GoldSafe Purchase Engine

Capacity, Security & Settlement Architecture

Reference: COV-GS-SPEC-2026-V1 · Demonstration configuration · Sandbox mode

Non-custodial conditional fund orchestration. GoldSafe never holds, controls or carries buyer funds on its balance sheet.

Buyer funds are placed into settlement-restricted rails operated by the underlying commercial infrastructure (Covalt). GoldSafe and the BookSafe engine coordinate evidence and stage approvals only. No stage of value is disbursed by the marketplace, and no marketplace instruction can release funds on its own — each release is executed by the infrastructure layer once the evidence conditions for that stage are confirmed.

Four-stage verification and release schedule

Stage	Verification gate	Allocation	Evidence required
1	Allocation & Documentation	10%	Trade confirmation, consignment allocation record, buyer identity and source-of-funds checks.
2	Independent Laboratory Assay	30%	Accredited laboratory assay certificate (PMMC or equivalent), purity and weight confirmation, serial/hallmark record.
3	Bonded Custody & Armored Transit	30%	Bonded custody receipt, insured armored transit manifest, export and customs sign-off where applicable.
4	Vault Intake & Final Settlement	30%	Vault intake receipt, allocated holding confirmation, buyer acceptance of title transfer.

No funds release until accredited laboratory assay evidence is verified

Stage 2 is a hard gate. Beyond the opening 10% allocation stage, no portion of the consignment value can be released until an accredited laboratory assay certificate has been submitted and verified against the allocated serial and hallmark record. If assay evidence is not produced, or fails verification, the remaining stages do not advance and the trade is resolved through the cancellation or dispute path defined on the trade confirmation.

Security and capacity posture

Tenant isolation. Each portal is a separate tenant. Trades, buyers, dealers and documents are readable only within the owning tenant, enforced at the database layer rather than in the interface.

Credential handling. Infrastructure credentials are held server-side only and are never exposed to the browser or to portal users.

Event integrity. Settlement events arrive on a single signed endpoint, are signature-verified with a timestamp tolerance, and are processed idempotently so duplicate deliveries cannot double-advance a stage.

State discipline. Financial and stage state is only ever copied from confirmed infrastructure events; it is never inferred by the portal.

Capacity. Consignments are processed per trade with no batching dependency, so throughput scales with dealer and assay capacity rather than with portal load.

Scope note

This briefing describes system architecture and configuration. It is not a statement of regulatory approval, licensing, trading history or available payment methods in any jurisdiction. Settlement behaviour depends on the connected infrastructure configuration and the applicable agreements.