

ECZ-ID Service & Workload Passport Operations, Lifecycle and Troubleshooting Guide

Operate service/workload identity safely over time as owner/operator, provider, runtime, deployment, state and evidence context change.

SERVICE & WORKLOAD PASSPORT · OPERATIONS

PRIMARY READER

Platform administrator, cloud/platform operations, security operations, service owner and estate owner.

SECONDARY READER

Support engineers, developers, platform engineers, service/workload owners and governance teams.

WHEN TO READ THIS

The Service & Workload Passport exists and you need to operate, update, recover or troubleshoot it safely.

RELEASE

2026.10 · 16 October 2026

WHAT YOU WILL KNOW AFTER READING

You can preserve canonical identity, update provider/runtime/deployment context, re-check Resolver proof, avoid duplicates and escalate failures without leaking secrets.

WHAT THIS DOCUMENT DOES NOT ESTABLISH

Operational changes do not automatically imply a new service/workload identity; identity continuity must follow the actual service/workload/runtime object boundary.

NEXT Use the Technical Reference when you need machine consumer semantics or integration detail.

FIRST OPERATIONAL CHECK

Confirm the canonical service/workload before changing anything

Start every maintenance or troubleshooting action by identifying the intended Service & Workload ECZ-ID and its current organisation/Parent/owner/operator context.

1 · IDENTIFY

Confirm Service & Workload ECZ-ID and Passport family.

2 · INSPECT

Check Dashboard relationship, state, provider/runtime/deployment/service bindings and evidence.

3 · RESOLVE

Open the same ECZ-ID in Resolver and compare public proof.

4 · SCOPE THE CHANGE

Decide whether you are changing context or the service/workload object itself.

OPERATING LAW

Preserve the canonical identity when the intended service/workload object remains the same; update context rather than minting a duplicate.

DASHBOARD VERSUS RESOLVER

Control privately; prove publicly

Use Dashboard for authenticated permitted actions and Resolver for public independent re-check.

DASHBOARD

Authenticated customer control:
inspect/manage permitted organisation
relationship, bindings, evidence, state and
lifecycle actions.

RESOLVER

Public, read-only proof surface for
counterparties and automation.

DO NOT CONFUSE

Do not attempt to mutate public proof through Resolver; do not expose private customer/control data merely because Resolver is public.

AFTER A CHANGE

Use Resolver to confirm the intended public
result.

**BEFORE A HIGH-CONSEQUENCE SERVICE/WORKLOAD
DEPLOYMENT OR MIGRATION DECISION**

Re-resolve if freshness matters.

CHANGING PROVIDER, RUNTIME, DEPLOYMENT OR SERVICE BINDINGS

Update context without fragmenting identity

Provider/runtime changes are normal. Treat provider-native workload IDs, account/project/subscription references, clusters, namespaces, service accounts, containers and runtime/deployment/service bindings as mutable supported context.

TYPICAL CHANGES

- provider or cloud-account/project migration
- cluster / namespace / service-account change
- container or runtime identity change
- deployment / service binding change
- environment or documentation change

OPERATOR SEQUENCE

- confirm canonical Service & Workload ECZ-ID
- update supported binding/relationship
- refresh evidence/state if needed
- re-resolve and verify public result

DO NOT MINT BY DEFAULT

A new provider-native workload ID, account/project/subscription reference, cluster, namespace, service account, container, runtime or deployment reference is not by itself a reason to create a new Service & Workload Passport.

PRESERVE IDENTITY WHEN

The same intended service/workload/runtime object persists.

RECONSIDER IDENTITY WHEN

The service/workload object itself has genuinely changed.

RUNTIME, AUTHORITY AND EVIDENCE REVIEW

Keep bounded workload context current

Where supported, runtime/deployment context and evidence should be reviewed when provider, owner/operator or environment context changes or when the evidence itself becomes stale.

REVIEW TRIGGERS

- material deployment/runtime change
- provider/runtime migration
- owner/operator change
- cluster/namespace/service-account/container change
- evidence expiry or replacement

REVIEW QUESTIONS

- is this still the intended service/workload?
- do provider/runtime/deployment/environment bindings match the current estate?
- is evidence still in scope/fresh?
- did organisation/owner/operator responsibility or lifecycle state change?

DO NOT CLAIM SAFETY OR PERMISSION WITHOUT EVIDENCE

Provider/runtime/deployment context and evidence can be useful, but it does not establish safety, configuration correctness, runtime/image integrity, availability or permission to act unless supported evidence and local policy explicitly establish them.

REFRESH

Update supported evidence/state through the canonical control path.

VERIFY

Resolve again and inspect what counterparties can now observe.

OWNER, OPERATOR AND RESPONSIBILITY CHANGES

Change relationships carefully

Services/workloads can move between operators, service owners, organisations or product teams. Preserve identity where the same service/workload persists, while updating supported relationship/state.

BEFORE CHANGING

Confirm the intended Service & Workload ECZ-ID and current Parent/organisation/owner/operator context.

AFTER CHANGING

Verify new relationship, current state and evidence in Resolver.

RESPONSIBILITY BOUNDARY

A owner/operator change can coexist with one persistent Service/workload identity where the object remains the same. A successor or fork should not inherit identity merely because it replaces the original.

AUDIT HABIT

Record material owner/operator/provider/runtime changes and re-check proof.

SECURITY HABIT

Re-evaluate workload authentication, IAM/authorization, container/image integrity, vulnerability/configuration and runtime policy separately from Passport identity.

LIFECYCLE STATES

Make material workload lifecycle changes visible

Operational truth is useful when counterparties can tell that a service/workload is current, deprecated, suspended, withdrawn or archived according to supported canonical state.

CURRENT

The published record represents the intended current service/workload/runtime object context.

DEPRECATED

Use supported state/evidence to communicate deprecation where available.

SUSPENDED / WITHDRAWN

Temporary or permanent withdrawal should not be hidden behind stale "current" assumptions.

ARCHIVED / RETIRED

Retain identity continuity where appropriate while making lifecycle status explicit.

CONSUMER EXPECTATION

Counterparties should re-resolve rather than assuming an old operator, provider/runtime, runtime/deployment or lifecycle state remains current.

RESOLVER RE-CHECK POLICY

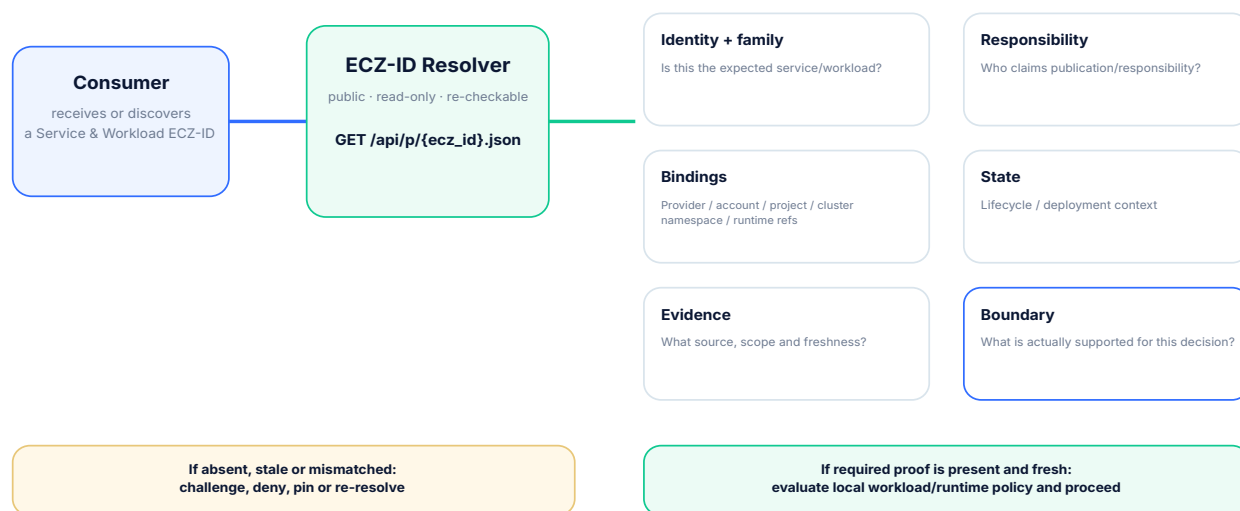
Freshness belongs in operations

Use re-resolution whenever organisation/owner/operator responsibility, provider/runtime/deployment bindings, runtime/environment context, evidence or lifecycle state can change faster than your cached decision.

RESOLVER RE-CHECK

Turn a Service & Workload ECZ-ID into a bounded decision input

Resolve the current public record, inspect only what is present, and fail safely when required proof is missing.



RE-CHECK AFTER

Deployment change ·
provider/runtime/deployment migration ·
operator change · evidence refresh · lifecycle
change.

RE-CHECK BEFORE

Consequential service/workload
deployment/upgrade decisions where stale
identity/context would matter.

CACHE RULE

Cache only according to use case. Re-resolve when freshness policy requires current proof.

DUPLICATE PREVENTION

One service/workload object, one canonical identity where supported

Duplicates create ambiguity for developers, security teams, counterparties and audit trails.

COMMON DUPLICATE TRIGGER

A new provider-native workload ID, account/project/subscription reference, cluster, namespace, service account, container, runtime/deployment reference, AWS subscription or sign-in issue is mistaken for a need to mint another identity.

CORRECT RESPONSE

Identify the intended service/workload, recover or reuse the canonical account/Parent/Passport where supported, then update bindings/state instead.

DUPLICATE CHECK

Before new issuance, resolve or search the known ECZ-ID and determine whether the existing record represents the same intended service/workload/runtime object.

SAME SERVICE/WORKLOAD

Preserve identity; update provider/runtime/deployment context.

FORK/SUCCESSOR/DIFFERENT WORKLOAD

Issue a distinct Passport when the object boundary genuinely differs.

ACCOUNT RECOVERY AND CUSTOMER ACCESS

Recover control without duplicating the service/workload estate

A sign-in or recovery problem is not evidence that the Service & Workload Passport should be reissued.

ACCOUNT PROBLEM

Recover supported account access and confirm the organisation/Parent context.

PASSPORT PROBLEM

Investigate issuance/reuse only if the canonical service/workload identity itself is missing or incorrect.

RECOVERY LAW

Restore access to the canonical estate first. Do not create replacement accounts, Parents or Passports merely to work around a sign-in failure.

AFTER RECOVERY

Confirm Dashboard shows the intended Service & Workload Passport.

THEN VERIFY

Resolve the same ECZ-ID publicly and confirm the record remains consistent.

COMMON FAILURES

Diagnose by layer

Separate acquisition/account/control problems from proof/binding/freshness and workload/runtime security problems.

WRONG WORKLOAD / ECZ-ID

Confirm object boundary and identifier before changing anything.

BINDING STALE

Update the supported provider/deployment/service reference/workload/deployment binding; do not mint by default.

PROVENANCE/EVIDENCE MISSING

Treat as absent unless supported evidence exists; do not infer runtime, image or software integrity.

RESOLVER NOT FOUND

Check identifier and acquisition/issuance state; distinguish from network/client failure.

STATE/EVIDENCE STALE

Refresh through the canonical control path, then re-resolve.

WORKLOAD SECURITY / RUNTIME-POLICY FAILURE

Diagnose workload authentication, IAM/authorization, container/image integrity, vulnerability/configuration or runtime/orchestration issues separately.

ESCALATE WITH LAYER CONTEXT

Tell support whether the failure is acquisition, account access, Passport issuance/reuse, Dashboard control, Resolver proof, binding/state or workload/runtime security.

SUPPORT ESCALATION

Send enough context - never secrets

Good support context shortens diagnosis while preserving security.

INCLUDE

- ECZ-ID / Passport ID if available
- AWS account context if relevant
- failed stage
- visible error
- occurrence time
- expected vs observed behaviour

NEVER INCLUDE

- passwords
- provider/runtime-provider/runtime access tokens
- AWS Marketplace registration tokens
- private signing keys / certificates
- other credentials or secrets

SUPPORT

support@ecocitizenz.com

If the issue affects a consequential production service/workload deployment or migration decision, apply your own workload/runtime security, change-control and runtime policies while the identity/proof issue is investigated.

ONE-MINUTE OPERATOR RUNBOOK

The recurring operational rhythm

Use this as the minimum repeatable check for a Service & Workload Passport in service.

1 Identify

Confirm the canonical Service & Workload ECZ-ID.

2 Inspect

Check Dashboard responsibility, bindings, state and evidence.

3 Update

Apply permitted contextual changes; preserve identity when the service/workload is the same.

4 Resolve

Re-check public proof after material change.

5 Challenge

If required proof is missing/stale/mismatched, do not silently infer.

6 Escalate

Send bounded context to support - never secrets.

OPERATING OUTCOME

Counterparties can continue to resolve one durable service/workload identity while supported provider-native IDs, owner/operator relationships, runtime/deployment bindings, state and evidence context change.