machine consumers can resolve the same Agent ECZ-ID again before consequence.



GET https://api.ecocitizenz.com/api/p/{ecz_id}.json

Absent required data = not established. Re-resolve according to freshness policy.

MACHINE-READABLE ROUTE

GET https://api.ecocitizenz.com/api/p/{ecz_id}.json

- Confirm Passport family = Agent and the expected Agent ECZ-ID.
- Inspect the Parent / organisation relationship where it matters.
- Read current published state and the bindings/evidence relevant to the interaction.
- Evaluate supported authority/delegation only for the specific action when required.
- Re-resolve according to freshness policy before consequential use.

EXAMPLE INTERACTION

A security team evaluates an agent before connecting it to a consequential workflow

The verification sequence keeps persistent identity, current context and local policy separate.

1

Receive Agent ECZ-ID

The integration presents the agent's ECZ-ID.

2

Resolve

Open Resolver or use the machine-readable route.

3

Check expected context

Confirm the expected organisation relationship, state and relevant binding.

4

Evaluate evidence / authority

Inspect only what the intended action requires.

5

Apply local policy

Permit, challenge or deny using your own control logic.

RE-CHECK PRINCIPLE

The same Agent ECZ-ID can be resolved again when the consequence requires fresher state, evidence or authority context.

SAFE INTERPRETATION BOUNDARIES

What the Passport proves - and what it does not

The strongest customer use of ECZ-ID comes from respecting the scope of each field and refusing to infer claims that are absent.

SAFE CONCLUSIONS

- This is the ECZ-ID record presented for the agent.
- The record publishes the shown organisation relationship.
- The record currently publishes the shown state.
- The shown bindings and evidence can be inspected.
- Supported authority/delegation can be evaluated where present.

NOT ESTABLISHED BY PASSPORT ALONE

- The agent is safe.
- The agent will behave correctly.
- The agent can spend money.
- The agent can call arbitrary APIs or tools.
- Every declaration has been independently verified.
- Standards or certifications that are not explicitly evidenced.

FAIL-SAFE RULE

If the decision requires a field or evidence item that is absent, stale or outside scope, treat it as not established rather than inferring it from branding, provider context or self-assertion.

Security handling

Never place passwords, API keys, AWS Marketplace registration tokens, certificates or other secrets in Resolver records, public documentation or support tickets.

DEPLOYMENT FIT

Who should use Agent Passport and what "good" looks like

Agent Passport is most useful when the agent needs to remain identifiable across changing technical surfaces and other parties need to re-check its context.

AI platform teams

Give production agents a stable ECZ-ID and consistent proof surface across model/runtime/provider changes.

Security architects

Separate identity, responsibility, authority, state, bindings and evidence at the decision boundary.

Integration owners

Share one persistent identifier with counterparties and re-check current proof before consequence.

A GOOD DEPLOYMENT

Uses the Agent ECZ-ID as the durable reference; keeps external endpoints/provider IDs as bindings; reuses the canonical Parent/Passport; re-checks proof when freshness matters.

Free identity primitive

Agent Passport is one of the seven canonical free ECZ-ID Passport families.

No forced upsell

Paid ECZ-ID capabilities are not prerequisites for basic Agent Passport identity and verification.

QUICK REFERENCE

The Agent Passport decision card

Use this page as the one-minute summary for an evaluation or architecture review.

OBJECT

AI / software agent

PERSISTENT IDENTITY

Agent ECZ-ID remains the referenceable identity for the intended logical agent.

RESPONSIBILITY

Organisation / Parent context where supported; interpret it according to the published record.

MUTABLE CONTEXT

State, bindings, evidence and action-specific authority/delegation may change.

RE-CHECK

Use Resolver again when freshness or consequence requires current proof.

NEXT ACTION

Ready to acquire it? Read ECZ-ID Agent Passport - AWS Marketplace Getting Started and Technical Guide.

Support: support@ecocitizenz.com