USE CASE 03 / COTO PPT 56

Physical carpet identity and digital passport

Proposed operating design, version 2.0, 28 October 2026. Source concepts are from the COTO presentation; detailed controls, timelines, test gates and charging units are implementation proposals, not PPT quotations or live-service promises. All examples are synthetic. Prices and trade principal remain USD; local labour payments follow mandatory local rules. No invented partners, committed customers, tariffs or efficiency results are asserted.

Business outcome

Give each carpet a durable scannable identity and a truthful, permission-filtered product record, starting with low-cost QR labels before RFID investment.

Accountable roles

The passport administrator controls ID issuance and revocation; the manufacturer binds the tag to the rug; qualified reviewers approve claim scope; owners/custodians attest only their authorized events.

Required information

Opaque carpet ID; batch/design revision; construction/materials/dimensions; maker-group/site references; tag serial and issuance/replacement record; product photographs under permission; claim/evidence status and expiry; care/repair information; permitted public fields.

Separate lifecycle states

Passport: draft > identity-bound > reviewed > published > updated OR suspended > retired. Tag: issued > attached > checked > replaced/revoked. A public passport scan has no power to change ownership, payment or private data.

THE OPERATING WORKFLOW

From a real input to an approved outcome

01 / Define the minimum passport

Responsible: Passport administrator

Choose the essential fields and audience: public product/care summary, partner trade history and restricted evidence. Identify supplier declarations distinctly. Do not expose worker identity, home address, bank information, private prices or the buyer's personal details.

02 / Bind a physical identity

Responsible: Manufacturer + checker

Print a durable label with a random ID, a first-party HTTPS scan link and a human-readable fallback. Attach it without damaging the rug, photograph the association and verify the scan against the right product. A QR code can be copied; it is a link, not proof of authenticity.

03 / Check before publication

Responsible: Reviewer

Match specifications and lawful design permissions to the rug; inspect relied-on certificates and issuer/scope/expiry. Publish only fields actually supported. Missing evidence stays marked pending or unknown rather than displaying an unconditional verification badge.

04 / Serve the appropriate view

Responsible: Passport service

Public scans show only approved product/care details and current claim status. Signed-in businesses receive authorized information. Rate-limit retrieval, use unguessable references and enforce authorization server-side; obscurity alone does not protect private records.

05 / Maintain the journey

Responsible: Authorized custodian/service partner

Append receipt, repair and authorized claim updates with evidence and timestamps. Replacing a tag requires a reason, old/new serial linkage and reviewer approval. Revoke the old scan mapping or show a replacement notice; do not issue a second independent product identity.

06 / Review expiry and anomalies

Responsible: Administrator + reviewer

Queue certificate expiry, repeated anomalous scans or a reported counterfeit for investigation. Do not treat scan geography as definitive identity or use tracking without a lawful purpose. Suspend disputed claims while preserving safe access to basic care information.

CONTROLS AND IMPLEMENTATION

Make exceptions visible

Failure handling and human safeguards

Lost/damaged tag: validate against batch, photos and custody evidence before reissue. Duplicate tag: mark disputed and investigate both physical goods. Sold rug: do not publicly expose its new owner. Recalled/unsafe item: display the authorized service notice and retain a safe reporting route. Withdrawal of image permission: remove affected publicity where required without falsifying product history.

Blockchain, AI and private evidence

The public passport resolver is a new service, not currently deployed. Add signed QR/RFID issuance records if needed, but physical checks remain essential. Future blockchain anchoring can record a version digest and revocation reference, never personal ownership details. AI may draft care text from approved materials/specifications; a qualified person verifies it before publication.

Start with the existing pilot

Create the source product sheet, record the pilot lot and evidence fingerprint, and test printed QR labels against controlled prototype product sheets. Do not distribute a public scan URL until the resolver and privacy filtering have passed testing.

Additional software required

Add item-level records, a permission-filtered public resolver, tag serial registry, claim/expiry fields, revocation/reissue workflow, access logging and abuse controls. RFID is optional and must be costed per reading site; no requirement to buy it for the first pilot.

Current boundary: invited profiles, lot/order records and approvals, selected fulfilment events, invoices, operator-attested receipts, balances and protected private audit are configured. Several actions are API-only. Public blockchain worker, payments/crypto/escrow, AI, bidding, public passport resolver, evidence-vault uploads and the richer registers described here are not activated by publishing this design. Roles are proposed functions to assign and resource, not additional named team appointments.

PILOT AND COMMERCIAL VALIDATION

Prove the mechanism before scaling

Synthetic worked scenario

Prepare ten synthetic item passports across two batches. Use QR labels, then simulate one copied tag, one expired certificate and one legitimate replacement. Confirm a public visitor cannot retrieve buyer, wage, price or restricted evidence records.

Required acceptance tests

Guess another identifier; open a revoked tag; substitute a label onto another rug; inspect the public API response for restricted fields; confirm scan itself cannot change title. The test must include a physical mismatch, not just working URLs.

Measures and go/no-go

Correct physical-to-record matches; unauthorized field exposure (target zero in the test); successful legitimate reissues; expired-claim suppression; cost per maintained passport. No counterfeit-prevention guarantee is inferred.

Proposed payer, charging unit and cost drivers

Proposed payer: manufacturer/retailer under a passport service order. Unit: issued and maintained item/batch, plus optional tagging or inspection cost. Quote external tag/reader costs transparently; no extra fee for inventing a claim.

Pilot sign-off record

Before execution, assign the actual responsible people, permitted data source, cohort/route, approved costs, test dates, evidence reviewer and release authority. Record each test outcome, unresolved exception, manual fallback and rollback procedure. Do not activate an unapproved model, payment provider, public-chain transaction or unsafe equipment connection.

Source and scope

COTO presentation slides 56. Detailed operating steps, test cases and commercial units are new implementation proposals. Read operating-model.pdf for shared controls, templates, release gates and primary technical references. The legal pack remains draft until completed and reviewed.