

Crypto Software — Enterprise Architecture Brief

Reference architecture & due-diligence brief • v0.1

Purpose

Bank/fintech-facing technical discovery reference. No unverified certifications, production metrics, customer volumes or insurance claims.

Architecture

Access/API → Policy & Risk → HSM/MPC signing boundary → blockchain nodes/indexers.
On-premise/private-cloud options depend on trust boundaries and residency.

Custody

Hot/warm/cold tiers, maker-checker, allowlists, limits, time locks, 2-of-3 or 3-of-5 quorum patterns, recovery ceremony and audit trails.

Cryptography

HSM/MPC/trusted-execution are threat-model decisions. GG18/GG20/CMP, Thales Luna, Utimaco, AWS CloudHSM, Intel SGX and Nitro Enclaves are evaluation families, not universal-use or partnership claims.

Exchange

REST/WebSocket, optional FIX adapter, order-book snapshot/delta, event pipeline, idempotency and reproducible benchmark methodology.

RWA

ERC-20/ERC-1400/ERC-3643 families; eligibility may be on-chain, off-chain or hybrid based on privacy, regulation and lifecycle.

Regulatory engineering

Technical control mapping can cover SPK/MASAK, MiCA/DORA resilience and FATF Travel Rule integration boundaries. Legal compliance remains subject to the institution and authorities.

Resilience

SLA, RTO and RPO are contractual architecture inputs determined by topology, replication, operating model and acceptance tests.

Evidence

Threat model, ADRs, dependencies, access matrix, key ceremony, DR tests, benchmark method, audit trail, vendor register and exit/handover.

Evidence policy

SOC 2, ISO, PCI DSS, pentest, audit, insurance, TPS, latency, uptime and customer metrics are displayed only when verifiable evidence exists.

Due-diligence checklist

Area	Evidence expected
------	-------------------

Security	Threat model, access matrix, signing boundary, audit trail
Resilience	HA/DR topology, failover/failback tests, RTO/RPO
API	OpenAPI, idempotency, webhook signature, rate limits
Compliance	Control mapping, AML/KYT/Travel Rule adapter boundaries
Exit	Source/IP terms, runbooks, data export, key ownership