**PRD-21 — Supplier & Certificate Verification Hub**

**Intent**  
Verify supplier documents (CoC/CoA/test reports) tied to **product versions**. Detect tampering, expiry, and mismatches; block risky use until reviewed.

**Preconditions**

* Supplier linkage (Partner Store) established for each product or component.
* Allowed certificate types & schemas per category.
* Document vault with virus scan + hashing (from PRD-11).

**Flow (happy path)**

1. **Upload/Fetch**: supplier uploads via portal or you pull via connector; run scan; store **File Hash Receipt**.
2. **AI-Assist Parse** (advisory): OCR + layout → extract key fields (lot range, material spec, test results); show **Evidence Tiles** (page/snippet + confidence).
3. **Signature/Stamp Check**: verify digital signatures/watermarks where present; compute tamper score.
4. **Bind to Version**: link certificate to ProductVersion (and BOM component if kit); validate that lot/serial ranges (PRD-17) align.
5. **Compliance Verdict**: pass/warn/fail with WHY; create/refresh **Certificate Status** on product header; set reviewer as owner.
6. **Expiry & Renewal**: scheduler raises tasks before expiry; expired **FAIL** blocks new use; existing docs remain but flagged.

**Edge cases**

* Name/spec mismatch (supplier vs product) → open exception with side-by-side diff.
* Suspicious doc (tamper score high) → quarantine; notify compliance.
* Missing lots on a lot-tracked item → fail with fix link to PRD-17 capture.

**Done when**

* Each certificate is hash-tracked, version-bound, and has reviewer verdict + expiry.
* “New use” of products with **failed/expired** certificates is blocked until clearance.