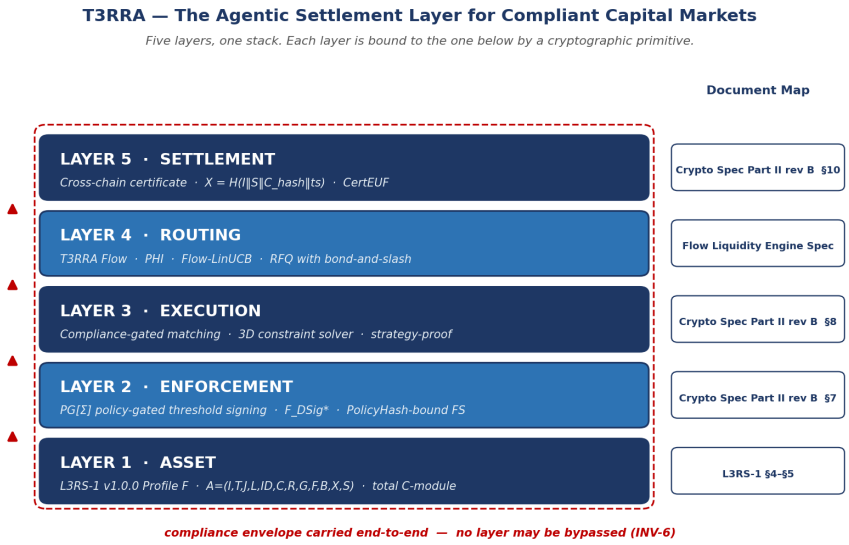
Architecture



T3RRA Architecture

Architecture v1.0 · April 2026

L3RS-1 v1.0.0 · Profile F (Full) Conformant

Zurab Ashvil · T3RRA Research

Contents

1. The One Sentence

> ***Reference convention.*** *Throughout this document,* ***§N*** *refers to* ***Section N of this Architecture paper****; clicking it jumps there. References prefixed with* ***L3RS-1*** *— for example,* L3RS-1 §15 *— refer to the corresponding section of the external L3RS-1 v1.0.0 standard.*

T3RRA is the cryptographic settlement layer for compliant capital markets.

Everything else in the T3RRA corpus — the L3RS-1 standard, the policy-gated threshold signing compiler PG[Σ], the compliance-gated matching engine, the Flow liquidity router, the cross-chain certificate — is one of five layers of that single sentence. This document is the master frame. It exists to make sure that no reader, whether a bank CTO, a cryptographer, or an investor, ever has to assemble the pieces themselves.

Read this document first. Read everything else as an expansion of one of its layers.

2. The Problem We Are the Only Ones Solving

Tokenization is solved. Compliance is solved. Liquidity is solved. Nobody has solved them on the same object at the same time, end to end, with cryptographic guarantees.

Tokenization platforms (Securitize, Tokeny, Polymath) issue compliant assets but stop at the wallet. Custodians and signers (Fireblocks, BitGo, Coinbase Custody) move assets but do not understand them. Liquidity routers (1inch, 0x, CoWSwap) find prices but treat compliance as someone else's problem. Bridges (LayerZero, Wormhole, CCIP) move bytes between chains but do not preserve regulatory state. The result is a tokenized RWA universe in which every individual link is plausible and the chain as a whole is uninvestable for a regulated balance sheet.

T3RRA closes the chain. It is the only system in which the same compliance object follows the asset through issuance, custody, signing, matching, routing, and cross-chain settlement, with each step cryptographically bound to the previous one. The compliance envelope is not enforced by policy and audit. It is enforced by the signature itself: if the compliance module rejects, the signing protocol aborts; if signing aborts, no transaction is broadcast; if no transaction is broadcast, no settlement occurs. Compliance is a precondition for cryptography, not a wrapper around it.

Compliance continuity is a cryptographic property in T3RRA, not an operational policy.

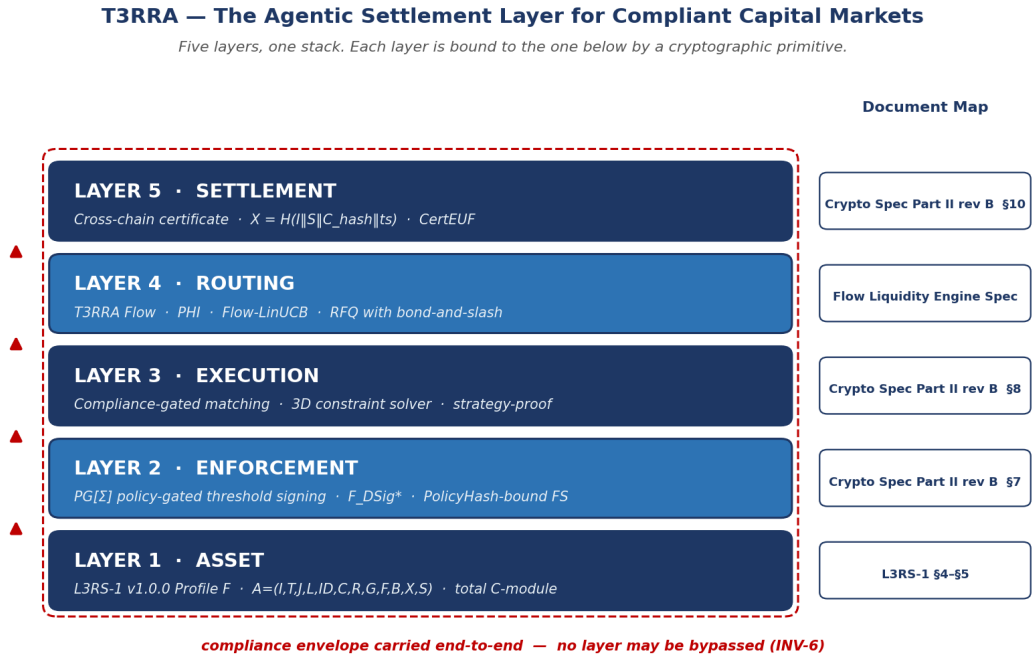


Figure 1. *The 5-layer T3RRA stack — Asset, Enforcement, Execution, Routing, Settlement.*

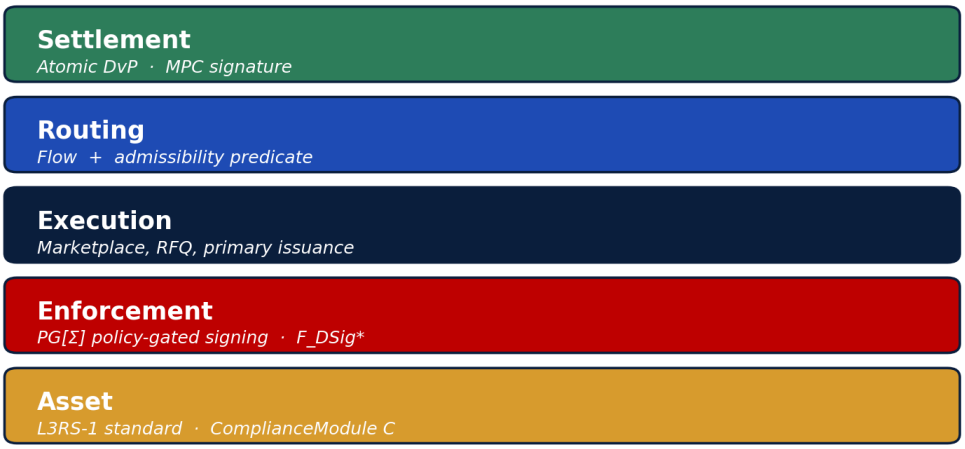


Figure 2. *Architecture-native view of the 5-layer T3RRA stack.*

3. The T3RRA Stack

T3RRA is one system in five layers. Every component, paper, and product in the corpus belongs to exactly one layer. There is no sixth layer, and there is no layer that belongs to two components.

3.1 The Stack Diagram

3.2 Layer-by-Layer Definition

Layer 1 — Asset. The asset itself, defined by L3RS-1, with its compliance module C as a total decision function. C is the source of truth for what is and is not allowed.

Layer 2 — Enforcement. PG[Σ] makes C a precondition for any signature. The compliance check is bound into the Fiat–Shamir challenge of the underlying threshold signature, so a signature on a non-compliant action is computationally infeasible — not policy-forbidden, but cryptographically out of reach.

Layer 3 — Execution. The compliance-gated matching engine fills orders only against counterparties whose envelope intersects the asset's. Strategy-proofness is a theorem, not a feature flag.

Layer 4 — Routing. T3RRA Flow extends compliance enforcement off-platform, into external liquidity sources. Flow does not 'find the best price' — it finds the best price in the admissible set, where admissibility is determined by Layer 1's compliance module evaluated along the route.

Layer 5 — Settlement. The L3RS-1 cross-chain certificate carries the compliance envelope across chains, with unforgeability reduced to the EUF-CMA security of the bridge committee's threshold signature. Settlement on a chain that cannot continue the certificate is not slower or harder; it is impossible.

3.3 The Reading Rule

Every existing T3RRA document maps to exactly one layer. There are no orphans and there are no overlaps.

Document	Layer	What It Specifies
L3RS-1 v1.0.0 Profile F	Layer 1	The asset object, the compliance module, the lifecycle
Crypto Spec Part II rev B §3–§6	Layer 2 (primitives)	DKG, threshold signing, refresh, identifiable abort
Crypto Spec Part II rev B §7	Layer 2 (compiler)	PG[Σ], F_DSig*, Theorems 7.1–7.3
Crypto Spec Part II rev B §8	Layer 3	Compliance-gated matching, strategy-proofness
Crypto Spec Part II rev B §9	Layer 4	Route admissibility predicate, tractability
Crypto Spec Part II rev B §10	Layer 5	Cross-chain certificate, CertEUF game
Flow Liquidity Engine Spec	Layer 4	PHI, Flow-LinUCB, RFQ, integration with Layer 2
T3RRA Whitepaper v3.1	All layers	Narrative integration of Layers 1–5

3.4 From Five Layers to Three Walls

The five-layer stack is the **technical** factoring of the system; it is how engineers, auditors, and regulators reason about what each component proves. The **commercial** factoring of the same system is the three-wall frame used in the T3RRA Investor Deck and in Whitepaper §2.0: Compliant Asset, Geographic Freedom, Roaming Liquidity. The two frames describe the same stack at different resolutions.

Commercial Wall	Technical Layers	What it delivers
Compliant Asset	Layer 1 (Asset) + Layer 2 (Enforcement)	L3RS-1 Profile F asset object with PG[Σ] binding the compliance predicate into the signature itself
Geographic Freedom	Layer 1 (LegalMirror) + jurisdiction mask J	SPV structuring, legal opinions, jurisdiction map, and the J-component of the route admissibility predicate
Roaming Liquidity	Layer 3 (Execution) + Layer 4 (Routing) + Layer 5 (Settlement)	Compliance-gated matching, the route admissibility predicate, and the cross-chain certificate

Figure 2. *The commercial three-wall frame mapped onto the technical five-layer stack. Every wall is fully cashed out in the layers it spans; removing any layer breaks the corresponding wall.*

The three-wall frame is the pitch; the five-layer stack is the proof. When reading this document alongside the Investor Deck or the Whitepaper executive summary, treat the three walls as the audience-facing projection of the layers described below.

4. Why Each Layer Has to Exist

This section answers the question every reviewer eventually asks: "why is there a bandit algorithm next to a UC functionality?" The answer is that they live on different layers and they are necessary for different reasons. Removing any one layer breaks the system.

4.1 Why Layer 1 (Asset) Has to Exist

Without a standardized asset object with a total compliance module, every other layer has to re-derive what "compliant" means from operational documentation. A regulator cannot audit operational documentation cryptographically. L3RS-1 makes the compliance envelope a piece of the asset's state, not a piece of the issuer's runbook. This is the precondition for every guarantee that follows.

4.2 Why Layer 2 (Enforcement) Has to Exist

Custody systems today enforce policy by refusing to sign. T3RRA enforces policy by binding the policy hash into the signature so that a signature on a non-compliant action is not produced — and could not be verified even if it were. This is the difference between "the wallet declined" and "no valid signature exists". Regulators care about the second statement and not the first.

4.3 Why Layer 3 (Execution) Has to Exist

A signed compliant transfer is not a market. Markets require matching, and matching requires a rule that decides which orders are eligible to fill against each other. A naive matching engine produces compliant trades only if every counterparty is compliant for every other counterparty, which is false the moment you cross a jurisdiction. The compliance-gated matching engine makes the cross-product check part of the match, with a strategy-proofness theorem so that no participant gains by lying about their tier.

4.4 Why Layer 4 (Routing) Has to Exist

Internal liquidity is never enough. The honest constraint is that institutional flow must reach external venues — Binance, Coinbase, OTC desks, AMM pools — without leaving the compliance envelope. Flow is not a smart-order router with a compliance flag. Flow is the projection of the compliance envelope onto the external venue graph. Every route Flow returns is, by construction, a route the L3RS-1 module C would have approved if it had been asked at every hop. The bandit is not the point; the bandit is the optimization that runs inside the admissible set.

Flow is not a router. Flow is the enforcement extension of compliance continuity into external liquidity.

4.5 Why Layer 5 (Settlement) Has to Exist

Cross-chain bridges today move bytes. They do not move regulatory state. A T-bill that is compliant on Ethereum is, after a generic bridge, an opaque token on the destination chain with no surviving evidence of its compliance posture. The L3RS-1 cross-chain certificate carries the compliance envelope across, and the CertEUF game proves that an adversary cannot forge a certificate without breaking the underlying threshold signature. This is what makes T3RRA assets multi-chain instead of merely multi-deployed.

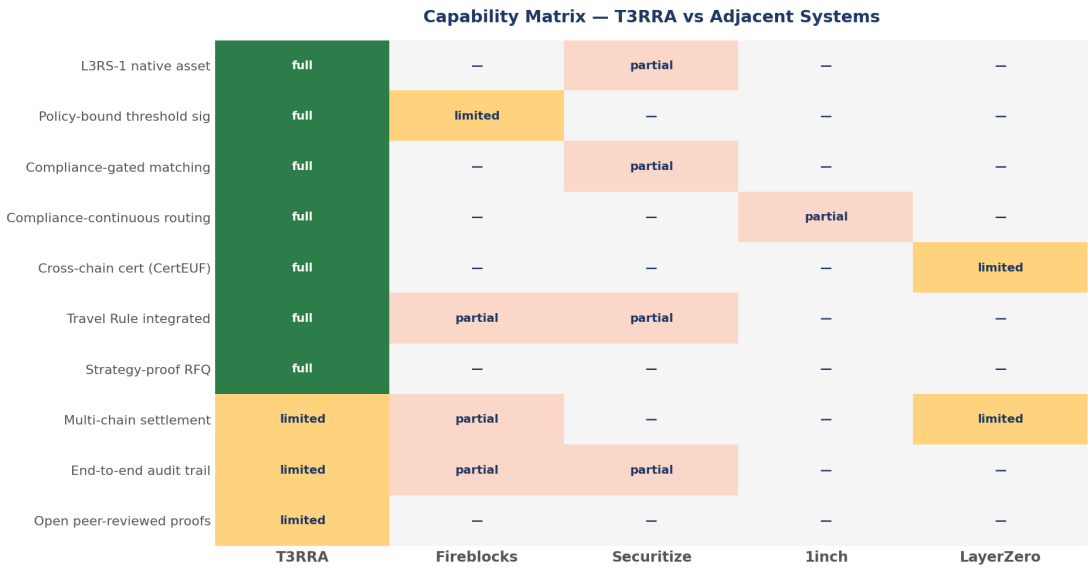


Figure 3. *Where T3RRA sits relative to existing systems.*

5. One Narrative, Three Audiences

The narrative does not change. The entry point does. The same one-sentence identity reaches each audience through a different layer, but the underlying story is identical.

5.1 For the Bank CTO

"This is brilliant, but I don't know where to start integrating."

Start at Layer 2. Replace your existing MPC custody with PG[Σ]. The integration surface is the same as Fireblocks or Coinbase Custody — sign endpoint in, signature out — except that the policy is bound into the signature itself, which collapses your compliance audit from a quarterly process into a per-signature property. Once Layer 2 is live, Layer 3 (matching) and Layer 4 (routing) plug in over your existing OMS without changing it. Layer 1 is the asset standard; you adopt it when you issue. Layer 5 is the bridge; you adopt it when you go multi-chain. There is a defined integration order and you do not have to swallow the whole system on day one.

5.2 For the Cryptographer

"Interesting protocol — but why is there a bandit algorithm here?"

Because the bandit lives on Layer 4 and the protocol lives on Layer 2. They are not adjacent in the same sense that ECDSA and AES are not adjacent: they live on different layers of the same system. The cryptography is in PG[Σ] (Layer 2), the certificate (Layer 5), and the strategy-proofness of the matching engine (Layer 3). The bandit is the optimization that runs inside the constraint set produced by Layers 1–3, and its only role is to make the system competitive on best execution conditional on admissibility. If you remove the bandit, T3RRA is still cryptographically sound; it is just operationally slower. If you remove PG[Σ], T3RRA is operationally fast and cryptographically meaningless. The two are decoupled by layer, and that decoupling is the whole point of the architecture.

5.3 For the Investor

"This is five companies in one."

It is five layers of one company. The five layers are not competitors; they are a stack. Stripe is also five things — issuing, acquiring, fraud, payouts, ledger — and nobody calls Stripe five companies, because the five things only make sense together. T3RRA is the same: each layer is necessary, none of the layers is sufficient on its own, and the moat is the integration. The TAM is the addressable market for compliant tokenized capital markets, which McKinsey, BCG, and Citi have independently sized at $4–16T by 2030. The wedge is Layer 2, because that is where the existing custodians are weakest and the regulatory pressure is strongest. The expansion path is Layers 3, 4, 5 in that order.

6. What This Document Changes

Nothing in the underlying technology changes. Every theorem, every protocol, every benchmark in the existing T3RRA corpus is preserved. What changes is the framing.

Before	After
Three documents with three centers of gravity	Five layers of one stack
Flow described as a smart-order router	Flow described as enforcement extension of compliance continuity
PG[Σ] described as a wallet feature	PG[Σ] described as Layer 2 of the settlement stack
L3RS-1 referenced as a standard T3RRA conforms to	L3RS-1 stated as Layer 1 of T3RRA itself
Compliance, cryptography, execution as parallel narratives	One narrative: cryptographic settlement for compliant capital markets
Multiple entry points with no order	Defined integration order: $2 \to 3 \to 4 \to 5$, with 1 as the asset prerequisite
The bandit looks adjacent to the cryptography	The bandit is on Layer 4; the cryptography is on Layers 2 and 5

The technology was already integrated. The story was not. This document makes the integration explicit so that no reader has to do the work of assembling it.

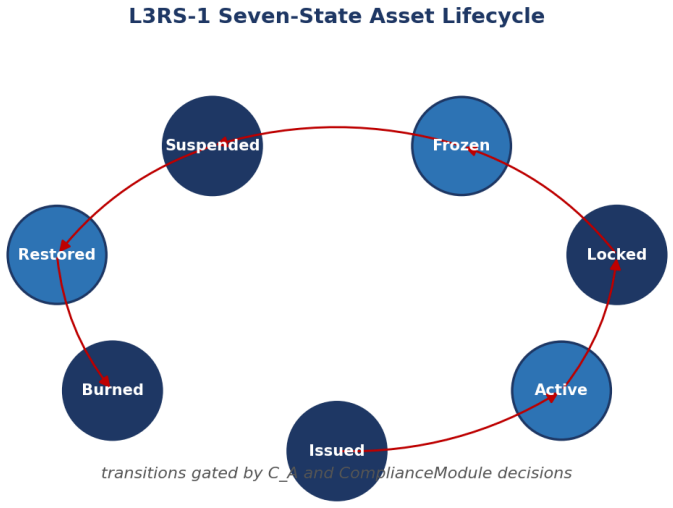


Figure 4. *L3RS-1 seven-state asset lifecycle that the invariants protect.*

7. System Invariants

The following six invariants hold across all five layers and define the T3RRA system as a whole. Any change to any layer must preserve all six. They are the architectural contract.

```
INV-1  Compliance Totality.
       For every asset A and every action α, the compliance module
       C_A is defined and returns either accept or reject. There is
       no undefined case, no exception, no human-in-the-loop fallback
       at the cryptographic layer.

INV-2  Signing-Compliance Binding.
       A valid signature on action α exists only if C_A(ctx(α)) = accept.
       Enforced by PG[Σ] (Layer 2). Any signature observed by any party
       on the network is, by the unforgeability of the underlying
       threshold scheme, evidence that compliance was satisfied at
       sign time.

INV-3  Match Admissibility.
       A fill is produced by the matching engine only if the cross-
       product compliance check between the two counterparties returns
       accept. Enforced at Layer 3.

INV-4  Route Admissibility.
       Every route returned by Flow is compliance-continuous in the
       sense of Definition 4.1 of the Flow Spec. Enforced at Layer 4,
       hard-filtered before any best-execution scoring runs.

INV-5  Certificate Continuity.
       For every cross-chain transfer, the destination chain receives
       a certificate X' = H(I‖S'‖C_hash‖ts') signed by the (5,9)
       bridge committee. No transfer completes without it.
       Enforced at Layer 5.

INV-6  No Layer Bypass.
       Layers may not be skipped. A signing call that bypasses Layer 2
       cannot produce a Layer 5 certificate; a Layer 5 certificate that
       does not chain to a Layer 2 signature is rejected by the bridge
       committee. The stack is not à la carte.
```

The invariants are checked statically at deployment (the build of any T3RRA component fails if its public surface area can violate one) and dynamically at runtime (each layer's interface refuses inputs that would cause an invariant to be violated downstream). This is what makes T3RRA an architecture rather than a bundle.

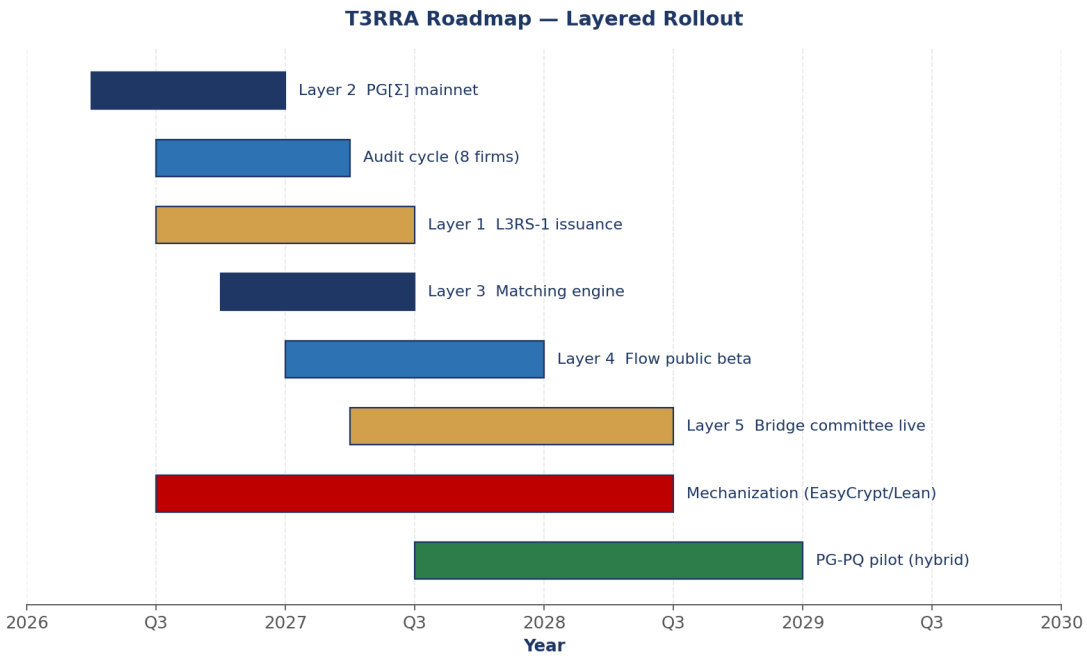


Figure 5. *Integration sequencing — Q2 2026 launch through 2028.*

8. The Integration Order

A bank, broker-dealer, or RWA issuer cannot deploy five layers in one quarter and should not be asked to. T3RRA is built so that the layers can be adopted in a defined order, with each layer producing standalone value before the next is added.

Phase	Layer Adopted	Standalone Value	Time to Value	Prerequisites
1	Layer 2 — PG[Σ]	Replace MPC custody; cryptographic compliance binding	6–10 weeks	Existing OMS, KMS
2	Layer 1 — L3RS-1	Issue first compliant asset; uniform compliance module	8–14 weeks	Issuance pipeline, legal opinion
3	Layer 3 — Matching	Internal venue with compliance-gated matching	10–14 weeks	Phases 1+2; counterparty panel
4	Layer 4 — Flow	External liquidity within compliance envelope	12–16 weeks	Phase 3; venue API access
5	Layer 5 — Certificate	Multi-chain settlement with regulatory continuity	16–24 weeks	Phases 1–4; bridge committee onboarding

Each phase is a contractually deliverable milestone with its own acceptance criteria. The integration is incremental, the value at each phase is real, and at no point does the customer hold a fraction of the system that does nothing on its own.

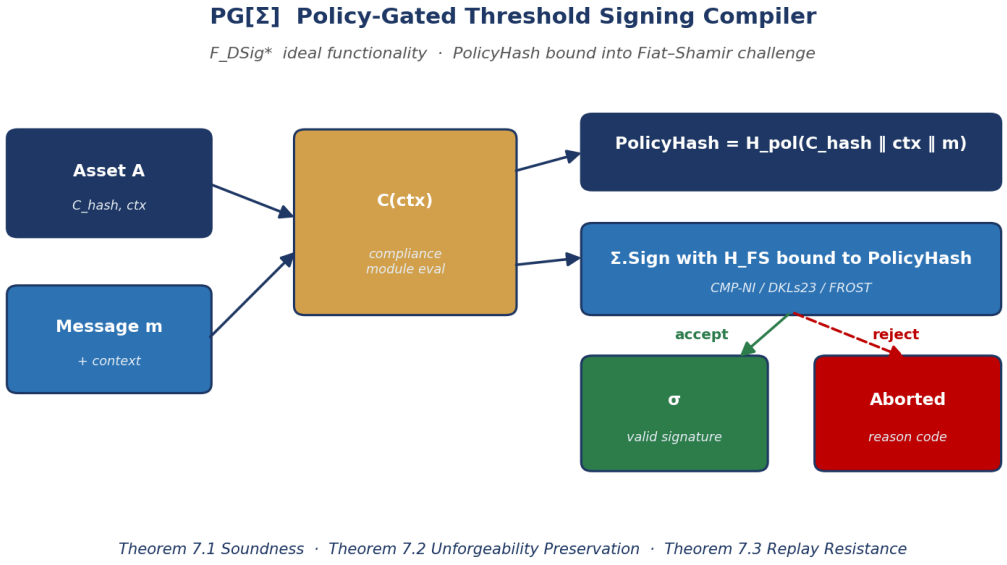


Figure 6. *PG[Σ] — the cryptographic core that the entire stack rests on.*

9. The Collapsed Pitch

This section is the document compressed to one page. Every external T3RRA communication — landing page, deck cover, investor memo, conference talk — should collapse to this and nothing else.

T3RRA is the cryptographic settlement layer for compliant capital markets.

It is one system in five layers: the asset (L3RS-1), the enforcement (PG[Σ] policy-gated threshold signing), the execution (compliance-gated matching), the routing (Flow), and the settlement (cross-chain certificate). Each layer is necessary, none is sufficient on its own, and together they make compliance a cryptographic property of the asset rather than an operational policy of the issuer.

Banks adopt T3RRA at Layer 2 to replace MPC custody with a system in which no signature ever exists for a non-compliant action. They expand to Layer 3 for an internal venue, to Layer 4 for external liquidity, and to Layer 5 for multi-chain settlement that preserves the regulatory envelope across bridges. The integration order is defined, the milestones are contractual, and at every phase the customer has something that works.

Cryptographers find a UC-style ideal functionality F_DSig*, a generic compiler PG[Σ] from any UC-secure threshold signature scheme, three theorems characterizing its security with concrete reduction tightness, a strategy-proofness theorem for the matching engine, a tractability theorem for the route predicate, and an unforgeability game for the cross-chain certificate. The bandit is on Layer 4 and is decoupled from the cryptography by design; removing it slows the system but does not weaken it.

Investors find a single five-layer stack that maps onto a $4–16T addressable market by 2030, with the wedge at Layer 2 (where the regulatory pressure is highest and the existing custodians are weakest) and a defined expansion path through Layers 3–5. There is no five-companies-in-one problem because there is no choice about which layer to pick: they are a stack, not a menu.

Compliance continuity is a cryptographic property. T3RRA is the only place that property exists end to end.

10. Where to Read Next

If you are…	Read this next	Then this
Bank CTO	Crypto Spec Part II rev B §7 (PG[Σ])	§8 of the Integration Order above
Cryptographer	Crypto Spec Part II rev B §7, §10	Flow Spec §11 (adversarial analysis)
Investor	T3RRA Whitepaper v3.1 (Exec Summary, Theses)	§9 above (Collapsed Pitch)
Regulator	T3RRA Whitepaper v3.1 §Compliance + L3RS-1	Crypto Spec Part II rev B §13 (Travel Rule)
Liquidity provider	Flow Spec §9 (RFQ, bond-and-slash)	Flow Spec §7 (Flow-LinUCB)
Bridge / cross-chain operator	Crypto Spec Part II rev B §10 (Cert + CertEUF)	§7 above (Invariant INV-5)

11. Disclaimer

This document is the architectural master frame for the T3RRA platform and supersedes any framing in earlier T3RRA documents that conflicts with it. It is a technical positioning document, not an offer or solicitation to buy or sell any security, digital asset, or financial instrument. The cryptographic and mechanism-design claims it references are paper-level: theorems are paper proofs, mechanization is in progress with explicit ETAs in Crypto Spec Part II rev B §15 and Flow Spec §14, and benchmarks in the referenced documents are targets, not measurements, pending public release of the reproducibility harness in Q3 2026. T3RRA Research welcomes corrections, adversarial review, and peer feedback.