

ECZ-ID IoT Passport Operations, Lifecycle and Troubleshooting Guide

Operate device identity safely over time as responsibility, fleet, software, network, provider and lifecycle context changes.

IOT PASSPORT · OPERATIONS

PRIMARY READER

IoT administrator,
platform operations,
security operations,
estate owner.

SECONDARY READER

Support engineers, fleet
managers, developers
and governance teams.

WHEN TO READ THIS

The IoT 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 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 device identity; identity continuity must follow the actual object boundary.

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

FIRST OPERATIONAL CHECK

Confirm the canonical device before changing anything

Start every maintenance or troubleshooting action by identifying the intended IoT ECZ-ID and its current organisation/Parent context.

DASHBOARD CHECK

- correct IoT Passport
- correct organisation/Parent
- current state
- expected fleet/network/service bindings
- evidence present where expected

RESOLVER CHECK

- same ECZ-ID resolves publicly
- family/object is IoT
- published responsibility matches expectation
- current state/bindings are visible where supported

DO THIS BEFORE RE-ISSUING

If something looks wrong, investigate account access, relationship, state and binding changes before creating another Passport.

OPERATOR GOAL

Preserve one coherent identity for the intended device/object.

COUNTERPARTY GOAL

Keep public proof current enough to be independently re-checked.

OPERATING MODEL

Preserve identity; maintain current context

The recurring lifecycle is to confirm the canonical device, update supported context, refresh evidence/state and re-check Resolver.

OPERATIONS LIFECYCLE

Preserve identity; update the context around it

Most lifecycle changes should update supported bindings, state and evidence rather than mint a replacement identity.



DEFAULT RULE

When the physical/logical device is the same intended object, update the context around it rather than minting a replacement ECZ-ID.

CONTROL PLANE

Use Dashboard for permitted authenticated estate changes.

PROOF PLANE

Use Resolver to confirm what counterparties can independently observe.

CHANGING FLEET, NETWORK OR PROVIDER BINDINGS

Update context without fragmenting identity

Device estate changes are normal. Treat gateway/provider/network/fleet references as mutable supported context.

TYPICAL CHANGES

- fleet or site reassignment
- gateway replacement
- network/provider migration
- cloud device-registry move
- service/workload relationship change

OPERATOR SEQUENCE

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

DO NOT MINT BY DEFAULT

A new gateway, network, provider or cloud device ID is not by itself a reason to create a new IoT Passport.

PRESERVE IDENTITY WHEN

The same intended device/object persists.

RECONSIDER IDENTITY WHEN

The physical/logical object itself has genuinely changed.

FIRMWARE, SOFTWARE AND EVIDENCE REVIEW

Keep bounded operational context current

Where supported, software/firmware context and evidence should be reviewed when device software changes or when the evidence itself becomes stale.

REVIEW TRIGGERS

- firmware/software update
- device re-provisioning
- gateway/provider cutover
- fleet reassignment
- evidence expiry or replacement

REVIEW QUESTIONS

- is this still the intended device?
- does software context match current deployment?
- is evidence still in scope/fresh?
- did responsibility or lifecycle state change?

DO NOT CLAIM ATTESTATION WITHOUT EVIDENCE

Software/firmware version context can be useful, but it is not cryptographic hardware/firmware attestation unless the supported evidence explicitly establishes that.

REFRESH

Update supported evidence/state through the canonical control path.

VERIFY

Resolve again and inspect what counterparties can now observe.

RESPONSIBILITY, TRANSFER AND REASSIGNMENT

Change relationships carefully

Devices can move between teams, organisations, sites or operational owners. Preserve identity where the same device persists, while updating the supported relationship/state.

BEFORE CHANGING

Confirm the intended IoT ECZ-ID and current Parent/organisation/operator context.

AFTER CHANGING

Verify new relationship/assignment, current state and evidence in Resolver.

TRANSFER BOUNDARY

A reassigned device can retain its ECZ-ID where the object remains the same. A replacement device should not inherit identity merely because it fills the same fleet slot.

AUDIT HABIT

Record material relationship/assignment changes and re-check proof.

SECURITY HABIT

Re-evaluate local command/access credentials separately from Passport identity.

LIFECYCLE STATES

Make material device lifecycle changes visible

Operational truth is useful when counterparties can tell that a device is current, suspended, degraded, reassigned, withdrawn or retired according to supported canonical state.

CURRENT

The published record represents the intended current device context.

DEGRADED

Use supported state/evidence to communicate material degradation where available.

SUSPENDED / ISOLATED

Temporary unavailability or security isolation should not be hidden behind stale "current" assumptions.

RETIRED / WITHDRAWN

Retain identity continuity where appropriate while making lifecycle status explicit.

CONSUMER EXPECTATION

Counterparties should re-resolve rather than assuming an old state, fleet assignment or software context remains current.

RESOLVER RE-CHECK POLICY

Freshness belongs in operations

Use re-resolution whenever responsibility, fleet/network bindings, software context, evidence or lifecycle state can change faster than your cached decision.

RESOLVER RE-CHECK

Turn a presented device 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

Software update · provider/gateway migration · reassignment · evidence refresh · lifecycle change.

RE-CHECK BEFORE

High-consequence reliance, command or policy 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 device object, one canonical identity where supported

Duplicates create ambiguity for operators, developers, counterparties and audit trails.

COMMON DUPLICATE TRIGGER

A new cloud provider, device registry, gateway, AWS subscription, sign-in issue or fleet reassignment is mistaken for a need to mint another identity.

CORRECT RESPONSE

Identify the intended device, 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 device/object.

SAME DEVICE

Preserve identity; update context.

REPLACEMENT/DIFFERENT DEVICE

Issue a distinct Passport when the object boundary genuinely differs.

ACCOUNT RECOVERY AND CUSTOMER ACCESS

Recover control without duplicating the device estate

A sign-in or recovery problem is not evidence that the IoT 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 device 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 IoT 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 device-runtime problems.

WRONG DEVICE / ECZ-ID

Confirm object boundary and identifier before changing anything.

BINDING STALE

Update the supported fleet/network/provider/service binding; do not mint by default.

SOFTWARE/EVIDENCE MISSING

Treat as absent unless supported evidence exists; do not infer attestation or 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.

DEVICE AUTH/CONTROL FAILURE

Diagnose credentials, command authorization, network policy or safety controls separately.

ESCALATE WITH LAYER CONTEXT

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

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
- device credentials / API keys
- AWS Marketplace registration tokens
- private keys / certificates
- other credentials or secrets

SUPPORT

support@ecocitizenz.com

If the issue affects a consequential production or physical interaction, apply your own operational, safety and security controls while the identity/proof issue is investigated.

ONE-MINUTE OPERATOR RUNBOOK

The recurring operational rhythm

Use this as the minimum repeatable check for an IoT Passport in service.

1 Identify

Confirm the canonical device ECZ-ID.

2 Inspect

Check Dashboard relationship, bindings, state and evidence.

3 Update

Apply permitted contextual changes; preserve identity when the device 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 device identity while supported network, fleet, provider, software, state and evidence context changes.