**ADD-12 — Customer-Managed Keys (CMK) Option**

**Status:** New (advanced/enterprise)

**Intent**  
Let tenants bring their own KMS keys to encrypt their data at rest, with provable separation.

**Actors**  
KMS Broker • Tenant Admin • Security • Audit Vault

**Preconditions**

* Your platform KMS live; envelope encryption pattern in place.

**Flow**

1. **Key Onboarding:** tenant links their KMS (AWS KMS/Azure Key Vault/GCP KMS); verify permissions.
2. **Scope Selection:** specify which artifacts are CMK-encrypted (KYC, partner IDs, tokens).
3. **Rotation:** support tenant-initiated rotation with minimal downtime.
4. **Key Unavailable:** fail-closed for sensitive ops; read caches honor TTL; alert tenant & ops.
5. **Attestation:** export **Encryption Proof Report** (which data uses which key + last rotation).

**Edge Cases**

* Tenant revokes key → suspend access; provide recovery guidance.
* Multi-region CMK policies → enforce regional KMS endpoints.

**Done when**

* Writes/reads succeed under CMK; rotation tested; reports generated; failure behaviors verified.

**Deliverables**  
CMK admin UI, KMS broker service, encryption attestation report.