

ECZ-ID IoT Passport Overview and Customer Guide

Persistent, resolver-verifiable identity for devices and IoT actors across changing networks, fleets, software and providers.

IOT PASSPORT · OVERVIEW

PRIMARY READER

Buyer, technical evaluator, IoT/security architect, device/fleet owner.

SECONDARY READER

Developers, enterprise architects, operations, governance and procurement.

WHEN TO READ THIS

You are deciding whether a device or IoT actor needs durable identity and independently re-checkable context.

RELEASE

2026.10 · 16 October 2026

WHAT YOU WILL KNOW AFTER READING

You can explain the device object, responsibility, fleet/network bindings, current state, evidence and safe verification boundary.

WHAT THIS DOCUMENT DOES NOT ESTABLISH

An IoT Passport does not imply hardware attestation, device safety, vulnerability-free status or permission to control a device.

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

EXECUTIVE EXPLANATION

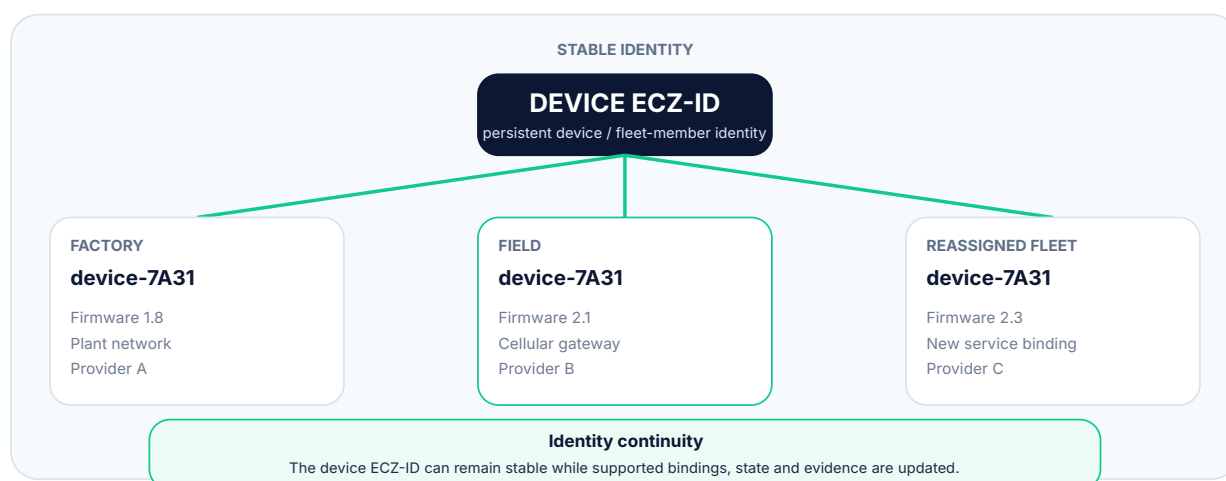
A durable identity anchor for devices that outlives one network or provider

IoT Passport separates the identity of the intended device or fleet member from current gateway, network, provider, software and service context.

PERSISTENT IOT IDENTITY

One device ECZ-ID; changing operational context

Keep the canonical device identity stable while supported network, fleet, firmware and provider context evolves.



WHY THIS MATTERS

A serial number, cloud resource ID or network address may be useful, but none alone necessarily provides a durable, provider-neutral identity that counterparties can independently re-check.

WHAT STAYS DURABLE

The IoT ECZ-ID for the intended device/object where continuity is appropriate.

WHAT CAN CHANGE

Fleet assignment, gateway/network, provider, firmware/software context, service bindings and evidence.

IOT PASSPORT IN ONE VIEW

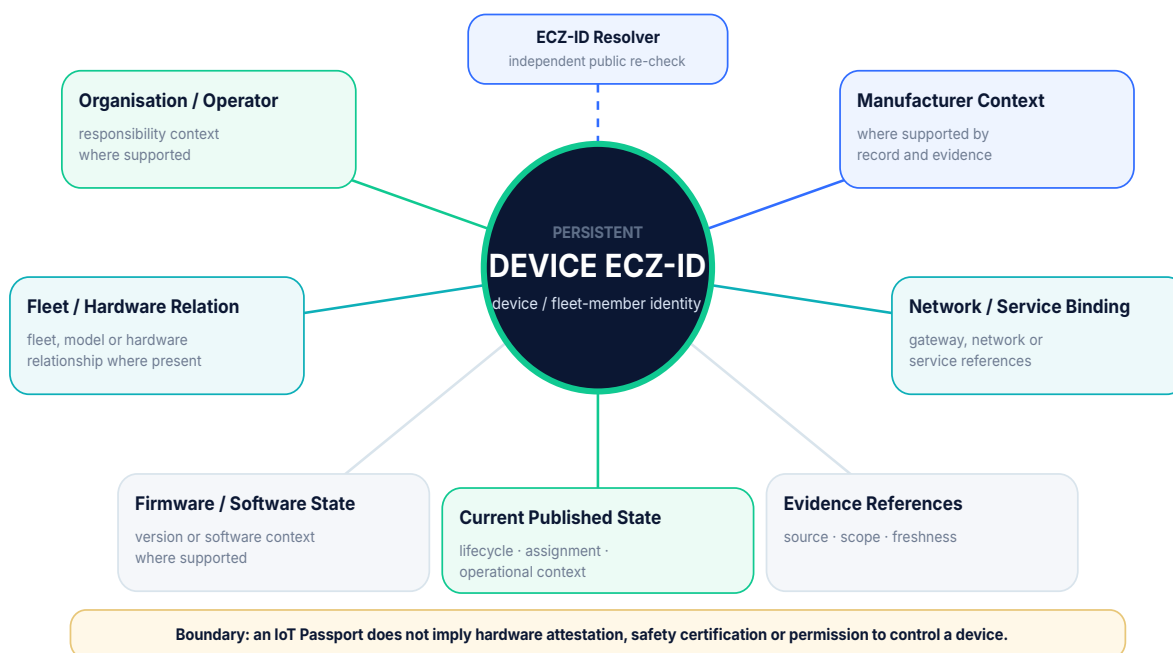
Identity at the centre; responsibility, relationships and evidence around it

The Passport can connect a persistent device ECZ-ID to organisation/operator context, fleet/hardware relationships, network/service bindings, current state and evidence where present.

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.



INTERPRETATION BOUNDARY

Do not infer hardware attestation, device safety, firmware integrity or command authority unless the relevant evidence and policy explicitly establish them.

RESOLVER

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

DASHBOARD

Authenticated customer control for permitted lifecycle and estate actions.

THE CUSTOMER PROBLEM

Physical identity, digital identity and operational context drift apart

Devices move between networks, gateways, cloud estates and fleets. Ownership, operator context and software state can change while the same physical/logical object persists.

WITHOUT A PERSISTENT IDENTITY

A device may be known by serial number, MAC address, cloud resource ID, gateway alias or fleet-local label - each tied to one context and vulnerable to reassignment or replacement.

WITH IOT PASSPORT

The device can present a stable ECZ-ID with bounded responsibility, state, bindings and evidence that counterparties can resolve again.

CORE QUESTION

Which physical/device actor is this, who is responsible for it, what current bindings/state are published, and can I independently re-check the record?

IoT Passport complements - rather than replaces - device credentials, hardware roots of trust, network admission, safety systems, firmware validation and runtime command authorization.

RESPONSIBILITY, OPERATOR AND MANUFACTURER CONTEXT

Know who is associated with the device - without overclaiming

Where supported, the canonical record can represent organisation/Parent responsibility, operator context and manufacturer-related evidence or relationships.

WHAT CAN BE PUBLISHED

Organisation/Parent responsibility, operator context, fleet or hardware relationship, and manufacturer-related evidence where supported.

WHAT IS NOT AUTOMATICALLY PROVEN

Ownership, manufacturer assurance, hardware authenticity or independent verification of every declaration. Read the actual evidence present.

CUSTOMER VALUE

Counterparties can evaluate a persistent device identity together with the organisation claiming responsibility and the bounded evidence actually available.

WHEN THIS MATTERS

Industrial IoT · fleet devices · partner equipment · connected infrastructure · multi-provider estates.

RE-CHECK DISCIPLINE

If responsibility or assignment can change, re-resolve before consequential use.

FLEET, NETWORK AND SERVICE BINDINGS

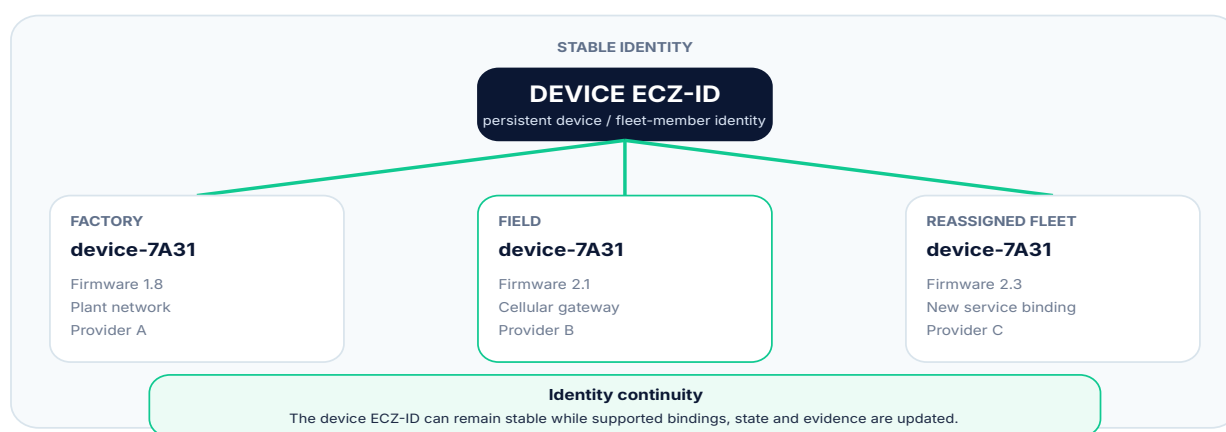
Stable identity; changing operational surfaces

Bindings connect the canonical device ECZ-ID to supported external references such as fleet membership, network/gateway identifiers, service/workload relationships and provider-native device IDs.

PERSISTENT IOT IDENTITY

One device ECZ-ID; changing operational context

Keep the canonical device identity stable while supported network, fleet, firmware and provider context evolves.

**BINDING ≠ IDENTITY**

A provider device ID, gateway alias, IP, MAC address or fleet-local reference can change or be reassigned. It remains context around the ECZ-ID.

HARDWARE RELATION ≠ ATTESTATION

A model, serial or hardware relationship can be useful context, but does not imply cryptographic hardware attestation unless supported evidence says so.

GOOD OPERATING MODEL

Preserve the ECZ-ID when the same intended device/object persists; update supported network, fleet, provider and service relationships around it.

SOFTWARE, FIRMWARE, STATE AND FRESHNESS

Current proof should be treated as point-in-time

Device identity may persist while firmware/software, assignment, connectivity, lifecycle state and evidence change.

IDENTITY

The persistent IoT ECZ-ID answers which device/object is being represented.

CURRENT PUBLISHED STATE

Point-in-time lifecycle, assignment, firmware/software or operational context where supported.

FRESHNESS

Do not cache a trust conclusion indefinitely. Re-resolve when the consequence requires current proof.

EVIDENCE

Interpret each evidence reference according to source, scope and freshness.

RE-CHECK REQUIRED

A previously valid fleet assignment, software state or network binding can become stale. Identity continuity only helps if consumers re-check current context when it matters.

IDENTITY IS NOT DEVICE CONTROL AUTHORITY

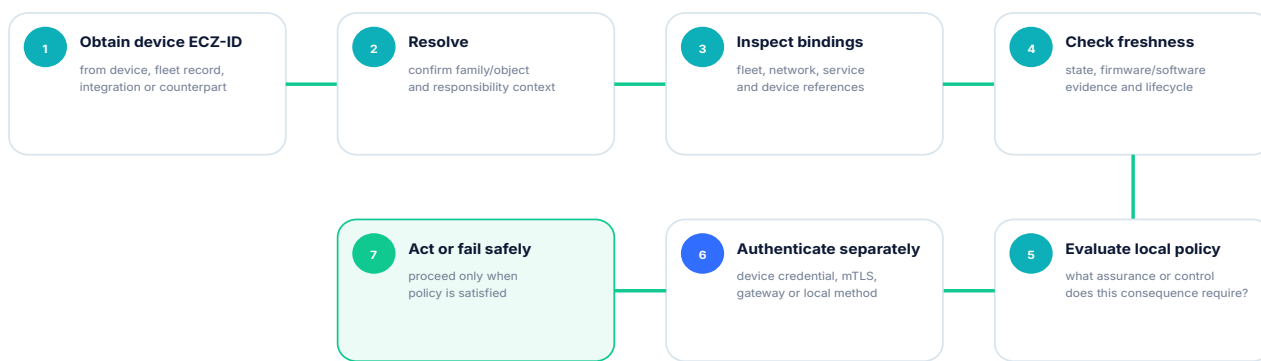
Use the Passport before the consequence - not instead of security controls

IoT Passport can help establish which device is intended and what context supports that identity. Authentication, authorization and physical safety remain separate.

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.

IDENTITY QUESTION

Is this the device/object I expected, with the responsibility and bindings I require?

CONTROL QUESTION

Is this actor/session allowed to command, configure, update or rely on the device under local policy?

DO NOT COLLAPSE THESE QUESTIONS

A valid IoT Passport is not automatic permission to send commands, approve firmware, trust sensor data or bypass safety controls.

HIGH-VALUE USE CASES

Where persistent, re-checkable device identity helps most

The strongest use cases are those in which device context changes while accountability and identity continuity still matter.

FLEET CONTINUITY

Keep one canonical device identity across fleet, gateway or provider changes.

PARTNER VERIFICATION

Give counterparties a re-checkable device identity instead of only a local alias.

OPERATIONAL HANDOFF

Preserve identity as responsibility, location or service relationships change.

SECURITY POLICY INPUT

Use device identity/state/bindings as one bounded input to local policy.

EVIDENCE NAVIGATION

Connect supported evidence to the persistent object rather than one transient endpoint.

CROSS-PROVIDER ESTATE

Treat cloud/provider-native identifiers as bindings around one ECZ-ID.

VALUE PATTERN

The Passport is most useful when the organisation needs a stable referent while the surrounding device estate keeps changing.

SAFE VS UNSAFE CONCLUSIONS

Use the record for the question it actually supports

A Passport creates bounded identity/proof context. It should not be stretched into claims that the record does not establish.

SAFE CONCLUSIONS

- this is the ECZ-ID record being presented for the device
- the record publishes the shown organisation/operator relationship
- the shown state/bindings/evidence are currently published
- the record can be independently re-checked

NOT ESTABLISHED BY PASSPORT ALONE

- hardware attestation
- device safety or vulnerability-free status
- firmware integrity
- permission to send commands
- accuracy of every sensor reading
- independent verification of every declaration

ABSENCE MEANS ABSENT

If evidence, state or a binding you require is not present, treat it as not established. Do not infer it from marketing or from the mere presence of a Passport.

RE-CHECK

Resolve again when freshness matters.

POLICY

Apply local safety/security/authorization controls to the actual consequence.

DEPLOYMENT FIT

Who should use an IoT Passport?

Adopt where persistent identity and independent re-checkability are valuable across a changing IoT estate.

STRONG FIT

Industrial/fleet IoT where device identity must survive network/provider/fleet changes.

STRONG FIT

External or partner interactions where a counterparty needs to verify a device object.

STRONG FIT

Multi-provider estates that need provider-neutral device identity with provider IDs retained as bindings.

NOT A REPLACEMENT

Device authentication, hardware attestation, PKI, network admission, safety systems or firmware controls.

BUYER DECISION

If your current identifiers are tightly coupled to one network/provider or cannot be independently re-checked, an IoT Passport can provide the durable identity layer around them.

HOW TO VERIFY AN IOT PASSPORT

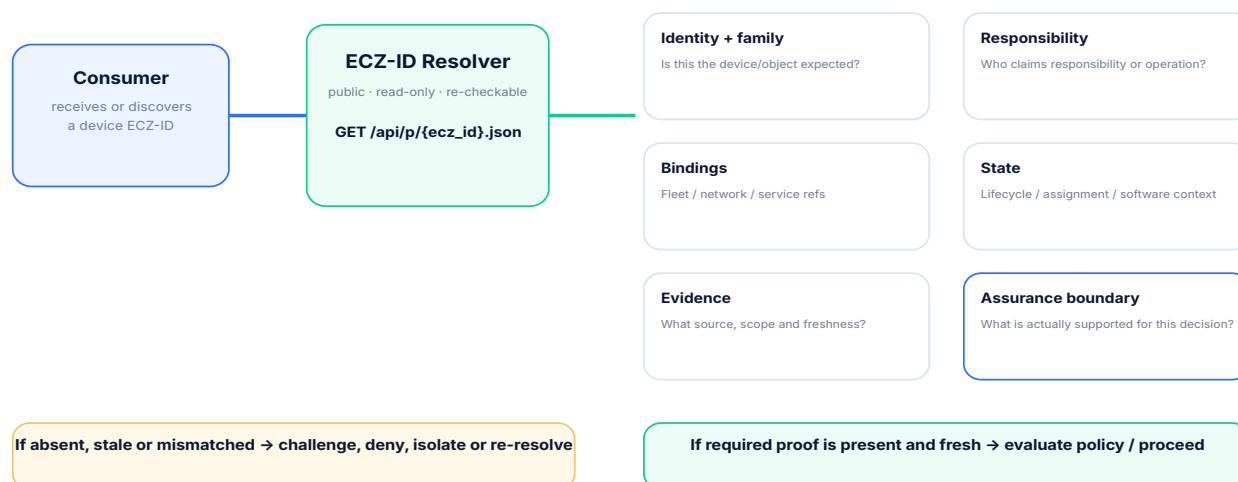
Resolve, inspect, interpret, re-check

Verification is intentionally bounded: identify the object, inspect responsibility and current context, then apply your own policy for the consequence.

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 PATH

Open Resolver, confirm family/object, responsibility, state, bindings and evidence, then re-check when freshness matters.

MACHINE PATH

GET
https://api.ecocitizenz.com/api/p/{ecz_id}.json
and fail safely when required data is absent.

NEXT

For acquisition, continue to the IoT Passport AWS Marketplace Getting Started and Technical Guide.

DECISION CARD

The IoT Passport in 60 seconds

Use this page as the executive summary before acquisition or architecture review.

OBJECT

Device / IoT system / fleet member where applicable.

PERSISTENT IDENTITY

One ECZ-ID can remain referenceable as network/provider/software context changes.

RESPONSIBILITY

Organisation/operator context where supported.

BINDINGS

Fleet, hardware, network, gateway, service and provider-native references where supported.

EVIDENCE + STATE

Bounded current context; re-check when freshness matters.

BOUNDARY

Not hardware attestation, safety certification or device-control permission by itself.

CUSTOMER OUTCOME

A counterparty can refer to and independently re-check a durable device identity instead of treating one transient network/provider identifier as the whole truth.