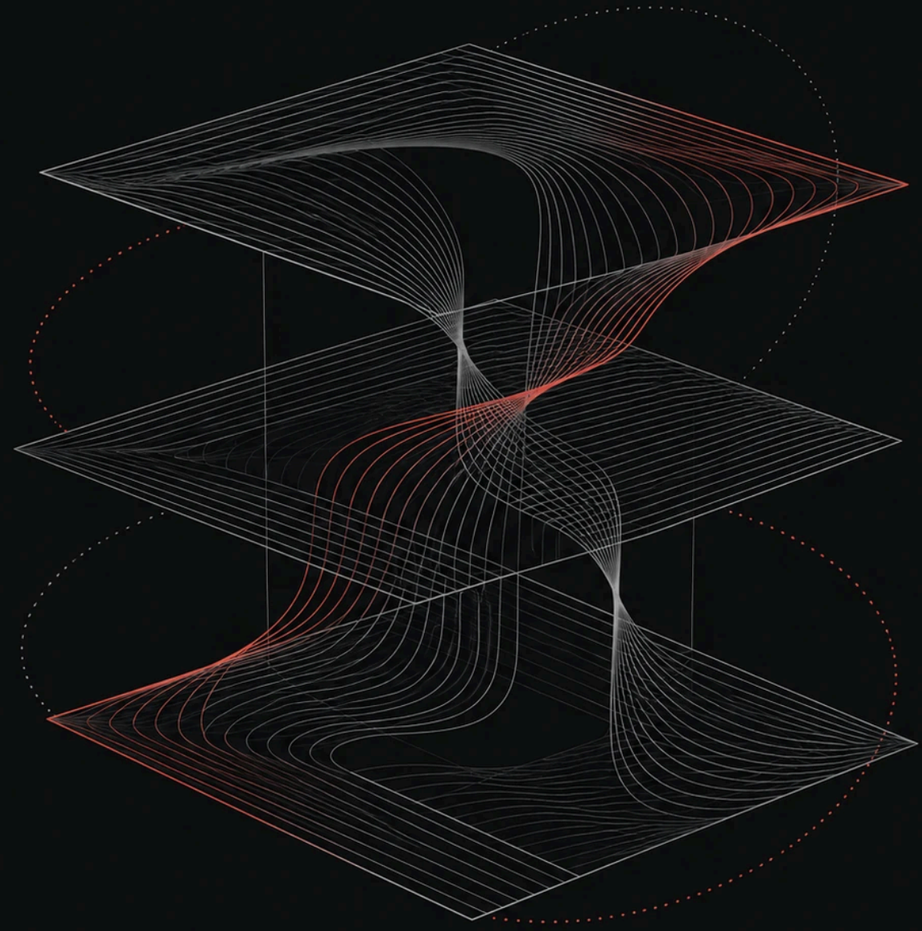
TECHNICAL ANNEX / ARCHITECTURE • CONTROLS • EVIDENCE

The architecture behind the experience.

A modular operating model for banking workspaces, approved services and accountable agent interactions.

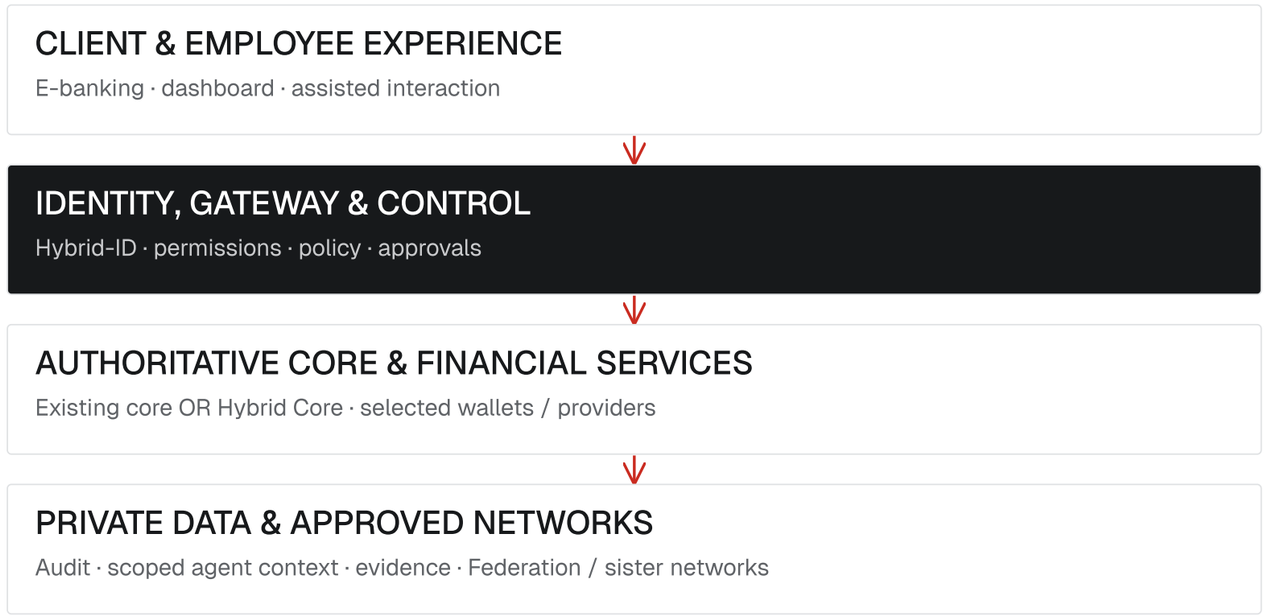


Built on Hybrid technology. Integrated by OVRYDE.

A01 / THE MODULAR STACK

One experience. Explicit system boundaries.

Compose the modules around the institution’s authoritative records and selected service providers.



Experience

Client e-banking, employee workspace and assisted interactions.

Control

Hybrid-ID, gateway, permissions, institutional policy and review.

Financial services

Hybrid Core OR an existing core; separately accepted wallets, payment routes and market providers.

Data & connectivity

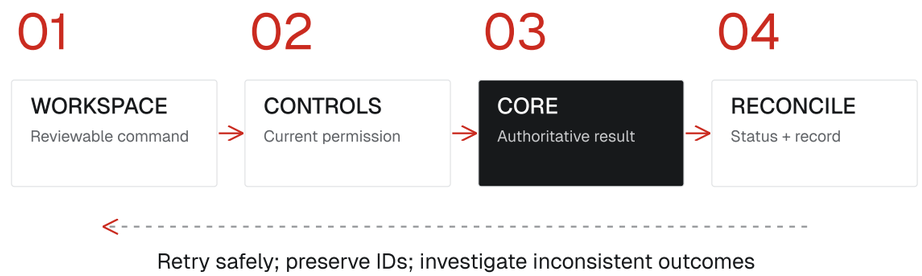
Private records, scoped agent context, proof services, Federation and approved sister-network connections.

Reference architecture. An architectural connection is not evidence that a specific provider adapter is already deployed.

A02 / RECORDS, COMMANDS & RECONCILIATION

One authoritative core. A synchronized working view.

In an existing-core deployment, Hybrid Banking prepares and routes instructions; the established core confirms what actually happened.



Read

Synchronize permitted context with source identifiers, timestamps and status.

Write

Validate the request, confirm authority and submit an idempotent command.

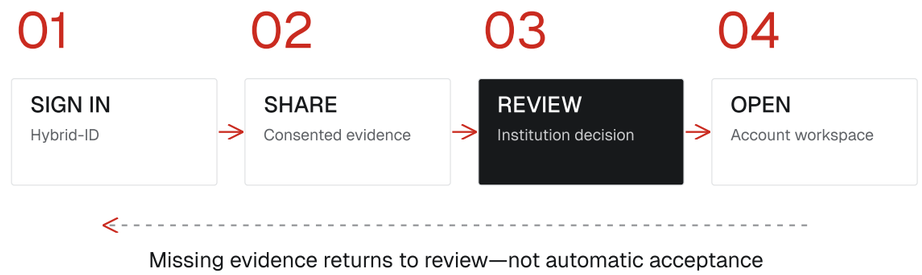
Reconcile

Receive the authoritative result; retry safely and investigate any mismatch.

A03 / IDENTITY & ONBOARDING

Reuse identity. Decide eligibility.

Hybrid-ID sign-in, permissioned verification evidence and bank onboarding are separate decisions.



Client

Authenticate; review requested disclosure; provide relationship details.

Institution

Apply onboarding rules, inspect evidence and resolve required reviews.

Workspace

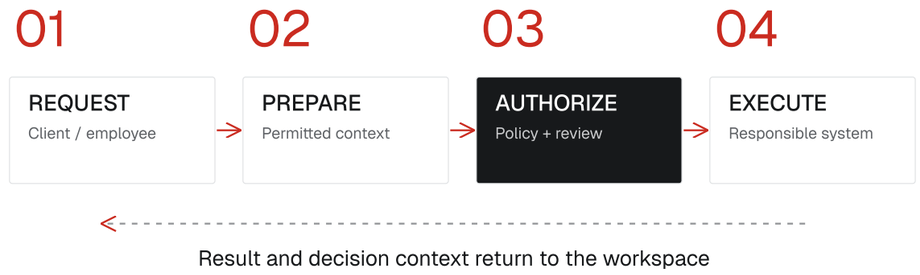
Record approval and create the appropriate account record; preserve the evidence trail.

Hybrid-ID trust metadata informs review; it is not a universal acceptance score. The controlled pilot starts accounts at zero and does not establish a licensed banking relationship.

A04 / AGENT AUTHORITY

Intent is an input. Authority is checked.

Use the same permission and policy boundaries whether a request comes from a form or an assisted interface.



Identity & scope

Bind the actor and permitted operation to the request.

Review & authorization

Present the proposed action, require client confirmation and independent approval where applicable.

Execution & record

Route to the responsible system and record the outcome, approval and relevant context.

Guided pilot commands are available. Portable external-agent credentials, open-ended orchestration and local-model interfaces must be integrated and tested; an agent never inherits unlimited spending authority.

A05 / PAYMENTS & RECIPIENTS

Validate the destination. Recheck before release.

Controls apply at recipient setup and again when a payment is authorized or processed.

01	**Recipient setup**	Capture the beneficiary and destination context. Route new or changed recipients through the configured checks and reviews.
02	**Instruction & approval**	Check amount, limits, current geographic policy and required screening. Preserve purpose, actor and independent approval where required.
03	**Processing & status**	Send only through an accepted execution connection. Keep pending, failed and confirmed outcomes distinct; reconcile against the authoritative record.

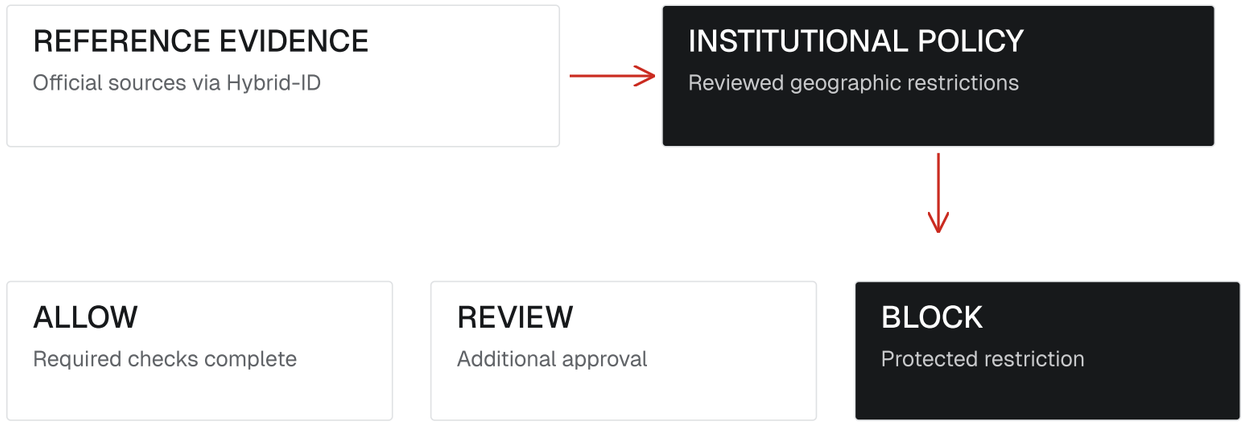
> Scheduled and salary workflows prepare instructions; the pilot does not imply external ACH or wire settlement.

The institution must scope inbound-origin handling and each rail's destination data. Internal simulation is not external money movement.

A06 / GEOGRAPHIC POLICY & SCREENING

A country rule is policy. A person match is evidence.

Keep geographic restrictions distinct from a listed person’s address or nationality.



A listed person’s address does not define a country ban.

Start conservatively

The pilot selects all six supported sanctions-list families by default; authorized compliance staff govern configuration.

Apply reviewed geography

Bind restrictions to reviewed country-program evidence and institutional policy. Protected exclusions cannot be relaxed by ordinary overrides.

Manage change & freshness

Record the actor, reason and policy version. Missing required evidence holds affected actions; refreshed evidence triggers reassessment.

Pilot country clearance presets: EU/EEA, UK, Switzerland, US and Singapore, subject to protected restrictions and all other checks. Other configured higher-risk countries require review; country clearance is not KYC approval.

A07 / TRANSACTION MONITORING

Turn a pattern into a reviewable case.

Help teams investigate changing behavior without presenting an alert as a finding of wrongdoing.

Detect & explain

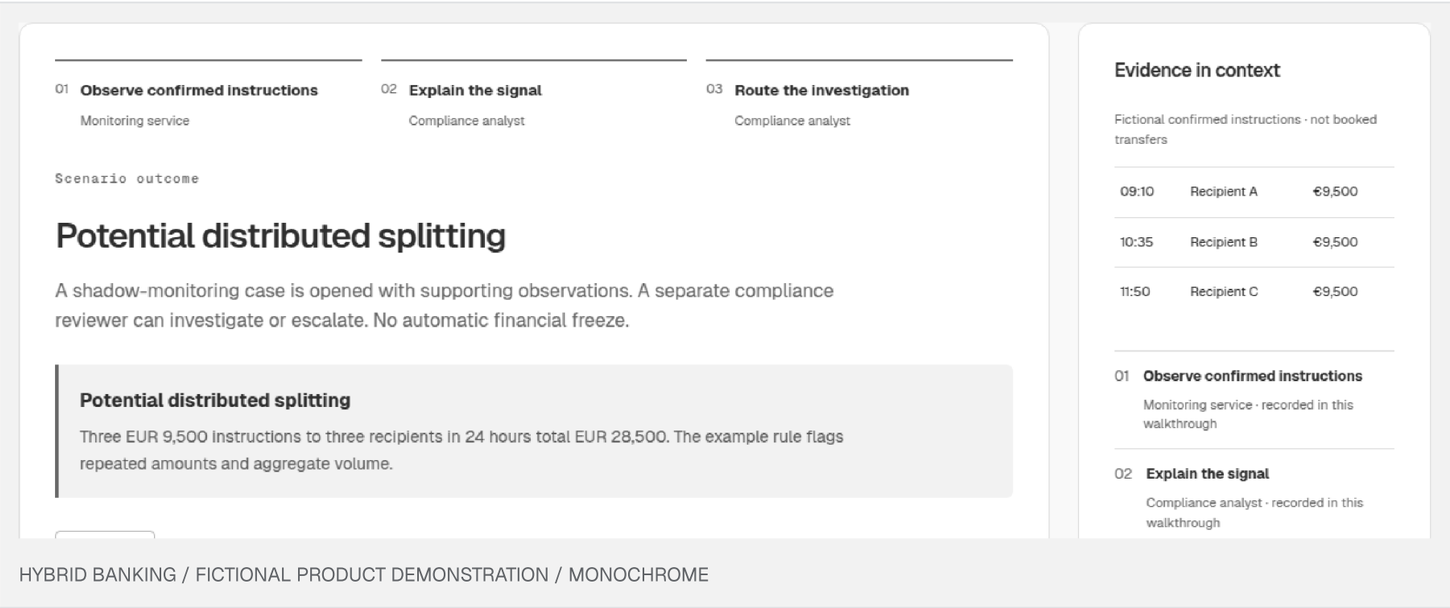
Surface configured indicators such as repeated smaller transfers, aggregated volume and rapid movement, with the rule and supporting events.

Investigate & decide

Assign an owner, inspect the client's risk factors, retain the rationale and reopen when new evidence warrants it.

Preserve the boundary

Shadow monitoring supports review; it is not an automatic freeze, accusation or regulatory filing.

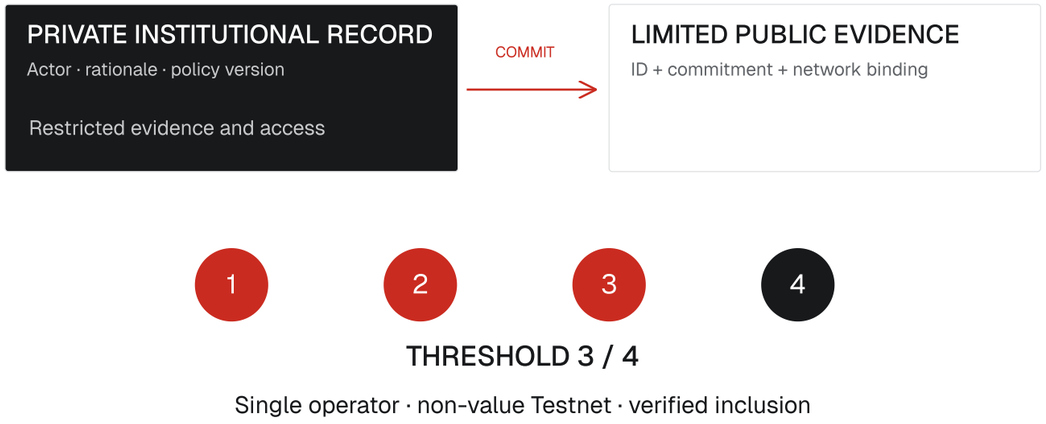


HYBRID BANKING / FICTIONAL PRODUCT DEMONSTRATION / MONOCHROME

A08 / PRIVATE AUDIT & PUBLIC PROOF

Keep the record private. Make its integrity verifiable.

Selected compliance-policy commitments can be checked without publishing the underlying client or policy detail.



Private record

Actor, reason, policy version and supporting evidence remain subject to restricted access and retention.

Publication

A bound publication ID and commitment enter the dedicated Testnet evidence service; intake alone is pending.

Verification

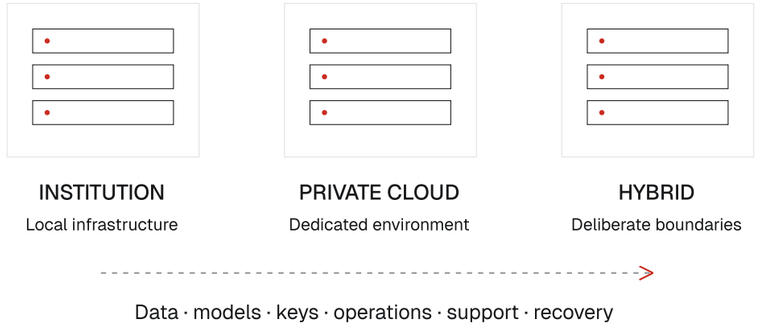
Check network and publication binding, signatures, quorum, Merkle inclusion and continuity against a trusted checkpoint.

3-of-4 validator signatures • single operator • non-value Testnet

A09 / DATA, MEMORY & DEPLOYMENT

Make context useful. Keep disclosure deliberate.

Choose where records and models run, what an agent may retrieve and how that access is revoked.



Institutional records

Define data residency, encryption, retention, audit access, recovery and support responsibilities.

Agent context

Scope what enters memory, who may retrieve it and for which purpose. Identity reuse does not automatically share bank data.

Model boundary

Evaluate local, private-cloud or hybrid inference against the approved data flow and model-governance requirements.

A10 / FEDERATION & PARTNER SERVICES

Connect businesses. Preserve their boundaries.

Use a common participation and permission model to make approved services easier to discover and integrate.

Service relationship

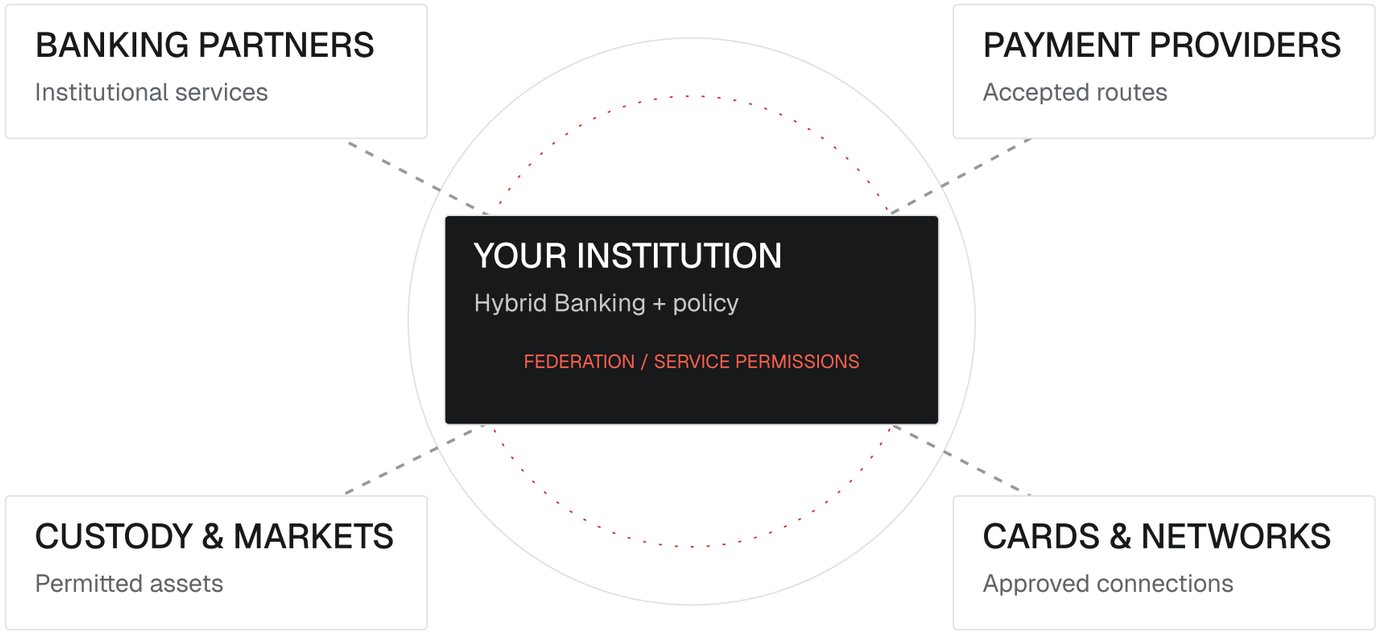
Agree the legal entity, jurisdiction, commercial terms and accountable operating party.

Technical relationship

Define authentication, operation scope, permitted data, asset/network coverage and failure handling.

Acceptance relationship

Test real counterparties, reconciliation, revocation, support escalation and exit before enabling the connection.



Partner categories replace unverified named-provider claims. Federation, DEX, exchange, custody and sister-network access each require specific permissions and proven connections.

A11 / INSTITUTIONAL ACCEPTANCE

Prove the workflow. Then expand the scope.

A release is accepted through business, control and operational evidence.

Functional proof

Complete onboarding and a payment instruction; reconcile authoritative records; distinguish rejected, pending and confirmed outcomes.

Control proof

Test unauthorized actors, stale sanctions evidence, blocked destinations, duplicate requests and invalid proof receipts.

Operational proof

Demonstrate outage recovery, restore, reconciliation, credential rotation, support ownership and export/exit.

Deliverable: an agreed capability register, acceptance record and narrowly defined activation decision.