**OPS-18 — Secrets/Keys Rotation Runbook (Zero Downtime)**

**Intent**  
Rotate API/webhook keys and KMS materials **without breaking tenants**.

**Preconditions**

* Dual-key support in gateway & webhook signer; KMS rotation policy.

**Flow**

1. **Announce**: publish rotation window & dual-key overlap.
2. **Mint**: issue new API/webhook keys; mark old as “deprecating”.
3. **Dual-sign/verify**: accept both keys; sign webhooks with both kids during overlap.
4. **Cutover**: flip primary to new; monitor error rates.
5. **Revoke**: disable old keys; verify all tenants switched.
6. **KMS**: rotate signing keys; re-seal Trust Stamps with new chain for future snapshots.

**Edge cases**

* Slow tenant migration → extend overlap window per tenant; alerts.
* Clock skew → tolerate with leeway in signature time windows.

**Done when**

* Zero auth failures post-cut; all keys rotated; rotation report stored (who/when, error rates, fallback invocations).