

ECZ-ID IoT Passport Technical Reference

Technical semantics for device identity, responsibility, bindings, state, evidence, Resolver representation and integration.

IOT PASSPORT · TECHNICAL REFERENCE

PRIMARY READER

Developer, architect,
IoT/security engineer,
integration engineer.

SECONDARY READER

Platform engineers,
automated-system
designers, auditors and
technical evaluators.

WHEN TO READ THIS

You understand the
product and need to
integrate or interpret IoT
Passport proof
precisely.

RELEASE

2026.10 · 16 October
2026

WHAT YOU WILL KNOW AFTER READING

You can identify the canonical object, supported
relationships/bindings, state/evidence semantics,
machine route, lifecycle and safe failure
behaviour.

WHAT THIS DOCUMENT DOES NOT ESTABLISH

This is not an internal schema dump and does not
promise fields or evidence that the current
canonical implementation does not expose.

NEXT Read the Operations Guide for lifecycle changes, stale context, duplicate prevention and troubleshooting.

CANONICAL OBJECT

What exactly does an IoT Passport represent?

The canonical object is a device / IoT system / fleet member where applicable - not the network address, cloud resource ID or credential used at one moment.

CANONICAL IDENTITY

A persistent IoT ECZ-ID represents the intended device/object in the ECZ-ID identity model.

EXTERNAL IDENTIFIERS

Serials, cloud device IDs, gateway aliases, MAC/IP/network IDs and provider-native references remain bindings/context where supported.

IDENTITY BOUNDARY

Changing provider, network, fleet, software version or gateway does not automatically mean the intended device/object has changed.

PRESERVE IDENTITY WHEN

The same intended device/object persists and surrounding context changes.

CREATE DISTINCT IDENTITY WHEN

The canonical object boundary genuinely differs - for example a separate device that must remain independently referable.

IDENTITY GRAPH

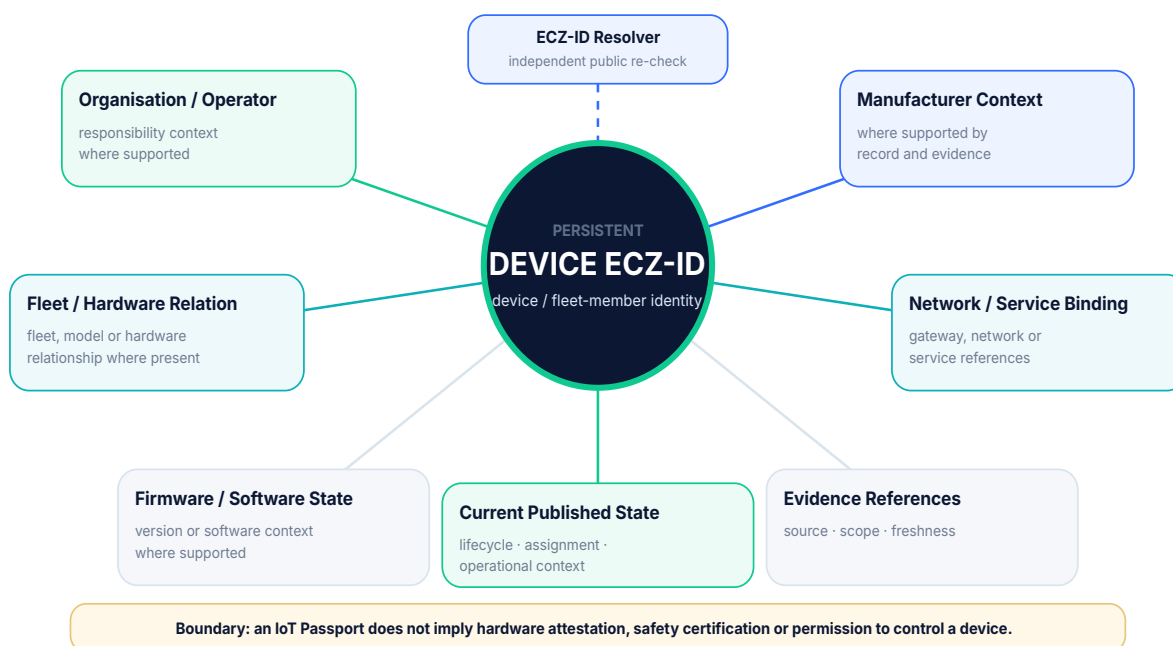
The IoT ECZ-ID at the centre of bounded context

The graph should be read as relationships and evidence around a persistent identity – not as a universal trust score.

IOT PASSPORT PROOF MODEL

What an IoT Passport can prove and contextualise

A persistent device identity with bounded responsibility, relationships, state, bindings and evidence that can be re-checked.



KEY LAW

Provider-native device identities, serials and network references may support the record but do not become the ECZ-ID authority root.

REQUIRED INTERPRETATION

Read only relationships and evidence actually present.

PROHIBITED INFERENCE

Do not infer attestation, safety or command authority from identity alone.

PARENT, ORGANISATION AND OPERATOR RELATION

Responsibility is represented as context, not universal assurance

Where present, a Parent/organisation relationship or operator context links the device object to the organisation claiming responsibility.

RELATIONSHIP SEMANTICS

The record can publish that this IoT ECZ-ID is associated with the shown Parent/organisation or operator context.

EVIDENCE SEMANTICS

The strength of any underlying claim depends on actual verification/assurance state and evidence present - not on the existence of the relationship alone.

TRANSFER / REASSIGNMENT

If responsibility or fleet assignment changes, preserve the device identity where appropriate and update the supported relationships/state rather than silently minting a new object.

CONSUMER BEHAVIOUR

Re-resolve after material responsibility changes.

AUTOMATION BEHAVIOUR

Treat missing responsibility context as missing; do not infer from provider metadata alone.

BINDINGS

How the persistent identity connects to a changing IoT estate

Bindings can associate the IoT ECZ-ID with supported external surfaces and identifiers.

FLEET RELATIONSHIP

Fleet, site or logical grouping reference where supported.

HARDWARE/MODEL REFERENCE

Model, serial or hardware relation where present and supported.

NETWORK/GATEWAY

Gateway, network or service connectivity reference where supported.

PROVIDER-NATIVE DEVICE ID

Cloud or platform device identifier retained as a binding/context.

SERVICE/WORKLOAD RELATION

References to the service/workload operating or consuming the device where supported.

REPOSITORY/PACKAGE EVIDENCE

Software/firmware package or description evidence where available.

BINDING LAW

A binding says the ECZ-ID record is associated with that external surface according to available state/evidence. It does not turn that external identifier into the canonical identity root.

FIRMWARE, SOFTWARE AND STATE

Separate persistent identity from mutable operational context

Where supported, current state can carry point-in-time lifecycle, assignment, firmware/software or operational context.

PERSISTENT LAYER

IoT ECZ-ID - stable referent for the intended device/object.

MUTABLE LAYER

Firmware/software version, fleet assignment, connectivity, lifecycle or operational state where present.

FRESHNESS

Consumers should re-resolve according to the consequence and expected rate of change.

ABSENT FIELD

Treat it as absent. Do not infer version, health, attestation or safety from another field.

STATE ≠ HEALTH CERTIFICATE

A published "current" or active state is not automatically proof of hardware health, firmware integrity or safe operation.

EVIDENCE

Bounded support for bounded claims

Evidence can support claims about identity, responsibility, state, bindings or other context. Its meaning depends on source, scope and freshness.

GOOD CONSUMER PRACTICE

- identify which claim the evidence supports
- inspect source and freshness
- avoid expanding scope beyond what is shown
- re-check when the evidence can change

UNSAFE PRACTICE

- treat any evidence as a universal trusted/safe badge
- assume hardware attestation when no attestation evidence exists
- assume every declaration was independently verified

PROOF MODEL

Evidence strengthens the interpretation of specific claims; it does not convert the Passport into a blanket device assurance certificate.

MACHINE RULE

Fail safely when evidence required by policy is absent.

HUMAN RULE

Read the evidence reference in the context of the actual decision.

AUTHORITY AND COMMAND BOUNDARY

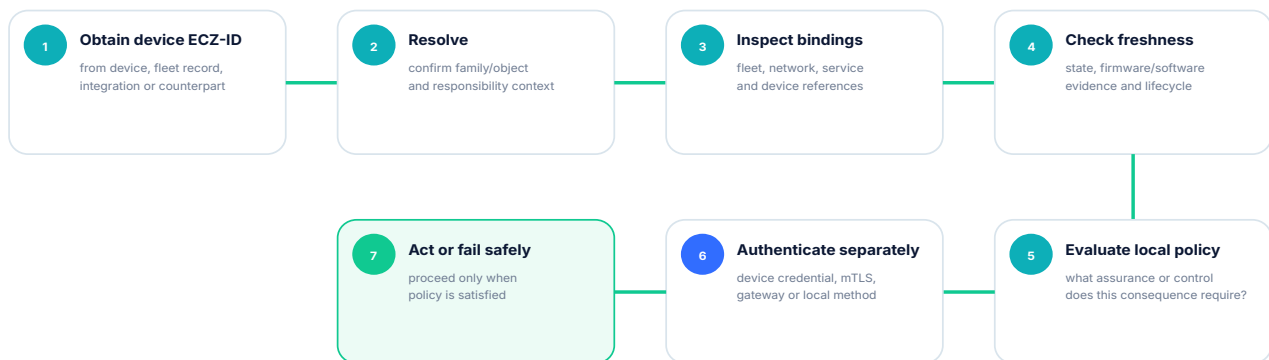
Identity is not permission to control a device

Some interactions require separate proof that an actor is allowed to send a command, change configuration, trigger an update or rely on a device signal.

PRE-CONSEQUENCE VERIFICATION

Verify identity and context before you rely on a device

Use Passport proof as one input; keep device authentication, command authorization and safety controls separate.



Boundary: IoT identity/proof does not replace device authentication, command authorization or physical safety controls.

If required proof is absent, stale or mismatched, challenge, deny, isolate or re-resolve according to policy.

PASSPORT INPUT

Which device is this and what responsibility/state/bindings/evidence are currently published?

CONTROL INPUT

What actor/session is permitted to take this specific action under local authentication, authorization and safety policy?

SEPARATE THE DECISION

Do not convert identity, responsibility or a provider binding into blanket command authority.

RESOLVER REPRESENTATION

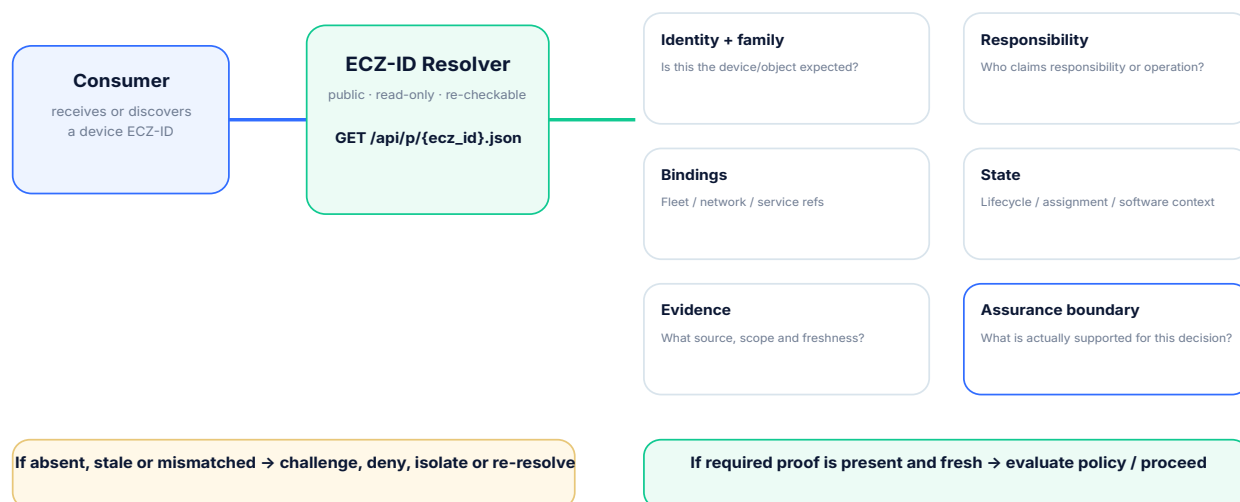
Public, read-only and independently re-checkable

Resolver exposes the bounded public record for an ECZ-ID. It is not the mutation/control plane.

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.



HUMAN ENDPOINT

Use the official Resolver experience to inspect the public record.

MACHINE ENDPOINT

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

INTERPRETATION

A 200 response means the record resolved; your system must still inspect family/object, state, bindings and evidence required for the decision.

MACHINE-CONSUMER CONTRACT

A safe integration pattern

Treat Resolver output as structured identity/proof context, not as an all-purpose “trust = true” signal.

1 · PARSE IDENTITY

Read the ECZ-ID and stable family/object fields.

2 · MATCH OBJECT

Confirm the expected IoT family and intended object relationship.

3 · EVALUATE CONTEXT

Inspect responsibility, bindings, state and evidence relevant to the decision.

4 · APPLY FRESHNESS

Re-resolve according to policy and consequence.

5 · FAIL SAFELY

If required proof is absent/mismatched/stale, challenge, deny or isolate.

6 · AUTHENTICATE SEPARATELY

Use the supported device/session authentication and command-authorization controls.

ANTI-PATTERN

Do not collapse one field, status pill or provider identifier into a universal decision across all IoT actions.

LIFECYCLE AND REASSIGNMENT

Keep the identity meaningful as the estate changes

A device can move through manufacture, provisioning, deployment, reassignment, maintenance, suspension and retirement while retaining one canonical identity where appropriate.

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.



UPDATE CONTEXT

Fleet/service/provider/network/software relationships and evidence can change around the same ECZ-ID.

UPDATE LIFECYCLE STATE

Make material operational/lifecycle changes visible through supported canonical state rather than leaving stale context.

OBJECT BOUNDARY

A replacement physical device is not automatically the same identity simply because it inherits the same role or fleet slot.

PROVIDER-SPECIFIC BINDINGS

Cloud/device platforms are context, not canonical authority

Provider identifiers can be useful for navigation and proof, but ECZ-ID remains the canonical identity layer.

EXAMPLES OF PROVIDER CONTEXT

Cloud IoT thing/device IDs, resource URNs/ARNs, project/subscription/account references, registry IDs, gateway IDs, fleet-group identifiers.

CANONICAL TREATMENT

Store or expose them only as supported bindings/evidence/relationships around the IoT ECZ-ID - never as the authority root.

PORTABILITY VALUE

When a device moves between provider/runtime contexts, counterparties can continue to refer to the same ECZ-ID while provider-native bindings are updated.

MIGRATION

Preserve identity; update provider/network/service references.

RE-CHECK

Verify the current binding after cutover before relying on cached context.

FAILURE HANDLING

Treat absence and ambiguity explicitly

Safe integrations distinguish not-found, missing-evidence, stale-context, wrong-object and transport/client errors.

NOT FOUND

Confirm the identifier; distinguish record absence from network/client failure.

WRONG FAMILY/OBJECT

Do not coerce a different Passport family into IoT semantics.

MISSING BINDING

Treat it as absent; do not infer from organisation or provider context.

MISSING EVIDENCE

Apply policy for unestablished proof; do not invent fallback assurance.

STALE CONTEXT

Re-resolve/refresh before consequential reliance.

AUTHENTICATION FAILURE

Diagnose device/session credential or authorization separately from Passport proof.

FAIL-CLOSED WHERE REQUIRED

The correct response depends on consequence and policy, but “missing” must never silently become “trusted”.

WORKED INTEGRATION EXAMPLES

Apply the model to real IoT patterns

Examples show how the same persistent identity can support different operational contexts without claiming more than the record proves.

INDUSTRIAL SENSOR

Resolve before accepting a high-consequence signal; confirm device identity, operator/fleet context, current state and required evidence.

PARTNER DEVICE

Verify the shared IoT ECZ-ID and responsibility context before onboarding the external device to an integration.

PROVIDER MIGRATION

Keep the device ECZ-ID stable while cloud/gateway/device-registry bindings change.

REASSIGNMENT

Preserve or change identity according to the actual device object; update responsibility/fleet relations and re-check proof.

COMMON THREAD

Use the ECZ-ID as the durable referent; use bindings/state/evidence as the current context; use separate security/safety controls for the actual action.

DEVELOPER QUICK REFERENCE

The external integration contract in one page

Use this page when implementing a verifier or integration around IoT Passport proof.

OBJECT

Device / IoT system / fleet member where applicable.

STABLE IDENTIFIER

Persistent ECZ-ID.

MACHINE ROUTE

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

INSPECT

Family/object · responsibility · state · bindings · evidence.

NEVER INFER

Hardware attestation · safety · firmware integrity · command authority.

WHEN FRESHNESS MATTERS

Re-resolve immediately before the policy decision.

SUPPORT

support@ecocitizenz.com — include ECZ-ID, failed step and visible error; never send secrets.