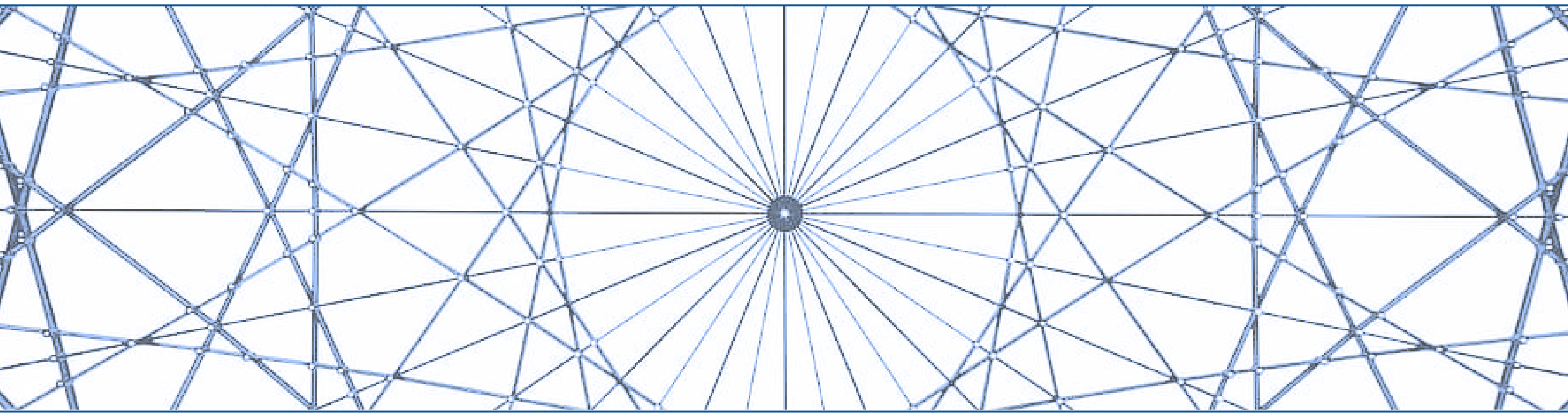


SETU – Semantic Electronic Trust Utility

A Semantic Network DPI with Accountable Agentic AI

Concept for a National DPI Connector for Reusable Verifiable Proofs and Policy-Bound Automated Agentic Actions

This paper, developed at CyStar @ IIT Madras, in collaboration with CDAC Mumbai, describes public-value outcomes, principles, governance arrangements, and standards-aligned building blocks. It intentionally avoids proprietary implementation detail.

Abstract

India's Digital Public Infrastructure (DPI) has demonstrated that shared national rails can unlock inclusion at population scale while enabling competitive private innovation. The next bottleneck is "repeated proof": citizens and businesses repeatedly submit documents, re-run KYC, and re-validate the same claims across agencies and enterprises. This duplication increases friction, cost, and fraud risk, while expanding the privacy attack surface through uncontrolled data replication.

Crucially, the current trajectory of digital expansion poses a latent risk: the emergence of disconnected 'trust silos.' As individual sectors—from education and agriculture to finance and logistics—independently adopt distributed ledger technologies and credentialing systems, we face the threat of a fragmented digital landscape. Without a unifying national interoperability layer, these vertical solutions will evolve into digital fiefdoms, forcing citizens to navigate a labyrinth of incompatible wallets and verification standards. This paper integrates the strategic rationale for a sovereign, converged infrastructure, demonstrating how SETU acts not just as a connector, but as the critical antidote to digital fragmentation, ensuring that India's digital economy remains seamless, inclusive, and citizen-centric.

SETU is proposed as a new **DPI that connects DPIs**: a neutral, consortium-run backbone for reusable, privacy-preserving proofs with uniform validity semantics and auditability. It is designed to complement India's existing DPI landscape—including **Aadhaar** (identity), **DigiLocker** (document issuance and retrieval), **UPI** (payments), and **Account Aggregator / DEPA** (consent-based data sharing)—and to interoperate with emerging sector rails such as the **Unified Energy Interface (UEI)**.

SETU is further positioned as a **Semantic DPI**: its infrastructure includes an intelligent programmable layer that enforces techno-legal policy and enables governed automation at scale. Secure Agentic AI is not an add-on; it is embedded from the foundation through a trust-first protocol that turns the system from a passive pipe into an active checkpoint**.** Secure Agentic AI binds every agent action to verified identity (Agent DID), explicit purpose, least-privilege tool access, and mandatory traceability—using semantic guardrails (including a machine-readable DPDP legal ontology) to intercept and block non-compliant requests.

SETU is designed to be **monopoly-resistant** by default through multi-operator operation, transparent accreditation, portability rules, and independent oversight ("conscience keepers"). Sustainability is achieved through transparent, minimal event-based charges settled via CBDC rails, enabling cost-neutral public-good operation without monetising personal data.

At the same time, public services are entering an era of **agentic interfaces**—where software agents complete workflows on a person's behalf. This raises a new "trust gap": without protocol-level guardrails, agents can over-collect data, be tricked through prompt-injection, execute unsafe tool calls, and leave weak evidence trails when something goes wrong.

Table of Contents

1. Context: why a new DPI layer is emerging

India's DPI trajectory suggests a repeatable pattern: when the country standardises a national bottleneck into interoperable rails, the ecosystem composes new services faster than any single institution could build alone. The next bottleneck is not connectivity or payments; it is **repeated proof**—the constant re-submission of identity, eligibility, credential, registration, and compliance artefacts across everyday journeys.

This duplication manifests as citizen burden (time, travel, delay), institutional burden (cost, risk, compliance overhead), and systemic vulnerability (forgery, synthetic identities, deepfakes, and inconsistent checks). More recently, the risk profile has shifted sharply: large-scale data breaches are being aggregated into dark-web pools, mined and recombined for impersonation, and weaponised through AI-enabled fraud—deepfakes, voice cloning, synthetic identities, and automated social engineering. As personal data is replicated across many downstream systems with uneven safeguards, the attack surface expands and the cost of failure rises.

Furthermore, this fragmentation has profound implications for. If digital trust infrastructures are built solely on disparate, private, or non-interoperable rails, the state risks losing the ability to guarantee a uniform standard of privacy, security and user experience for its citizens.

There is an emerging paradigm shift in terms of 4 aspects:.

- Firstly, the need of the hour is a transition from 'digitized verticals' to a '**sovereign horizontal**'—a shared, secure, and programmable substrate. As India accelerates toward a $5 trillion economy, the next wave of innovation is being driven by sector-specific digital adoption. However, in the absence of a unified national framework, these efforts are rapidly crystallizing into isolated verticals. The profound risk of data sovereignty and resilience due to fragmentation. We are witnessing a proliferation of standalone ledger initiatives and proprietary credentialing systems that, while effective individually, lack the semantic glue to talk to one another.
    - This inevitable 'silo-isation' creates a heavy integration tax on innovation, where startups and developers must rebuild trust anchors for every new sector they enter, rather than leveraging a common national trust fabric.
    - By standardizing how value and verified claims are exchanged across these verticals, we move from merely having digital systems to possessing a coherent Digital Public Infrastructure that is greater than the sum of its parts.
- Secondly, DPDP-aligned, **user-empowered sharing** is becoming the default expectation: individuals and enterprises should be able to authorise what is shared, for what purpose, and for how long—rather than having their data replicated and retained across countless systems. Trust and compliance move from "paper consent" to enforceable, purpose-bound access with accountability.
- Thirdly, **privacy preservation** is increasingly treated as a mandatory design discipline, not a best effort. Services should request only what they need, and users should be able to satisfy those requests through partial disclosures or derived proofs—for example, proving eligibility, identity assurance level, or a threshold (such

as a minimum GPA) without revealing or fully revealing the underlying document. This reduces exposure, limits misuse, and still enables high-assurance verification at scale.

- A fourth force is accelerating at the same time: **agentic automation**. Citizens and enterprises increasingly interact through assistants that fill forms, assemble applications, submit requests, and coordinate follow-ups. Without protocol-level guardrails, this becomes “automation without accountability”: agents can request too much data, execute unsafe actions, and create disputes with weak evidence.

SETU reframes the national problem in one move: rather than copying personal data everywhere, the country can allow **trust to travel** through **minimal, verifiable proofs** that are revocable, auditable, and interoperable—and can allow **actions to travel** through a governed agent protocol (Bharat MCP) that turns trust into safe execution.

In other words: SETU is the missing layer that makes interoperability meaningful, and makes automation legitimate.

2. Proposition: what SETU is (and is not)

2.1 What SETU is not

SETU is not a new centralised personal-data database. It is not a replacement for existing DPIs or sector systems. It is not a single application. It is a full-fledged national infrastructure: shared rails, governance, standards-aligned interfaces, and a trust-first agent protocol that governs automation. It is like UPI for eligibility and proofs.

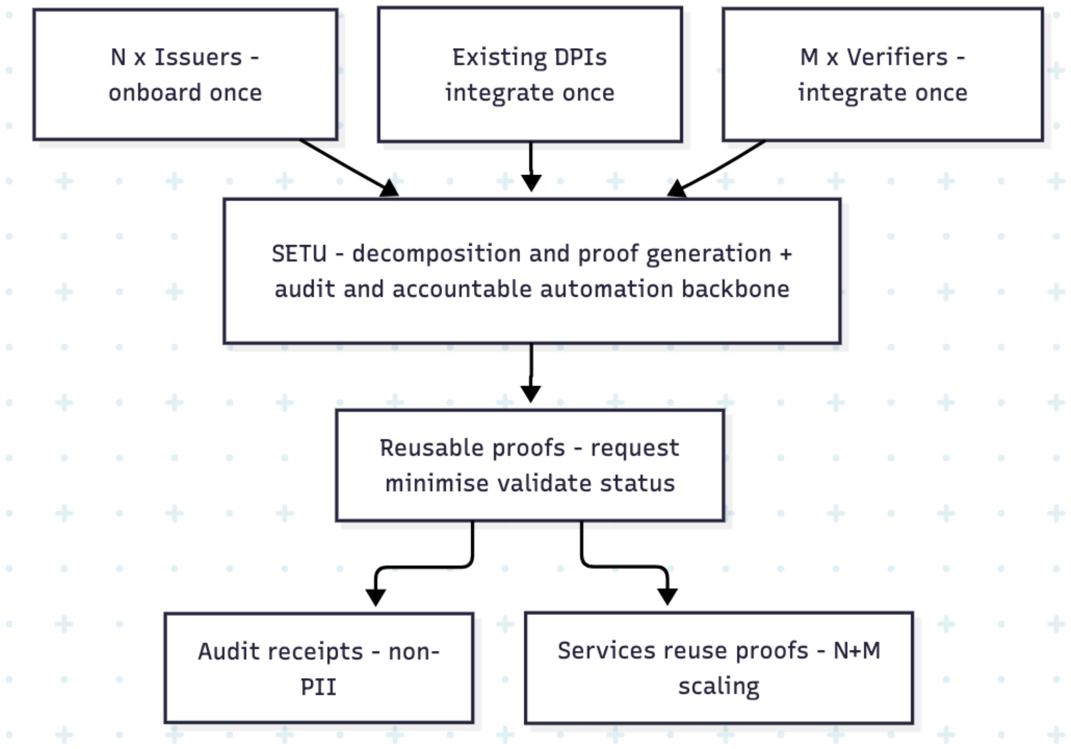
2.2 SETU as a "DPI that connects DPIs"

SETU is a **connector DPI**. It complements existing DPIs and domain systems-of-record by standardising how proofs are issued, requested, minimised, validated, revoked/superseded, and audited across ecosystems.

SETU's design goal is composability: issuers onboard once; verifiers integrate once; services reuse proofs rather than rebuilding verification pipelines. This shifts national integration from an **N×M** pattern to a more scalable **N+M** pattern.

Existing DPI-issued documents and credentials—such as identity and tax artefacts, registrations, licences, academic records and ancillary credentials (upskilling /micro-learning credentials, sporting achievements, musical/art achievements and qualifications, and records for various things like blood donation, yoga, health, charity work etc.)—can be used within SETU as **authoritative source attestations**.

Figure 1 — Scaling enabled through standards-based interfaces


N x Issuers - onboard once
Existing DPIs integrate once
M x Verifiers - integrate once
SETU - decomposition and proof generation + audit and accountable automation backbone
Reusable proofs - request minimise validate status
Audit receipts - non-PII
Services reuse proofs - N+M scaling

Currently, systems like Account Aggregator and DigiLocker do not have the ability to store this variety of data nor enable selective disclosure or derived proofs from the said data, although that is subject to change..

SETU is designed to decompose these document-based proofs into granular, reusable claims and generate derived proofs that enable the disclosure of only what is necessary for a specific purpose, rather than requiring the full document to be shared. For example, a marksheet can yield a verifiable GPA claim, or a simple "meets minimum GPA threshold" predicate proof, without exposing the marksheet or subject-level marks.

By mapping documents to standardised claims and enforcing purpose-bound, time-bound minimisation through the semantic policy layer, SETU enables rapid adoption through efficient reuse of existing DPI channels—while materially reducing friction, verification cost, and unnecessary data exposure.

2.3 SETU as a Proof + Action backbone (embedded agentic execution)

A reusable proof layer is necessary—but no longer sufficient. Most real services follow the same shape: **request minimal proof → verify + live status → decide → act → record outcome**. SETU therefore treats action as a first-class citizen.

Bharat MCP is embedded within SETU as the native mechanism for **accountable agentic execution**. It ensures that actions (submissions, approvals, disbursements, renewals, acknowledgements) can be triggered by tool-using agents only when they are justified by valid proofs, constrained by purpose and minimisation, and recorded as tamper-evident traces. This transforms the system from a passive connectivity layer into an **active checkpoint**—where compliance is enforced at runtime, not promised in documents.

2.4 SETU is not an unregulated AI layer

SETU does not "sprinkle AI" on top of existing systems. Agentic AI is bounded by protocol-level identity, guardrails, and traceability. The system's default posture is that **agents are purpose-specific, accountable participants**, not opaque bots.

At a national scale, the issue is not whether AI is powerful; it is whether AI is legitimate—aligned to lawful purpose, constrained by minimisation, and contestable when errors occur. SETU therefore treats automation as governed infrastructure: any agent-mediated request or action must be explainable in terms of purpose, supported by valid proofs, and attributable to a responsible entity.

This preserves innovation while preventing "black-box government." Models and applications can evolve competitively at the edge, but they operate through SETU's shared trust rails so that citizens receive the benefits of automation without losing privacy, agency, or accountability.

3. Design principles that SETU makes enforceable

SETU adopts DPI principles as explicit commitments and governance obligations. These are not slogans; they are enforced by architecture and operating rules.

1. Citizen agency and privacy (including DPDP)

The system must minimise disclosure, preserve user control, and encode consent and purpose limitation into the rails. When data is used or shared either by an AI agent or human user, they must be done only on a **time-bound, purpose-restricted, consent-driven** basis—never uncontrolled.

2. Interoperability and modularity

The system must be composed of open, modular building blocks that prevent lock-in and enable competitive innovation. This includes interoperability not only for credentials and registries, but also for **agent tool descriptions and invocation contracts**.

3. Techno-legal regulation

Policy is not documentation; it is machine-enforceable guardrails: **DPDP-aligned** purpose limitation, minimisation rules, accreditation constraints, and auditable receipts. Guardrails must intercept both proof requests and tool calls.

4. Monopoly resistance

The system must resist capture by any single operator or market actor through multi-operator design, portability rules, and transparent governance. This applies equally to the agent ecosystem: no single "agent platform" should become the gatekeeper for public workflows.

5. Non-weaponisation

The system must reduce misuse risk by limiting retained data, enforcing oversight, and creating accountability mechanisms that constrain coercion and exclusion. Mandatory traces and sanctionable identities are core to this safety posture.

6. Operational security governance

SETU must enable clean onboarding, scoped permissioning, and safe offboarding for all entities (issuers, verifiers, wallets, agents, and operators), so trust can be granted, constrained, suspended, or withdrawn consistently.

4. SETU as a Semantic DPI: the intelligent programmable layer

A **Semantic DPI** is a DPI whose core infrastructure includes a programmable layer that can interpret intent, enforce rules, and orchestrate journeys safely at scale.

In SETU, the semantic layer is not a convenience feature; it is the **compliance brain** of the network. It couples shared meaning (schemas and vocabularies) with computable policy and runtime enforcement—so the country can scale interoperability without scaling risk.

SETU's semantic layer combines three capabilities, so that interoperability is not merely "data exchange" but **meaningful, policy-bound reuse**:

1. **Shared meaning:** credential schemas, vocabularies, and proof types are versioned and discoverable so "what a credential means" is consistent across India.
2. **Computable policy:** policies (purpose limitation, minimisation constraints, step-up requirements, retention and audit rules) are expressed in machine-readable forms and enforced at runtime. This includes semantic models and **DPDP-aligned legal ontology patterns** that let the guardrails evaluate whether a request's intent is legitimate.
3. **Programmable journeys:** services compose proofs into journeys (education to employment, farmer to finance, grants/subsidy/entitlement delivery, health insurance/continuity) while producing auditable evidence.

This semantic layer is the bridge between trust and action: it ensures that decisions and automation remain anchored to verifiable proofs and legitimate purpose—and that agentic execution is governed rather than improvised.

5. Citizen empowerment: selective disclosure and self-sovereign vaults

SETU changes a basic interaction rule: **a person should not have to share a full document when a service needs one fact**.

Selective disclosure enables presentations such as "over 18", "resident of Gujarat state", or "eligible for benefit Y" without exposing full underlying data. Business credentials can similarly prove compliance states (e.g., "GST active", "MSME category") without revealing full filings.

SETU supports vault-based user control: proofs are held in a wallet/vault under user agency. Where relevant, SETU can reuse familiar citizen touchpoints (for example, **DigiLocker-linked issuance** for official credentials, and consent patterns inspired by **Account Aggregator / DEPA**) while still preserving the principle that the user controls disclosure.

Crucially, this empowerment extends to agentic journeys: a citizen may authorise a verified agent to act as a **legal-style representative** for a specific purpose and timeframe (e.g., apply, renew, schedule, claim). Under Bharat MCP, that authorisation is explicit, minimised, and traceable—so the user is empowered by automation without being exposed by automation.

Requests are purpose-bound and time-bound, the user can consent or refuse, and the system generates consent and verification receipts that support accountability.

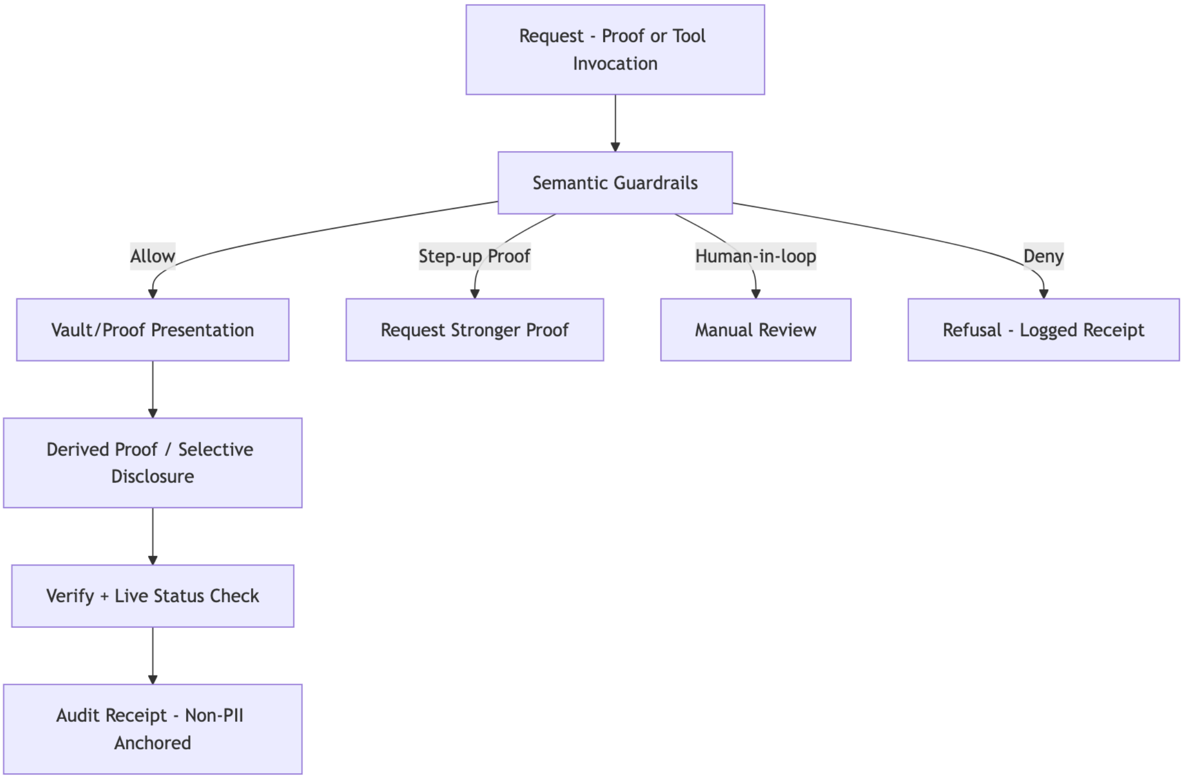
Safety discipline: personal data remains in authoritative systems-of-record and user vaults. SETU anchors only non-PII integrity artefacts (commitments/hashes, timestamps, schema/policy references, accreditation and status semantics).

6. Execution layer: proof-bound automation

SETU is designed for an "**assisted-by-default**" future, where citizens and enterprises increasingly interact through agents that complete journeys end-to-end. Without protocol-level guardrails, this becomes automation without accountability: agents can over-collect data, invoke unsafe tools, and leave weak evidence trails. SETU therefore embeds **Bharat MCP** as part of its core execution layer—so every automated action is justified by proofs, constrained by policy, and recorded as a trace.

Bharat MCP is a **sovereign, trust-first protocol layer** for agentic systems. Its function is to transform "connectivity" into **governed participation**: connect verified entity A to verified entity B, under participant consent, for explicitly defined purpose, with enforceable constraints.

Figure 2 — Semantic DPI guardrails (policy + ontology enforcement)



At a high level, Bharat MCP inside SETU consists of three coupled layers:

1. **Protocol transport:** exchanges are not raw data calls; they are **signed proofs** with mutual authentication via DIDs.

2. **Guardrail layer (compliance brain):** intercepts every agent request and tool invocation, evaluating intent against semantic policy (including DPDP-aligned rules) and enforcing minimisation.
3. **Agent governance layer (orchestrator):** manages agent identity and lifecycle, including **Agent DIDs**, reputation/assurance scoring, and risk-tiered permissions (e.g., low-trust agents limited to read-only; higher-assurance agents permitted for write/execute tasks).

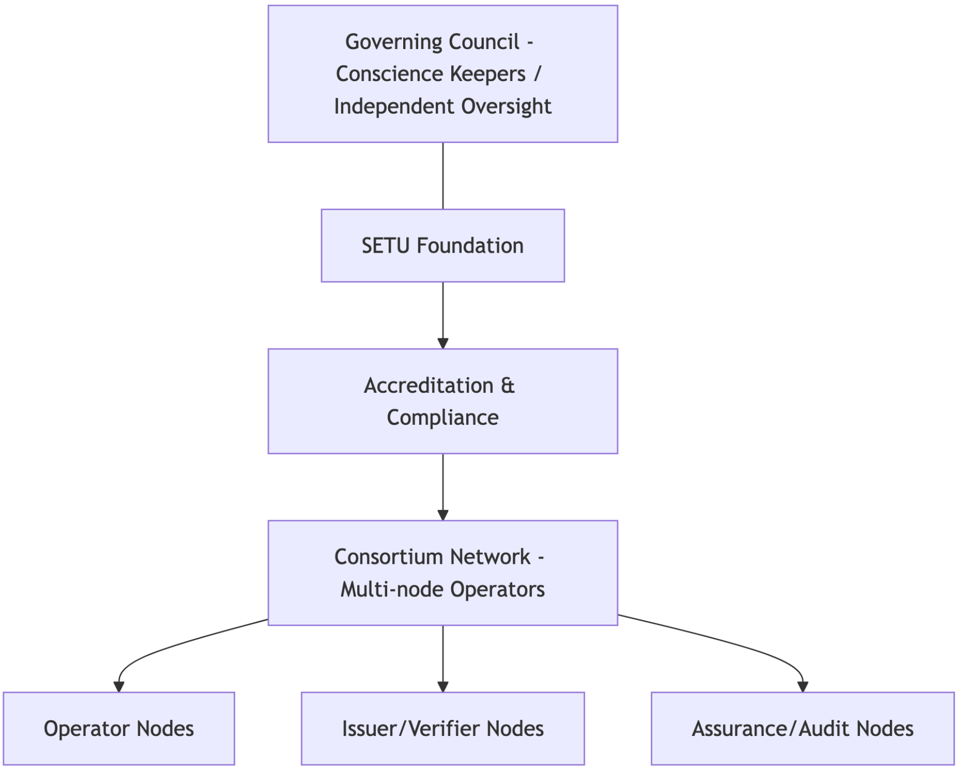
This turns SETU from a passive pipe into an **active checkpoint**: agents do not directly access user data sources or tools; they operate through interception, policy evaluation, and mandatory traceability.

In SETU, Bharat MCP is embedded from the foundation as the native mechanism for safe, auditable automation at national scale—turning SETU into a **Proof + Action backbone** where proofs are reusable and actions are executed safely because policy and auditability are built into the rails.

7. Monopoly resistance as a system property

Interoperability is also market design. SETU's monopoly-resistance is achieved through architecture and governance that reduce switching costs and prevent operator capture.

Figure 3 — Consortium governance and monopoly resistance


Governing Council - Conscience Keepers / Independent Oversight
SETU Foundation
Accreditation & Compliance
Consortium Network - Multi-node Operators
Operator Nodes
Issuer/Verifier Nodes
Assurance/Audit Nodes

SETU's design includes multi-operator, multi-node operation; transparent accreditation criteria; portability across wallet providers and service operators; separation of powers (foundation stewardship vs competitive applications); and independent oversight ("conscience keepers") to strengthen legitimacy and transparency.

8. Secure Access Governance Principles

SETU supports graceful onboarding, permissioning, and exit for every participating entity—issuers, verifiers, wallet/vault providers, agents, and node operators—so that trust can be granted, constrained, suspended, or withdrawn cleanly and consistently. Participation is not permanent: credentials, keys, authorisations, and operating rights are revocable and time-bound by default, with controlled pathways for renewal, remediation, and re-entry.

Offboarding is safe and accountable: when an entity is deactivated—whether by self-request, policy violation, security compromise, regulatory direction, or judicial order—the network will prevent further actions, preserve non-PII audit evidence, and ensure portability so citizens and relying parties are not stranded.

In summary, SETU participation involves the following:

- **KYX**: Standard onboarding processes for Know your Agent (KYA), Know your Business (KYB), Know your Customer (KYC), Know your Govt. Department (KYD)
- **Tiered Permissioning:** based on accreditation + assurance tiering; least-privilege permissions; time-boxed scopes (purpose, domain, tool access).
- **Due process for ecosystem safety:** event-driven processes for breach, fraud, repeated non-compliance, unsafe agent behaviour, or compromised keys → immediate containment + defined appeal/remediation.
- **Order-driven controls:** system enforces lawful directions (regulator/court) through **policy switches** and status semantics, without spreading personal data.
- **Portability on exit:** if a wallet/provider/operator is removed, users can migrate vault custody and verifiers can re-route, avoiding lock-in
- **Data minimisation on deactivation:** disable future access, rotate/retire keys, revoke authorisations; retain only the minimum audit artefacts needed for accountability.

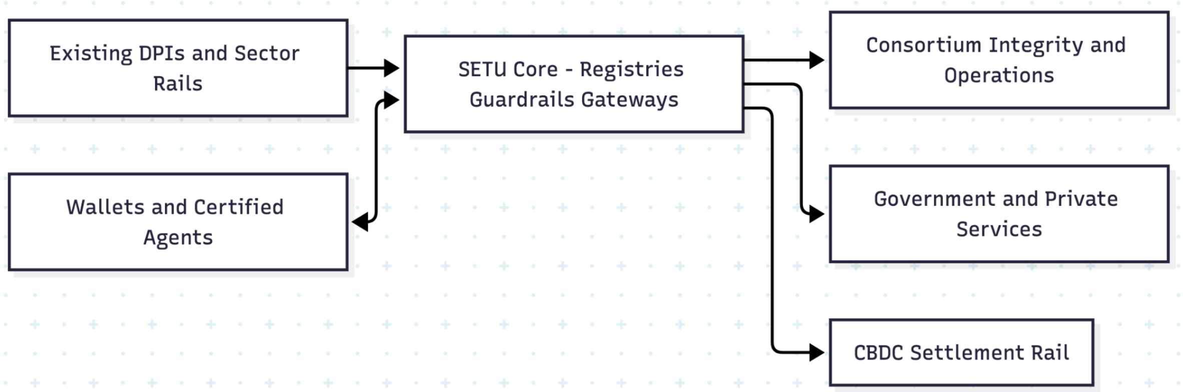
9. Reference architecture

SETU is best understood as a standards-aligned stack with these components;

1. **Consortium integrity layer:** permissioned ledger or equivalent tamper-evident log anchoring non-PII receipts and governance artefacts.
2. **DPI connectors:** integration patterns that allow SETU to interoperate cleanly with Aadhaar, DigiLocker, UPI, Account Aggregator/DEPA, and sector interfaces such as UEI—so SETU connects DPIs without replacing them.

3. **National registries:** DID/key registry, schema registry, policy registry, accreditation registry, status registry (revocation/supersession/dispute semantics), and (where policy requires) **agent trust/assurance registries**.
4. **Wallet/vault layer:** citizen and business custody, consent UX, derived proof generation, assisted-channel support.
5. **Verification gateways:** APIs/webhooks for request templates, verification, status checks, and receipt generation.
6. **Semantic guardrails:** policy enforcement and legal ontology alignment at runtime (purpose, minimisation, step-up, retention, dispute).
7. **Embedded agent protocol (Bharat MCP):**
    a. **Transport:** DID-authenticated exchange of signed proofs.
    b. **Guardrails:** interception of proof requests and tool calls using semantic policy.
    c. **Governance:** agent identity (Agent DID), assurance scoring, risk-tier permissions, tool registry and certification, mandatory traces.
8. **Settlement rail:** CBDC-based event settlement and transparent accounting.

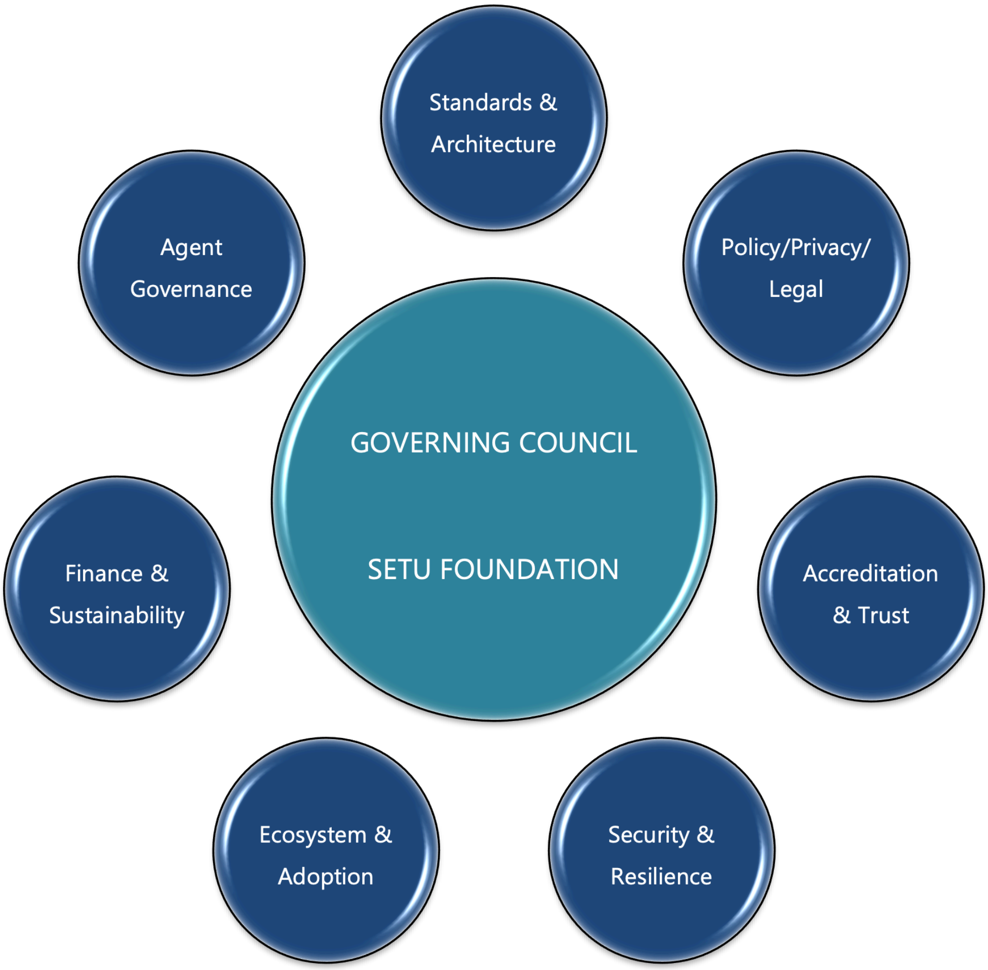
Figure 4 — High level reference architecture


Existing DPIs and Sector Rails
Wallets and Certified Agents
SETU Core - Registries Guardrails Gateways
Consortium Integrity and Operations
Government and Private Services
CBDC Settlement Rail

10. Operating model: Foundation stewardship + public–private consortium

A credible national backbone must be neutral, resilient, and continuously improved. SETU must be stewarded by a **SETU Foundation** and operated by a **public-private consortium**.

Figure 5: Typical governance bodies for SETU



The Foundation must provide standardisation, accreditation rules, compliance frameworks, ecosystem enablement, and transparency reporting. The consortium must operate the multi-node network under licensing arrangements and published obligations.

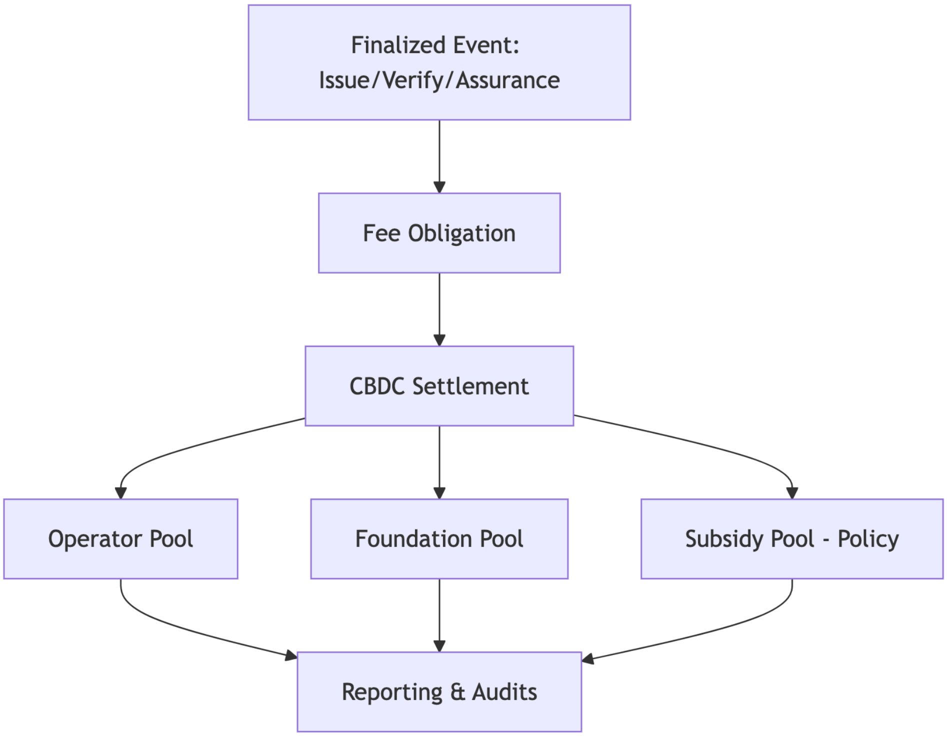
11. Sustainability: CBDC event settlement for a cost-neutral public good

SETU should remain a cost-neutral public good by relying on transparent, minimal event-based charges rather than monetising personal data.

CBDC settlement enables programmable micro-fees for issuance and verification events, accreditation and renewal, and high-assurance verification where needed, alongside policy-driven exemptions and subsidy pools for equity.

The operating rule is simple: **fees fund operations; trust remains a public good.**

Figure 6 — CBDC cost-neutral settlement



12. The Future Citizen Experience

The Fork in the Road: Fragmented Silos vs. Unified Agency

To understand the urgency of the SETU proposal, we must project the current trajectory of digital development five years into the future. We stand at a fork in the road regarding the Citizen Experience (CX) in India.

The Default Trajectory: The "Siloed" Citizen

If the current trend of fragmented, sector-specific blockchain and credential implementations continues unchecked, the digital experience for the average Indian citizen in 2030 will be defined by **high friction and cognitive overload**.

In this scenario, a citizen seeking a home loan would face a disjointed ordeal:

- **Multiple Wallets:** They would need a specific 'Land Record Wallet' to prove ownership, a separate 'University Wallet' to prove education for employment eligibility, and a 'Bank Wallet' for financial history.
- **Repeated Proofs:** Because the 'Land' ledger does not interoperate with the 'Bank' system, the citizen must repeatedly download, notarize, and re-upload documents.

- **The "Agentic Gap":** AI Agents, however smart, would be rendered useless. An AI assistant trying to "Auto-fill Loan Application" would fail because it cannot securely bridge the air-gapped data silos of the local municipality, the university, and the credit bureau.
- **Result:** The citizen is reduced to a "manual router" of data, constantly ferrying proofs between incompatible digital bureaucracies. The promise of a seamless digital economy is lost to "App Fatigue" and "Credential Chaos."

The Proposed Trajectory: The "Sovereign" Citizen

By implementing the unified architecture proposed in this paper (aligned with the Bharat Trust Backbone ethos), we shift the paradigm from **application-centric** to **citizen-centric**.

In this unified future:

- **Singular Agency:** The citizen utilizes a single, interoperable interface (or Agent) that can resolve credentials across any sector—whether it is a Green Building rating from the municipality, a Skill Certificate from the Skill Council, or a GST return from the tax authority.
- **Semantic Interoperability:** A bank's AI agent can instantly read and verify a "Green Building Certificate" issued by a municipal node because both share a common semantic schema and trust root. The loan interest rate is automatically lowered based on this verified data, with zero manual paperwork.
- **Portable Trust:** Trust becomes portable. A street vendor's repayment history recorded on a supply-chain ledger becomes instantly usable evidence for a working capital loan on a separate financial ledger.
- **Result:** The citizen moves from being a data-carrier to a data-commander. Technology fades into the background, and the focus shifts to value creation and ease of living.

The cost of fragmentation results in inefficiencies on the citizen's time and agency, as well as systemic technology debt. Consolidating these rails now is not merely an IT upgrade—it is a prerequisite for a frictionless, AI-ready society.

13. Early domains where SETU creates disproportionate value

SETU creates disproportionate value in high-volume journeys where verification is repeated, where fraud and compliance costs are material, and where institutions today solve the same trust problem in parallel. The common pattern is consistent across sectors: **request minimal proof** → **verify + live status** → **decide** → **act** → **produce receipts**. With SETU, this pattern becomes reusable, DPDP-aligned, and automation-ready.

Below are illustrative sector workflows (non-exhaustive) that show how proof reuse and policy-bound automation translate into measurable efficiency.

13.1 Education → employment and skilling mobility

SETU enables institutions to issue portable credentials to a learner vault, and employers to verify only what they need (e.g., qualification or threshold) without collecting full documents. Live validity checks reduce fraud and repeated manual verification. Agent-assisted onboarding can then proceed with clear accountability.

13.2 Financial services onboarding

SETU reduces repeated KYC by allowing regulated proofs to be reused across institutions with purpose-bound sharing. Banks and fintechs request only minimal verification outcomes rather than full document sets. This improves privacy, speeds onboarding, and lowers compliance cost while maintaining auditability.

13.3 Entitlement delivery and welfare programs

SETU supports eligibility proofs that can be verified instantly and kept current through status updates, reducing duplicate submissions and leakage. Services can confirm eligibility with minimal disclosure instead of collecting sensitive dossiers. Outcomes remain traceable for audit and grievance handling.

13.4 Health journeys - privacy-preserving continuity

SETU allows patients to share limited, purpose-specific proofs needed for care or claims without exposing full medical records. This reduces form-filling and repeated documentation while improving privacy. Validity and consent are enforced consistently, supporting safer coordination across providers.

13.5 Energy and utilities - UEI-linked service portability

SETU enables common utility proofs (connection, meter, eligibility) to be reused across service providers without repeated paperwork. Requests are minimised and verifiable, reducing activation delays and disputes. This improves interoperability across the energy ecosystem while keeping users in control.

13.6 Agriculture, supply chains, and farmer-to-finance

SETU helps farmers and enterprises reuse verified proofs for finance, insurance, and program access without repeated verification cycles. Services can rely on minimal, purpose-bound attestations rather than full document bundles. This shortens turnaround times and reduces fraud exposure.

13.7 Trade, logistics, and customs documentation

SETU supports reusable proofs across handoffs so parties can verify compliance states without resubmitting the same documents repeatedly. Consistent validity semantics reduce delays and disputes. The result is faster processing and clearer accountability across the chain.

14. Case Study: Solving the “Settlement Trust Gap”

Atomic Property Transfers via SETU & Bharat Trust Backbone

The Problem:

The Two-Week Trust Void In India’s current real estate landscape, the transfer of funds (payment) and the transfer of title (mutation/registration) are asynchronous. A buyer often pays days or weeks before the official record reflects their ownership. This "Trust Gap" can be exploited by fraudsters for double-selling and this creates high systemic risk for lenders, requiring expensive, manual title searches and physical escrow.

The Solution:

SETU Semantic Settlement: By utilizing SETU as a semantic connector between the **Land Registry (L2)** and the **Banking System (L2)**, anchored on the **Bharat Trust Backbone (L1)**, India can achieve "Atomic Settlement"—the simultaneous exchange of value for ownership.

The Workflow:

1. **Unified Workspace:** A buyer, seller, and their respective banks enter a "SETU Transaction Workspace."
2. **Verifiable Proofs:** The seller’s bank issues a **Lien-Release VC**, and the Registrar issues a **Ready-to-Transfer VC**. These are not PDFs but machine-readable proofs that SETU understands.
3. **The Atomic Swap:** A SETU Smart Contract acts as a digital escrow. It holds the buyer’s funds (via CBDC or locked UPI) and the digital title in a state of "pending."
4. **Instant Execution:** Once all policy conditions are met (Taxes paid VC, KYC verified VC), the contract executes:
    - **Funds** move to the seller’s account instantly.
    - **The Title** is updated on the Bharat Trust Backbone.
    - **Mutation VCs** are issued to the buyer’s wallet and the lender.
5. **Agentic AI:** A horizontal ecosystem of AI Agents for all sorts of functions and utilities such as compliance, analysis, reporting, communications, scheduling etc.

Strategic Benefit:

Preventing "Digital Fiefdoms" Without SETU, a citizen buying property in a different state would face a "Silo Tax"—having to navigate different state-run apps and bank-specific portals that do not speak the same language. SETU ensures that a "Property Proof" from Karnataka is mathematically and legally valid to a Bank in Maharashtra, creating a **Single National Market for Real Estate**.

Metric	Current State	SETU + Bharat Trust Backbone
Settlement Time	15–45 Days	Minutes (Atomic)
Verification	Manual/Physical Search	Automated/Verifiable Proof

Fraud Risk	High (Double Selling)	Zero (Blockchain Lock)
Cost	High (Intermediary Fees)	Low (DPI Rail Cost)

15. Implementation pathway

SETU should be introduced in a DPI-typical sequence.

- First, establish governance: priority proof types, schema and policy primitives, accreditation criteria, and selective disclosure profiles.
- Second, run limited pilots that demonstrate DPDP-aligned behaviour and audit-ready receipts.
- Third, scale by connecting existing DPIs and sector networks through stable gateways and onboarding patterns.
- Fourth, expand embedded agentic journeys under Bharat MCP governance for high-volume workflows.

16. Conclusion

This proposed new national network is an emerging Semantic layer that connects DPIs and upgrades the national experience from digitising forms to digitising **trust and accountable automation**; from manual engagement through multiple portals to a hyper productive singular wallet experience with assisted and purpose-bound sharing of specific data.

It is citizen-centric through selective disclosure and vault-based control, resilient through consortium multi-nodal operation, and credible through monopoly-resistant governance. By embedding Bharat MCP from the foundation, SETU treats AI not as an unregulated overlay but as a governed public utility—faster because it is accountable.

This is a timely call to government departments and the private sector to champion this mission, signal national intent, work with this national architecture and rally India Inc. to shape a secure, trusted, interoperable future that catalyses innovation across all sectors of India's economy.

Endnotes

1. Observer Research Foundation and partners, *Decoding Digital Public Infrastructure: Scripting Inclusive Digital Futures*.
2. Government of India, *Digital Personal Data Protection Act, 2023 (DPDP Act)*.
3. UIDAI, Aadhaar ecosystem references.
4. DigiLocker ecosystem references.
5. NPCI, UPI ecosystem references.
6. Account Aggregator / DEPA ecosystem references.
7. Unified Energy Interface (UEI) ecosystem references.
8. W3C, *Decentralized Identifiers (DID) Core*.
9. W3C, *Verifiable Credentials Data Model*.
10. NIST, *Digital Identity Guidelines (SP 800-63 series)*.
11. BIS and central bank publications on CBDCs, digital identity, and resilience of public financial infrastructure.
12. ONDC/OCEN and other sector DPI references.
13. Bharat GenAI and API SETU program references.

Acknowledgements

- Mr. Deepak Norman - IIT Madras
- Mr. Kamlesh Nagware- IIT Madras
- Prof. Dr. John Augustine - IIT Madras
- Mr. Rammohan Srinivasan - IIT Madras
- Dr. Padmaja Joshi - CDAC Mumbai