

ECZ-ID MCP Passport Overview and Customer Guide

Persistent, resolver-verifiable identity for MCP servers and tool surfaces across changing endpoints, tools, versions and providers.

MCP PASSPORT · OVERVIEW

PRIMARY READER

Buyer, technical evaluator, security architect, AI platform owner and MCP operator.

SECONDARY READER

Developers, enterprise architects, procurement, governance and operations.

WHEN TO READ THIS

You are deciding whether an MCP server or tool surface needs a durable identity and independently re-checkable context.

RELEASE

2026.10 · 15 October 2026

WHAT YOU WILL KNOW AFTER READING

You can explain the MCP object, operator responsibility, endpoint/tool bindings, current state, evidence, change context and verification boundary.

WHAT THIS DOCUMENT DOES NOT ESTABLISH

An MCP Passport does not certify tools as safe, grant tool permission or prove every capability claim has been independently verified.

NEXT

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

EXECUTIVE EXPLANATION

A durable identity anchor for MCP surfaces that keep changing

MCP Passport separates the identity of the server/tool surface from its current endpoint, manifest, runtime and provider context.

One MCP identity across changing endpoints, tools and deployments

The server or tool surface can evolve while the canonical MCP ECZ-ID remains independently referenceable.



Persistent identity anchors a changing MCP surface

Endpoints, tool manifests, versions and provider context can change without treating the URL itself as the identity.

WHY THIS MATTERS

A URL or tool manifest describes where or what an MCP surface is now. MCP Passport is designed to keep a persistent ECZ-ID referenceable as that surface changes.

What stays durable

The MCP ECZ-ID for the intended logical server/tool surface.

What can change

Endpoint, tool set, manifest, runtime, provider, version and evidence context.

What gets re-checked

Current Resolver proof before connection or consequence.

MCP PASSPORT IN ONE VIEW

Identity at the centre; operator, surface and evidence around it

The Passport can connect a persistent MCP ECZ-ID to responsibility, endpoint/tool surface, current state, bindings and evidence where present.

What an MCP Passport can represent

Persistent MCP identity at the centre; operator, surface, state and evidence around it; Resolver for independent re-check



INTERPRETATION BOUNDARY

Identity is not tool permission. A listed capability is not automatically a behavioural guarantee. Evidence must be read according to source, scope and freshness.

Resolver

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

Dashboard

Authenticated customer control for permitted lifecycle actions.

THE CUSTOMER PROBLEM

MCP discovery is easy; durable accountability is harder

An MCP client can discover an endpoint and tools, but discovery alone does not answer who is responsible, whether the surface changed, or whether the proof is still current.

Without a persistent identity

A changing URL, runtime, proxy or manifest can make it difficult to tell whether today's surface is the same intended MCP object.

Self-description is useful, but it is still self-description.

With MCP Passport

The MCP surface can present a stable ECZ-ID, operator context and bounded proof that counterparties can resolve again before they connect or invoke.

CORE QUESTION

Which MCP server/tool surface am I connecting to, who is responsible for it, what changed, and can my agent independently re-check the current proof?

- Persistent identity complements - rather than replaces - authentication, TLS, credentials and runtime policy.
- Provider-native or endpoint identifiers remain bindings/context; they do not replace ECZ-ID as the canonical identity root.
- Where change history, warnings or other evidence are available, treat them as bounded evidence - not a universal trust score.

RESPONSIBILITY AND OPERATOR CONTEXT

Who claims responsibility for this MCP surface?

A Passport can publish a Parent/organisation relationship or operator context where supported. That relationship is meaningful, but it must not be over-interpreted.

Responsibility can establish

The record publishes which organisation/Parent is associated with the MCP object, plus supported relationships and evidence.

Responsibility does not establish

That every tool is safe, that every capability claim is verified, or that the organisation grants every caller permission to invoke tools.

OPERATOR

Who runs or is responsible for the MCP surface?

OBJECT

Which logical MCP server/tool surface does the ECZ-ID represent?

COUNTERPARTY

Who is resolving the proof and for what interaction?

RULE

Read the relationship that is actually published. Do not infer ownership, safety, certification or invocation authority that is absent.

ENDPOINT AND TOOL-SURFACE BINDINGS

Identity persists while the connection surface changes

MCP Passport can associate the canonical ECZ-ID with supported external surfaces such as endpoints, manifests, repositories, provider IDs and tool metadata.

ENDPOINT

Current supported network/location reference where published.

MANIFEST / TOOLS

Tool or capability surface references where supported.

REPO / PROVIDER

Repository, package or provider-native references where supported.

BINDING LAW

A binding says the ECZ-ID record is associated with an external surface according to the available evidence and state. The endpoint itself is not the ECZ-ID authority root.

- When an endpoint moves, update the binding rather than minting a second identity for the same logical MCP surface.
- When tools change, re-check the published context before consequential use.
- If evidence or binding data is absent, treat it as absent - do not infer it from marketing or self-assertion.

CHANGE CONTEXT AND FRESHNESS

Tool surfaces evolve; proof must be re-checkable

MCP estates can change quickly: tool lists, manifests, versions, endpoints and operator context may move on different timescales.

CURRENT STATE

Read the current published state as a point-in-time signal from the canonical ECZ-ID system. Re-resolve when the action requires fresh proof.

CHANGE / EPOCH CONTEXT

Where supported evidence captures change history or a trust epoch, use it to understand what changed since a prior observation - not as a guarantee of safety.

FRESHNESS RULE

Do not cache a trust conclusion indefinitely. Cache only according to the use case and re-check the Resolver when the consequence requires current proof.

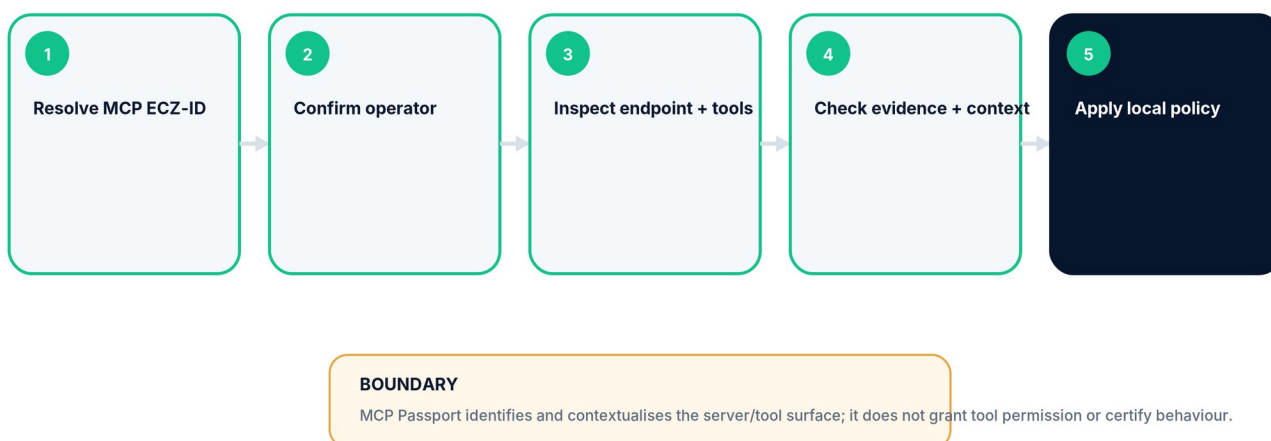
AGENT ↔ MCP RECIPROCAL TRUST

The connection is a relationship, not a one-sided assertion

An agent can present its own identity while independently resolving the MCP surface it intends to use. The MCP surface can likewise be associated with its responsible organisation and current proof context.

Re-check the MCP surface before connection or consequence

Use MCP Passport proof as input to local policy - not as a universal safe/unsafe verdict.

**DECISION BOUNDARY**

Use MCP Passport proof as input to local policy. Authentication, tool permissions, runtime controls and action-specific authority still apply.

SECURITY-RELEVANT EVIDENCE

Warnings can inform a decision without becoming a universal verdict

Security teams may care about secret exposure warnings, dangerous tool chains, manifest change and other signals where separately supported by evidence or connected tooling.

Appropriate interpretation

A warning or evidence reference can support a bounded conclusion about the specific source, scope, timestamp or observed condition.

Unsafe leap

Do not turn a warning into "unsafe forever", or the absence of a warning into "safe". MCP Passport itself is not a secret scanner or behavioural auditor.

FAIL-SAFE PRINCIPLE

If your policy requires a field, binding or evidence item and it is absent or stale, treat the requirement as not established and challenge/deny according to policy.

HIGH-VALUE USE CASES

Where MCP Passport adds the most practical value

The strongest use cases are those where identity continuity and independent re-check matter more than a one-time endpoint discovery.

AGENT BEFORE CONNECT

An agent receives an MCP ECZ-ID, resolves it, confirms the expected operator and endpoint/tool surface, then applies local policy.

ENDPOINT MIGRATION

The server moves to a new endpoint or provider while counterparties continue to resolve the same canonical MCP ECZ-ID.

TOOL-SURFACE CHANGE

A client re-checks the Passport after a manifest/tool change rather than treating a cached surface as current indefinitely.

ENTERPRISE REVIEW

Security or architecture teams inspect operator context, bindings, evidence and freshness before onboarding an MCP surface.

WHAT MCP PASSPORT DOES NOT PROVE

Boundaries are part of the product, not footnotes

A strong identity system is useful partly because it is explicit about the conclusions it does not support.

- It does not automatically prove the MCP server or tools are safe.
- It does not automatically prove future behaviour.
- It does not grant an agent or human permission to invoke tools.
- It does not replace authentication, authorization, credentials, runtime policy or sandboxing.
- It does not prove every tool/capability declaration has been independently verified.
- It does not imply code is vulnerability-free or secrets are absent unless supported evidence specifically establishes that condition.

SAFE INTERPRETATION

Use the identity, state, bindings and evidence that are actually present for the specific decision being made.

SHOULD YOU DEPLOY MCP PASSPORT?

A quick decision card

MCP Passport is most relevant where an MCP surface is expected to persist longer than any single endpoint, manifest, tool set or provider context.

STRONG FIT

- Multiple agents/clients connect
- Endpoints/tools can change
- Operator responsibility matters
- Security teams require re-checkable evidence
- Provider portability matters

DO NOT EXPECT

- Automatic tool permission
- Behavioural certification
- Replacement for IAM/auth
- Universal trust score
- Proof absent fields are true

CUSTOMER OUTCOME

A stable MCP ECZ-ID becomes the anchor that counterparties can use to re-check current responsibility, surface and evidence as the estate evolves.

NEXT STEPS

From evaluation to working proof

The free Passport is designed to move from discovery to verification without requiring a paid capability.

1 ACQUIRE

Use AWS Marketplace or the supported ECZ-ID acquisition path.

2 ACTIVATE

Reuse or create the supported account / Parent and issue or reuse the MCP Passport.

3 VERIFY

Open Resolver and re-check the public proof.

READ NEXT

ECZ-ID MCP Passport - AWS Marketplace Getting Started and Technical Guide

THEN

ECZ-ID MCP Passport Technical Reference for integration patterns and machine-safe interpretation.

SUPPORT

support@ecocitizenz.com