FRANKBANKER RESEARCH

India's DPI Stack

A Banker's Guide

India's Digital Public Infrastructure mapped for financial services practitioners.

FrankBanker Research • April 2026

Section 1: Introduction to India's DPI Stack

Digital Public Infrastructure, or DPI, refers to the shared digital systems that make large-scale, interoperable service delivery possible across institutions. In India's case, these systems have digitised identity verification, document exchange, payment settlement, digital execution, and data sharing across banking, government and beyond, without the need for each participant to build bilateral connections with every other participant.

DPI is infrastructure in the same sense that roads, telecom networks, or power grids are infrastructure: shared, standardised, and meant for others to build on. During India's G20 presidency in 2023, DPI was described as a set of secure and interoperable digital systems, built on open standards, that can deliver public and private services at population scale. The World Bank has similarly described it as an approach to digitalisation built around foundational digital building blocks designed for public benefit.

India's contribution in this context lies not only in scale, but in the fact that it is multi-layered system, addressing a variety of population scale use cases. Banks, NBFCs, insurers, payment companies, government agencies, and fintechs increasingly operate on a common digital base. For example in Banking, what appears as a single customer flow like onboarding, verification, underwriting, execution, disbursement, repayment, often rests on multiple underlying DPI elements working together.

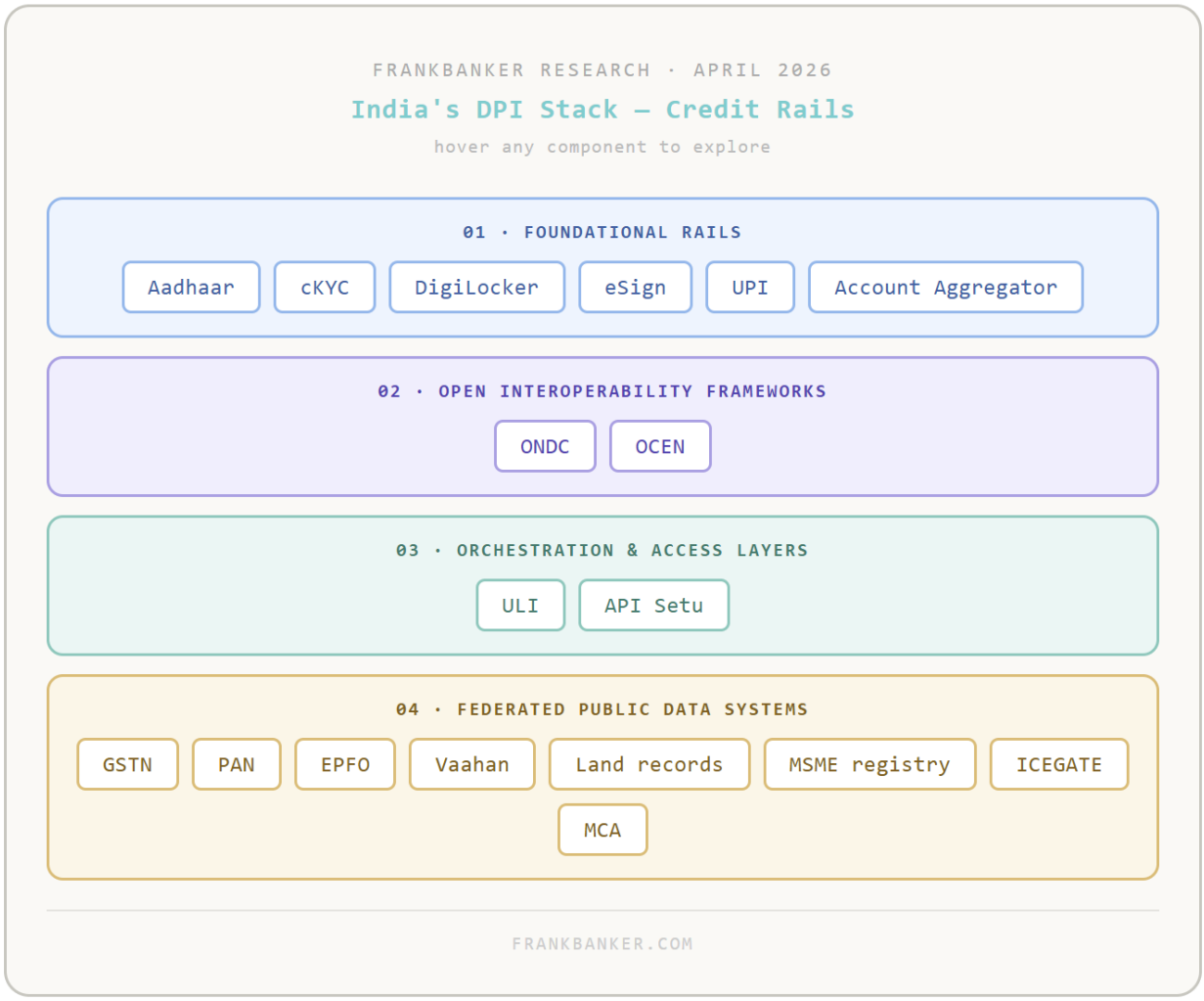
While the different components of DPI have emerged for different purposes and across different phases, we at FrankBanker read this as a DPI stack or a layered system that works in tandem. To ensure a more holistic view, we have expanded on what constitutes this stack with platforms, protocols or registries and divided these into 4 major layers from a practitioner's perspective.

The first is foundational rails: the systems that perform a core shared function such as identity, document exchange, digital execution, payments, or consented financial data sharing. In this guide, that includes Aadhaar, cKYC, DigiLocker, eSign, UPI, and the Account Aggregator framework.

The second is open interoperability frameworks: protocol-led systems that allow multiple market participants to transact or originate through common standards rather than proprietary bilateral integrations. ONDC and OCEN are the principal examples covered here.

The third is orchestration and access layers: systems that aggregate, standardise, or simplify access to multiple underlying services and data sources. ULI and API Setu are best understood in this way.

The fourth is federated public data systems and registries: government-held records that are increasingly becoming accessible through digital interfaces and are therefore becoming important parts of underwriting, onboarding, and verification workflows. Access to APIs of GSTN, income-tax records, EPFO, and Vaahan and even the land records, have increasingly become crucial part of lending workflows. While the literature on DPI often misses these, FrankBanker team believes these are important rails that enable deeper digitisation in the banking context.



Section 2: DPI Platforms in Detail

This section profiles each component covered in the guide- its background, the use case for financial services practitioners, and the technology in brief. The components are grouped into four buckets**: foundational rails**, **open interoperability frameworks**, **orchestration / access layers**, and **federated public data systems / registries**.

2.1 Foundational Rails

2.1.1 Aadhaar (Identity and Authentication)

Aadhaar is a 12-digit individual identification number issued by UIDAI to any usual resident of India, backed by biometric and demographic data, under the Aadhaar Act 2016. By March 2026, 144 crore numbers had been generated and 2,707 crore authentication transactions completed in FY 2024-25.[11]

Each Aadhaar number is linked to biometric data consisting of ten fingerprints, two iris scans, and a photograph. Additionally, demographic data including name, date of birth, address, and gender is recorded. Authentication is available in two modes: biometric (fingerprint or iris match against UIDAI's Central Identity Data Repository) and OTP-based. In both modes, raw biometric data never leaves UIDAI's infrastructure. External systems receive a digitally signed cryptographic response, not the underlying data.

Access to Aadhaar authentication APIs requires licensing. Regulated entities like Banks, NBFCs, must obtain **Authentication User Agency (AUA)** or **KYC User Agency (KUA)** status from UIDAI.

In banking, Aadhaar enables paperless KYC. eKYC via OTP delivers a digitally signed XML packet with the individual's name, address, date of birth, and photograph, constituting full KYC under RBI's KYC Master Direction. For a bank opening a savings account or a NBFC onboarding a borrower, this replaces document collection, physical verification, and manual data entry with a sub-30-second API call. For business correspondents serving rural borrowers, biometric eKYC at a fingerprint device enables onboarding where mobile connectivity is poor. For institutions processing high transaction volumes, the Virtual ID allows identity authentication without storing the Aadhaar number itself.[12]

Four modes of Aadhaar-based verification are available in practice:

eKYC via OTP: UIDAI returns a digitally signed XML packet with demographic data and photograph. This constitutes full KYC under RBI Master Directions and can be used for digital account opening, loan origination, and investor onboarding.

eKYC via Biometric: Fingerprint or iris capture at a UIDAI-compliant device. Used for assisted onboarding through business correspondents, particularly where the individual does not have a mobile number linked to Aadhaar.

Offline KYC: A digitally signed XML file with masked Aadhaar (last four digits only), downloaded from UIDAI and shared by the individual. No real-time UIDAI connection required; applicable in low-connectivity settings.

Virtual ID (VID): A 16-digit temporary token that resolves to the Aadhaar number only within UIDAI's systems. External entities receive eKYC data without ever knowing the underlying Aadhaar number. Entities should store the VID or a derived token, not the Aadhaar number itself.

Technology: Aadhaar

Core concept: authentication returns YES or NO. Biometric data never leaves UIDAI's CIDR. Templates are encrypted with AES-256 symmetric keys, themselves wrapped with 2048-bit RSA public keys; all key operations occur within HSMs (Hardware Security Modules — tamper-resistant physical devices that generate and store cryptographic keys).

De-duplication: UIDAI runs three independent ABIS (Automatic Biometric Identification System) solutions simultaneously across 1.4 billion records. This is the first multi-ABIS implementation at this scale and helps maintain de-duplication accuracy and reduce vendor dependency.

How to connect: AUA/KUA licence from UIDAI; Aadhaar Data Vault-compliant storage for derived tokens; NPCI SDK for biometric capture devices at branch or BC points.

Note: The Supreme Court's 2018 judgment in Puttaswamy v. Union of India established that mandatory Aadhaar authentication by private entities for commercial services is not permissible. Aadhaar-based verification in the private sector is voluntary, and every digital onboarding flow must maintain a working alternative path such as V-CIP, PAN with photograph, or DigiLocker document pull.[13]

2.1.2 cKYC — Central KYC Registry (Identity Repository)

The Central KYC Registry (cKYC) is a centralised repository that stores KYC records and enables their reuse across all regulated financial entities, operated by CERSAI under a cross-regulatory mandate from RBI, SEBI, IRDAI, and PFRDA.[17]

When any regulated entity completes KYC for a customer, that record is uploaded to CERSAI with a 14-digit cKYC number assigned. Subsequent regulated entities must search the cKYC registry before creating a new customer record. For a customer who already has a mutual fund relationship, opening a loan account should not require re-submission of PAN card, address proof, and photograph. If a valid record exists, it can be downloaded rather than documents recollected.

Technology: cKYC

Protocol: standardised XML schema for upload and download via CERSAI portal APIs; search by PAN, Aadhaar, or mobile number.

Limitation: no auto-update mechanism when customer details change; records can become stale between KYC renewal cycles.

How to connect: CERSAI API registration; XML schema compliance; search cKYC before creating new customer records as a regulatory obligation.

*Note: CERSAI stands for **Central Registry of Securitisation Asset Reconstruction and Security Interest of India,** a government-mandated central registry that records security interests created on property by secured creditors, primarily to prevent fraud through multiple financing of the same asset.*

2.1.3 DigiLocker (Trusted Documents and Credentials)

DigiLocker is a government-operated secure cloud platform for the storage, sharing, and verification of authentic digital documents, operated by MeitY under the Digital India programme and the IT Act 2000. By March 2026, it had 67.63 crore registered users and over 950 crore documents issued by government departments.[14]

DigiLocker has two document types with fundamentally different trust weights.

Issuer-pull documents are placed directly by government departments: driving licences from the transport authority, PAN cards from NSDL/UTI, income tax returns from ITD, vehicle registration certificates from MoRTH. These carry the issuing authority's PKI digital signature, verifiable against the CCA (Controller of Certifying Authorities) trust chain, and are the legal equivalent of the original document.[15]

Self-uploaded documents are scanned copies placed by the individual. They carry no issuer verification and should be treated with the same scepticism as a physical document handed across a counter. Treating all DigiLocker documents as equivalent is an underwriting risk. The

distinction is visible in document metadata: a signed document has a verifiable certificate chain; an unsigned upload does not.

In lending, DigiLocker issuer-pull is used to verify vehicle ownership for asset-backed products, income tax return data, driving licence for credit assessment of transport operators, and vehicle registration for commercial vehicle finance. The pull is consent-based. The borrower authenticates with their Aadhaar-linked credential and the lender's system receives time-limited API access to specific document types.

Technology: DigiLocker

Core concept: issuer-pull documents carry the CCA-issued PKI signature of the issuing authority. Signature verification against the CCA trust chain confirms authenticity and integrity.

Protocol: OAuth 2.0 for authorisation; REST APIs over TLS for document pull via verified URIs; time-limited access tokens prevent persistent access.

Data residency: DigiLocker infrastructure is hosted on NIC Government Cloud within India.

How to connect: DigiLocker API key from MeitY; OAuth 2.0 integration; CCA trust chain access for signature verification.

Note: CCA is the Controller of Certifying Authorities, established under the IT Act 2000. It is the root trust authority for digital signatures in India, operating under MeitY.

2.1.4 eSign (Digital Execution and Consent)

eSign is an Aadhaar-based electronic signature service that enables digital execution of documents using Aadhaar OTP, without a physical cryptographic token or smart card. It is legally valid under IT Act Section 5 and the Electronic Signature Rules 2015. RBI's Digital Lending Directions 2025 require IT Act-compliant digital signatures for loan agreement execution; OTP-only acceptance and click-wrap agreements are no longer sufficient.[16]

A document is sent to a CCA-empanelled eSign Service Provider. The signatory receives an OTP on their Aadhaar-linked mobile. On OTP validation, the provider generates a PKI-based digital signature from its HSM and attaches it to the document. The signed document is returned within seconds and is independently verifiable against the CCA trust chain by any party. eSign is used for loan agreements, insurance proposals, property documents, and mandate registration.

eSign is an element of the consent and controls layer rather than merely a document tool. It is where consent becomes enforceable: a signed loan agreement, a registered mandate, an insurance proposal. For a NBFC disbursing personal loans digitally, eSign means the loan agreement can be signed by a borrower in Bidar or Barabanki without a branch visit and with a legally binding signature that will hold in any court. The distinction from click-wrap matters operationally. Click-wrap is a digital acceptance mechanism where a user clicks 'I Agree' without identity verification. While a click-wrap record shows that a button was pressed, an eSign record shows that a specific individual, verified by Aadhaar OTP at a specific time, authorised a specific document.

Technology: eSign

Core concept: Aadhaar OTP authentication triggers a PKI signature from a CCA-empanelled provider's HSM. The signature is legally equivalent to a handwritten signature and independently verifiable against the CCA trust chain.

How to connect: engagement with a CCA-empanelled eSign Service Provider; API integration with that provider.

Note: Hardware Security Module (HSM) is a tamper-resistant physical device that generates, stores, and manages cryptographic keys in a secure environment that software cannot access directly.

2.1.5 Account Aggregator Framework (Consent and Data Sharing)

The Account Aggregator (AA) framework is a consent-based financial data sharing architecture where RBI-licensed NBFC-AAs act as data-blind intermediaries between financial data sources (**Financial Information Providers, FIPs**) and data consumers (**Financial Information Users, FIUs**). Established by the RBI Master Direction of 2016 (updated 2021). By December 2025, 126 financial institutions were live as both FIP and FIU, 17 AAs were licensed, and 2.61 billion financial accounts were enabled for data sharing.[9, 20]

The framework has three roles. The FIP is a regulated entity holding financial data: a bank, an NBFC, an insurer, GSTN. The FIU is a regulated entity requesting data: a lender assessing creditworthiness, an insurer underwriting a policy, or an investment platform assessing suitability. The AA is the RBI-licensed intermediary that manages consent and carries encrypted data but cannot read it. An October 2023 RBI circular introduced a bilateral data commons requirement: any entity that pulls data as an FIU must also contribute its own data as a FIP.[9, 21]

The **consent artefact** is the architectural heart of the system. It is a digitally signed JSON document specifying exactly what data is shared, from which source, for what purpose, covering what time period, at what frequency, and expiring when. The FIP verifies the consent artefact before releasing any data. The individual can view, pause, or revoke consent at any time through their AA app.

Through AA framework, for example, a MSME borrower applying for a business loan can authorise the lender to pull 24 months of bank statement data from three current accounts, 36 months of GST return data from GSTN, and ITR data from ITD, in a single consent flow that takes under two minutes, without physically producing a single document. The lender receives verified, machine-readable data directly from the source institution, not a scanned statement that could be altered.

Technology: Account Aggregator

Core concept: the AA is data-blind. The FIP encrypts data using the FIU's public key before transmission. The AA carries an encrypted payload it cannot read; only the FIU can decrypt. Consent is a signed artefact with a non-repudiable audit trail, not a checkbox.

Protocol: all integrations follow ReBIT technical specifications at api.rebit.org.in — covering consent management APIs, data fetch APIs, encryption standards (ECDH key exchange, AES-256 payload encryption), and audit logging requirements.

Data flow: FIU sends consent request to AA → AA presents to individual → individual approves → AA sends signed artefact to FIP → FIP encrypts data with FIU's public key → AA forwards encrypted payload → FIU decrypts.

How to connect: regulated entity status (RBI/SEBI/IRDAI/PFRDA); ReBIT-compliant FIP/FIU module or empanelled TSP; Sahamati certification; consent management system.

2.1.6 UPI (Payments)

UPI (Unified Payments Interface) is a real-time interoperable payment protocol developed by NPCI under RBI mandate. It enables instant bank-to-bank transfers through Virtual Payment Addresses (VPA), without requiring account numbers or IFSC codes. By January 2026, it was processing 21.70 billion transactions worth Rs. 28.33 lakh crore monthly across 691 participating banks — approximately 49 percent of global real-time payment transaction volume.[18]

UPI operates on a four-party model: the user's **Payment Service Provider (PSP) app**, the **remitter bank**, the **NPCI Central Switch**, and the **beneficiary bank**. PSP apps provide the user interface but do not hold funds or execute settlement; they are front-ends on the shared rail. The user's MPIN is encrypted at the device by the NPCI SDK before transmission and never transits the network in plaintext.

UPI transaction history, accessed through the AA framework with explicit user consent, can be a significant alternative credit signal for individuals without formal income documentation. A 12-month UPI flow can demonstrate cash inflow consistency and payment behaviour where no payslip or income tax return exists.

More recently, use has expanded to UPI Mandate , an autopay feature that enables recurring debit authorisations. A user authorises a standing instruction specifying amount, frequency, and tenure once, at the point of agreement execution. Subsequent debits occur automatically without further user action. As of December 2024, RBI extended the scope of pre-sanctioned credit lines on UPI to Small Finance Banks, enabling credit drawdown via UPI transactions[19] . In lending, UPI Mandate can replace NACH mandates for urban digital borrowers: registration is faster, confirmation is real-time, and the mandate framework integrates directly into digital loan origination workflows.

Technology: UPI and UPI Mandate

Core concept: the four-party model separates user experience (PSP app) from payment infrastructure (NPCI switch) and funds (banks). No PSP holds funds. The NPCI switch routes, validates, and manages net settlement via RTGS.

Security: MPIN encrypted at device via NPCI SDK before any transmission; PKI authentication for all API calls; multi-zone replication supports 24×7 availability.

UPI Mandate: a standing debit instruction registered via the NPCI switch with specified amount, frequency, and tenure. Mandate failure rates should be monitored in real time — a failed debit may

not automatically notify the collecting institution; failure patterns are a leading indicator of borrower financial stress.

How to connect: NPCI member bank relationship or PSP sponsor bank arrangement; PCI-DSS audit; NPCI SDK for MPIN capture.

*Note: **NACH (National Automated Clearing House)** is an NPCI-operated platform that enables bulk, electronic bank transactions such as recurring debit mandates, salary payments, subsidies, EMIs, and utility collections.*

2.2 Open Protocol Frameworks

2.2.1 Open Network for Digital Commerce (ONDC)

ONDC is an open network protocol that decentralises digital commerce. Any buyer app, seller app, payment service provider, or logistics provider conforming to the Beckn Protocol can transact across the network regardless of which platform the counterparty uses. As of early 2026, ONDC operates across 630+ cities with 1.16 lakh active retail sellers and approximately 154 million cumulative orders processed. It is governed by DPIIT.[23]

ONDC is a protocol, not a marketplace. There is no central platform through which all transactions flow. Buyer apps and seller apps communicate directly via the Beckn standard; the ONDC Network acts as registry and governance body, not as a transaction processor. A seller listed on one ONDC-compliant app is discoverable through any other.

The significance for lenders lies in the data ONDC generates and bridges loan originators and Banks. A merchant transacting on the network creates a verifiable record of order volumes, GMV, buyer diversity, fulfilment rates, and supplier relationships. These records are independently verifiable on-network rather than self-reported. If the merchant or its customer requires loans, the same can be routed to the banks. Triangulated with AA-sourced bank statements and GSTN return data, ONDC commerce data creates a multi-source view of a merchant's business or customer transactions. Banks themselves can participate as buyer apps, receiving on-network transaction data from seller apps for further credit processing.

Technology: ONDC

Core concept: a decentralised protocol where buyer and seller apps communicate directly via Beckn. The ONDC Network is a registry and governance body; on-network transaction data is independently verifiable.

Protocol: Beckn open specification (beckn.network); JSON-LD for data representation; standardised schemas for discovery, order, fulfilment, and post-fulfilment.

How to connect: Network Participant registration with ONDC; Beckn-compliant adapter; integration with ONDC Gateway for discovery routing.

Note: Beckn is an open, decentralised protocol that enables any two platforms to transact without a central intermediary, by defining a common language for discovery, ordering, and fulfilment across digital commerce networks.

2.2.2 Open Credit Enablement Network (OCEN)

OCEN is an open credit protocol connecting Loan Service Providers (LSPs) and lenders through the AA framework via standardised APIs. Conceived by iSPIRT and operationalised through CredAll, a non-profit protocol operator, OCEN facilitated approximately 70,000 loans and over Rs. 1,600 crore in disbursements in 2025, with Q4 2025 volumes 400 percent above Q1 2025.[25]

OCEN addresses the interaction of three roles. The first is the **borrower**, whose credit need is contextualised within an existing platform relationship. The second is the **Loan Service Provider (LSP)**, which is the platform that aggregates borrower demand from within that relationship, such as a GST filing application, agri platform, ecommerce platform, payment gateway, or supply chain management tool. The LSP does not provide capital, assume credit risk, or make underwriting decisions. The third is the **lender**, which is a regulated entity such as a bank or NBFC. Supporting this interaction, a data-sharing layer such as the **Account Aggregator (AA) framework** can be used to transmit consented financial data from Financial Information Providers (FIPs) to the lender's underwriting system.

The efficiency is architectural. A lender integrates with OCEN once and becomes accessible to all LSPs on the protocol. Conversely, an LSP integrates once and can route applications to all participating lenders. OCEN is envisaged as a mechanism for a bank or NBFC seeking to grow MSME origination without proportionate investment in branch infrastructure and field staff. The lender sets its own credit policy and pricing and receives applications from LSPs who have already contextualised the borrower's need.

Technology: OCEN

Core concept: standardised JSON API schemas mean a lender integrates with OCEN once and becomes accessible to all LSPs on the protocol. The AA framework handles data consent; OCEN handles the credit origination workflow.

Protocol: open JSON API specifications at ocen.dev; standardised schemas for loan application, offer, consent linkage, disbursement, and repayment events.

Governance: CredAll (credall.org) acts as non-profit protocol operator; TSPs empanelled by CredAll reduce the integration barrier for smaller institutions.

How to connect: regulated entity status; OCEN API integration via TSP or in-house; AA FIU status for data access; CredAll onboarding.

Note: LSP arrangements are governed by RBI's Digital Lending Directions 2025. The lender remains fully responsible for borrower-facing conduct, while LSPs cannot handle loan funds. Risk sharing, where permitted through Default Loss Guarantee (DLG) structures, is capped at 5%.

2.3 Orchestration / Access Layers

2.3.1 Unified Lending Interface (ULI)

Background. ULI is a unified data aggregation gateway for financial services, operated by the Reserve Bank Innovation Hub (RBIH), a wholly-owned subsidiary of RBI. A pilot was launched in August 2023; a national scale-up programme was initiated in 2024-25.[27]

ULI extends the data layer of the foundational stack into territory the AA framework cannot reach. The AA framework connects regulated financial institutions as data providers. ULI

envisages data aggregation from government databases with no regulated financial custodian: state land registries, satellite crop assessment outputs, kisan credit card repayment histories, milk cooperative payment records, and weather indices. A single ULI API endpoint gives a participant access to multiple government databases simultaneously, without separate integrations with each source. Integration is proceeding state by state, with DFS-coordinated nodal officers nominated by each ministry.[28]

At the ULI pilot launch in August 2023, the RBI Governor said ULI could have an even bigger impact on lending than UPI, because it addresses rural and agricultural financial inclusion in a way earlier DPI layers could not. A smallholder farmer may have land records, satellite-assessed crop data, and a milk cooperative payment history that together constitute a credible financial profile. ULI is the architecture for making that profile legible to any authorised lender. For an agriculture-focused lender or small finance bank serving rural borrowers, ULI eventually provides a pathway to underwrite borrowers who are invisible to the AA framework: no formal bank statements, no GST registration, no employer on EPFO. ULI is still evolving and would be sometime before it reaches a scale of impact.

Technology: ULI

Core concept: a single API gateway aggregating multiple government data sources — including those with no regulated financial custodian — and presenting them through a unified interface with a standardised consent layer.

Data flow: participant sends data pull request with individual consent to RBIH gateway → gateway routes to relevant databases (land registry, GSTN, EPFO, agri data) → aggregated data returned.

Consent: a standardised framework for non-financial government data is being developed as ULI scales; state-level data integration quality varies significantly.

How to connect: regulated entity status; RBIH ULI gateway onboarding; consent management system integration.

2.3.2 API Setu (Government API Marketplace)

API Setu is a MeitY initiative, built on National Informatics Centre (NIC) infrastructure, that serves as a unified API marketplace and gateway for government digital services. Its function in the DPI context is aggregation and standardisation. A regulated entity can discover and access multiple government APIs through a single platform with standardised authentication, monitoring, and sandbox testing [37] , rather than building separate integrations with UIDAI, GSTN, ITD, and other government departments.

The platform operates on a publisher-consumer model. Government departments publish APIs under categories such as document APIs, service APIs, and listing APIs. Regulated entities subscribe to specific APIs and receive access after publisher approval. API Setu provides common governance, data standardisation, secure access controls, and audit monitoring across all integrations.

For lenders and regulated financial entities, API Setu's most relevant capabilities are at the front end of the lending lifecycle like identity verification, business validation, and compliance

checks. Key integrations include PAN validation, Aadhaar-based authentication (where AUA licensing applies), GSTN status checks for business onboarding, and MCA records for company verification. For example, Ministry of External affairs' online verification platform eSanad enables verification of education and professional credentials.

API Setu is not a consent layer and does not carry financial data in the way the AA framework does. It is best understood as reducing integration overhead for institutions that rely on multiple government data lookups during KYC and onboarding. An NBFC that previously maintained separate API integrations with UIDAI, GSTN, and MCA can consolidate those through a single API Setu endpoint with unified authentication and monitoring. The platform also includes a sandbox environment for testing integrations before going live, which reduces time-to-integration for newer participants.

Technology: API Setu

Core concept: a publisher-consumer API marketplace where government departments list APIs and regulated entities subscribe to access them after publisher approval. Single integration point replacing multiple bilateral government API arrangements.

Protocol: REST APIs with standardised OAuth 2.0 authentication; API keys for access control; unified monitoring and audit dashboard; sandbox environment for pre-production testing.

How to connect: registration on apisetu.gov.in; API subscription with approval from the relevant publisher department; integration with specific API endpoints per use case.

2.4 Federated Public Data Systems / Registries

Government-held financial and compliance data sits outside the regulated financial system but is often the most informative data available for borrowers with limited formal banking history. While the focus is on orchestrator layers like AA framework or ULI that integrate these datasets, we at FrankBanker consider these individual APIs as the building blocks for the DPI expansion. The list is ever expanding and list below is only representative of the most popular ones especially in the banking context.

Source	What It Provides	Primary Lending Use	Integration Status
GSTN	GSTR-3B (monthly summary returns), GSTR-1 (outward supply invoices)	Reconstruct monthly turnover, buyer diversity, and seasonal cash flows for MSMEs without audited financials	AA FIP since November 2022[10]
PAN / ITR / AIS	Income Tax Returns, Form 26AS (TDS credits), Annual Information Statement	Verified multi-year income history; TDS data helps corroborate employer and income trails for salaried borrowers	Consent-based pull via ITD-linked APIs and account aggregator-led flows

EPFO (UAN)	Provident fund passbook, contribution history, employer details	Employment tenure and approximate salary band; often more reliable than a self-submitted payslip	AA FIP integration in progress
Vaahan (RC)	Vehicle registration details: owner, class, chassis number, insurance validity, fitness certificate	Asset verification for vehicle-backed products and transport-sector businesses	DigiLocker issuer-pull; API-based integration available
State land record systems	Record of Rights (RoR), mutation records, cadastral maps, registration-linked ownership data	Title and ownership verification for land-backed lending, mortgage creation, agricultural credit, and collateral due diligence	State-specific and uneven; digitised at scale under DILRMP, but not a uniform national AA rail
MSME registration data	Udyam / Udyam Assist registration details, enterprise category, business activity, location, and formalisation status	MSME eligibility validation, borrower profiling, and support for PSL/MSME tagging	Portal/API-based verification; not a standardised AA FIP rail
Customs	Import-export filing and trade transaction data through customs systems such as ICEGATE	Exporter/importer validation, trade-flow verification, and trade finance / working-capital underwriting	Platform/API access; not a mainstream AA-style lending rail
MCA	Company incorporation records, director details, charges registered, and compliance filing history via MCA21	Corporate borrower onboarding, promoter identity and charge verification, and business vintage assessment	Portal/API-based access via MCA21; not an AA FIP rail

Note: TReDS (Trade Receivables Discounting System) is sometimes grouped with DPI in practitioner discussions but is architecturally distinct. TReDS platforms are RBI-licensed market infrastructure entities that facilitate invoice discounting for MSMEs through a three-party model of buyer, seller, and financier. They use DPI rails for identity and payments, but the platforms themselves are licensed, proprietary marketplaces, not open shared infrastructure. The distinction matters for practitioners evaluating integration strategy: OCEN and the AA framework are open protocol layers; TReDS is a licensed marketplace that rides on those layers.

Section 3: Challenges and Limitations

The DPI stack is real, functional, but still evolving. Several components have scaled significantly; others remain constrained by ecosystem depth, data quality, or integration completeness. In some areas, the infrastructure is ahead of ecosystem readiness. In others, the controls around data use and consent have not kept pace with the speed and scale of digital adoption.

The system continues to evolve, with newer features, improvements, and risks. A few material limitations are noted below.

The AA framework currently does not cover joint accounts, partnerships, or NRE/NRO accounts. These gaps are most consequential for MSME credit assessment where current account data from non-sole-proprietor entities is critical.

Private sector adoption of cKYC remains uneven, and records are not automatically updated when customer details change. A cKYC record created five years ago may carry a stale address or an outdated risk classification. It is best treated as a cross-institutional verification reference rather than a primary source of current information.

OCEN's adoption gap is primarily a market-depth issue. The protocol works, but participation remains limited. Its early use was concentrated in transaction-based products such as invoice discounting, which narrowed adoption. OCEN 4.0 has since expanded the framework to include term loans, credit lines, and personal loans, broadening the addressable product set. Even so, scale remains modest: Rs. 1,600 crore in a full year is meaningful, but still small relative to the credit gap it is meant to address.

ULI's limitation is genuine infrastructure immaturity. It is still nascent and would need fair bit of state level digitisation for differentiated value add beyond just being another orchestration layer.

ONDC data is directionally significant but traction remains slower than expected. The onboarding technicalities make it somewhat challenging for a seller or buyer app to go through a learning curve.

Early days of UPI exposed the vulnerabilities around social-engineering frauds like fraudulent collect requests and credential sharing. The controls have improved but serves as reminder that every new digital system opens new vulnerabilities as it scales.

The cybersecurity aspect is inherent in any digital infrastructure initiative. DPI made identity verification faster and more accessible. It made synthetic identity fraud faster and more accessible by the same mechanism. The same frictionless onboarding that serves a legitimate first-time borrower in 90 seconds serves a synthetic identity in 90 seconds. AI-generated identity combinations that pass basic eKYC checks, deepfake-based liveness spoofing, SIM-swap-driven account takeover, scams that target gullible UPI users, and inflated on-network commerce metrics form the current risk surface.

Final Note

DPI has already delivered meaningful gains for India- improving access, reducing process friction, and creating reusable public digital rails at national scale. India's DPI journey is now a studied reference point globally: the JAM Trinity demonstrated that identity, payments, and

bank accounts could be linked at population scale; Aadhaar showed that biometric de-duplication across 1.4 billion records was an engineering problem that could be solved; and UPI demonstrated that interoperable real-time payments could displace cash in a decade. During India's G20 presidency in 2023, DPI was placed at the centre of the global digital cooperation agenda, with India's stack cited as the working proof of concept.

These gains now need to be supported by strong institution-level controls for fraud, monitoring, cyber resilience, and responsible data use. The ecosystem will continue to evolve as adoption deepens and new risks emerge. The Digital Personal Data Protection Act 2023 strengthens the legal framework with more specificity: consent must be free, specific, informed, and unambiguous; individuals have the right to data deletion; penalties apply for misuse.

FrankBanker's view is that practitioners should align with what DPI can reliably deliver today, while keeping their processes and systems flexible enough to incorporate future improvements. India's progress so far has been substantial. The next phase is less about proving the value of DPI and more about strengthening adoption, controls, and governance as the stack matures.

Key Takeaways

India’s DPI for financial services can be organised into four operational buckets: foundational rails, open interoperability frameworks, orchestration / access layers, and federated public data systems / registries.

The core foundational rails in this guide are Aadhaar, cKYC, DigiLocker, eSign, UPI, and the Account Aggregator framework. Together, they support identity verification, reusable KYC, trusted document access, digital execution, payments, and consented financial data sharing.

ONDC and OCEN are protocol-led interoperability frameworks. ONDC enables interoperable digital commerce across network participants, while OCEN standardises contextual credit origination between Loan Service Providers and regulated lenders. ONDC had more than 1.16 lakh retail sellers across 630+ cities as of December 2025, while OCEN facilitated about 70,000 loans and over ₹1,600 crore in disbursements during 2025.

ULI and API Setu function as access and orchestration layers. ULI is being scaled as a unified lending data gateway, especially for rural and agricultural credit use cases, while API Setu provides a common access layer for multiple government APIs.

Public data systems such as GSTN, PAN / ITR / AIS, EPFO, Vaahan, land records, MSME registration data, Customs, and MCA are increasingly important to digital lending workflows because they extend underwriting and verification beyond the regulated financial data available through AA.

The Account Aggregator framework is a consent-based, data-blind financial data-sharing architecture. Its current coverage gaps, especially joint accounts, partnership and company current accounts, and NRE/NRO discoverability, remain relevant constraints in MSME credit assessment. More than 2.61 billion financial accounts were enabled on the AA framework as of 31 December 2025.

UPI, Aadhaar, and DigiLocker show the scale already achieved by India’s DPI stack. UIDAI reports about 144 crore Aadhaar numbers generated, more than 17,080 crore authentications, and over 2,327 crore eKYC transactions; NPCI reported 20.39 billion UPI transactions worth

₹26.84 lakh crore in February 2026 across 694 live banks; and PIB reported DigiLocker at 67.63 crore users and more than 950 crore documents by March 2026.

The main current limitations are uneven ecosystem adoption, incomplete coverage across some borrower and data categories, fraud and social-engineering risks, and gaps between consent design and consent implementation.

The Digital Personal Data Protection Act, 2023 provides the legal framework for consent-based processing, data fiduciary obligations, and penalties. Provisions relating to the establishment of the Data Protection Board of India were brought into force from 13 November 2025, so the current issue is less about the absence of a legal framework and more about phased operationalisation and enforcement.

References

1. *G20 New Delhi Leaders' Declaration, September 2023. g20.org*
2. *UN Secretary-General's Roadmap for Digital Cooperation, 2023. un.org*
3. *World Bank, Digital Public Infrastructure: Setting Standards with the Hourglass Model, 2025. thedocs.worldbank.org*
4. *IMF, Retail Digital Payments Report, June 2025. imf.org*
5. *PIB, India's Digital Public Infrastructure, March 2026. pib.gov.in*
6. *World Bank, Global Findex Database 2022. worldbank.org*
7. *IIMB Monograph, Decoding Digital Public Infrastructure: Scripting Inclusive Digital Futures, 2024. iimb.ac.in*
8. *NPCI; Ministry of Finance, JAM Trinity and DBT, 2024. npci.org.in; finmin.nic.in*
9. *RBI Master Direction on Non-Banking Financial Company — Account Aggregator (Reserve Bank) Directions, 2016 (updated 2021). rbi.org.in*
10. *RBI Circular on inclusion of GSTN as Financial Information Provider, November 2022. rbi.org.in*
11. *UIDAI Annual Report 2025-26; PIB Press Release, March 2026. uidai.gov.in; pib.gov.in*
12. *UIDAI Circular on Offline eKYC, 2018; RBI KYC Master Direction (updated 2023). uidai.gov.in; rbi.org.in*
13. *Supreme Court, Justice K.S. Puttaswamy (Retd.) v. Union of India, WP(C) No. 494 of 2012*
14. *MeitY; PIB, March 2026. digilocker.gov.in; pib.gov.in*
15. *MeitY DigiLocker API Documentation; IT Act 2000, Second Schedule. digilocker.gov.in*
16. *IT Act 2000, Section 5; Electronic Signature Rules 2015; RBI Digital Lending Directions, May 2025. meity.gov.in; rbi.org.in*
17. *RBI KYC Master Direction 2016 (updated 2023); SEBI Circular on CKYCRR 2016; CERSAI. rbi.org.in; sebi.gov.in; cersai.org.in*
18. *NPCI UPI Product Statistics, January 2026; ACI Worldwide, Prime Time for Real Time, 2024. npci.org.in; aciworldwide.com*
19. *NPCI UPI Procedural Guidelines; RBI Circular on Pre-Sanctioned Credit Lines at Banks through UPI, December 2024. npci.org.in; rbi.org.in*
20. *Department of Financial Services, Ministry of Finance, Account Aggregator Progress Update, December 2025. financialservices.gov.in*
21. *ReBIT API specifications, api.rebit.org.in; Sahamati, sahamati.org.in*
22. *RBI Circular on inclusion of GSTN as FIP, November 2022; Income Tax Department; EPFO; Ministry of Road Transport and Highways, Vahan. rbi.org.in*
23. *ONDC Network Statistics, Q4 2025. ondc.org*
24. *RBI Circular on TReDS; PIB, TReDS Statistics 2024-25. rbi.org.in; pib.gov.in*
25. *ProductNation / iSPIRT, OCEN 2025 Annual Review, January 2026. pn.ispirt.in; ocen.dev*
26. *RBI Digital Lending Directions, May 2025; iSPIRT OCEN 4.0 Specifications. rbi.org.in; ocen.dev*

27. *PIB, DFS High-Level Meeting on Scaling Up ULI, 2025; RBI Governor's Statement on ULI Pilot, August 2023. pib.gov.in*

28. *PIB, DFS High-Level Meeting on ULI Scale-Up, 2025. pib.gov.in*

29. *Centre for DPI, DPI Overview and Architecture Principles. docs.cdpi.dev*

30. *UIDAI AUA/KUA Technical Specification; ReBIT, api.rebit.org.in; RBI Data Localisation Circular April 2018; DPDP Act 2023*

31. *UIDAI; NPCI; MeitY; ReBIT, api.rebit.org.in; Sahamati; Beckn Network, beckn.network; ocen.dev; RBIH*

32. *CASParser, State of Account Aggregator 2026; ProductNation, OCEN 2025 Review; PIB DFS ULI Scale-Up 2025*

33. *The Tribune, Aadhaar Data Breach Report, January 2018; Resecurity, PII Belonging to Indian Citizens on Dark Web, October 2023. resecurity.com*

34. *NASSCOM-DSCI Cybersecurity Outlook 2024; RBI Bulletin, June 2025; Finance Ministry, Lok Sabha Statement, November 2024; CERT-In Advisory on Deepfake Fraud, 2024*

35. *DPDP Act 2023; RBI Master Direction on AA (2021); MeitY, DPDP Rules 2025 (under finalisation). meity.gov.in; rbi.org.in*

36. *Credit Information Companies (Regulation) Act 2005; DPDP Act 2023; US FTC v. ITMedia Solutions LLC, January 2022. ftc.gov*

37. *MeitY / National Informatics Centre, API Setu — Government API Marketplace and Platform Documentation. apisetu.gov.in*

Further Reading

Primary Regulatory Sources

RBI Master Direction — Account Aggregator (Reserve Bank) Directions, 2016 (updated 2021). rbi.org.in
RBI Master Direction — Know Your Customer (KYC) Direction, 2016 (updated 2023). rbi.org.in
RBI Digital Lending Directions, 2025 (issued May 8, 2025). rbi.org.in
RBI Circular — Pre-Sanctioned Credit Lines at Banks through UPI, December 2024. rbi.org.in
Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. indiacode.nic.in
Digital Personal Data Protection Act, 2023. meity.gov.in
Credit Information Companies (Regulation) Act, 2005. rbi.org.in
IT Act 2000, Second Schedule — Electronic Signature Rules. meity.gov.in
Supreme Court — Puttaswamy v. Union of India, WP(C) 494/2012

Government and Official Sources

UIDAI — AUA/KUA Framework and Aadhaar Technology Architecture. uidai.gov.in
Department of Financial Services — Account Aggregator Progress Update, December 2025. financialservices.gov.in
PIB — India's Digital Public Infrastructure, March 2026. pib.gov.in
NPCI — UPI Product Statistics and Procedural Guidelines. npci.org.in
MeitY — DigiLocker API Documentation. digilocker.gov.in
MeitY / NIC — API Setu Platform Documentation. apisetu.gov.in
CERSAI — Central KYC Registry. cersai.org.in
G20 New Delhi Leaders' Declaration, September 2023. g20.org

DPI Ecosystem References

Centre for DPI (CDPI) — DPI Overview and Architecture Principles. docs.cdpi.dev
Sahamati — FIP/FIU Ecosystem Status and Technical Documentation. sahamati.org.in
ReBIT — AA Technical Specifications. api.rebit.org.in
iSPIRT / ProductNation — OCEN 2025 Annual Review. ocen.dev / pn.ispirt.in
ONDC Network — Beckn Protocol Documentation. ondc.org / beckn.network
World Bank — Digital Public Infrastructure: Setting Standards with the Hourglass Model, 2025. thedocs.worldbank.org
IIMB Monograph — Decoding Digital Public Infrastructure, 2024. iimb.ac.in
Institut Montaigne — India's Digital Public Infrastructure: A Success Story for the World?, 2024. institutmontaigne.org

Risk and Data Protection

NASSCOM-DSCI — Cybersecurity Outlook India 2024. dsci.in
RBI Bulletin — June 2025 (account takeover fraud data). rbi.org.in
Resecurity — PII Belonging to Indian Citizens on Dark Web, October 2023. resecurity.com
US FTC v. ITMedia Solutions LLC — lead generator data misuse, January 2022. ftc.gov