Department of Agriculture
Government of Maharashtra

OATS
Open AgriTrace Stack

A UNIVERSAL SOVEREIGN TOOLKIT FOR THE DESIGN AND DEPLOYMENT OF POPULATION-SCALE AGRI- TRACEABILITY

Digital Public Infrastructure



Knowledge partners

THE WORLD BANK IBRD IDA WORLD BAN GROUP

KWPF Korea-World Bank Partnership Facility

AIAIC AI and AgriTech Innovation Center — AI for Every Acre —

TRST01 TRUST-TRANSPARENCY-TRACEABILITY



Open AgriTrace Stack

Open Protocols. Sovereign Data. Compliant

A Universal Sovereign Toolkit for the Design and Deployment of

Population-Scale Agri Traceability Digital Public Infrastructure

Preface

This Blueprint development has been commissioned by the World Bank in partnership with the Department of Agriculture, Government of Maharashtra as a global public good, to develop a coherent, standards-grounded reference architecture for population-scale agri-food traceability Digital Public Infrastructure. The work has been financed through a grant from the Korea-World Bank Partnership Facility (KWPF), whose support has enabled the Blueprint to be developed, peer-reviewed, and published without recourse to commercial licensing models.

The document serves two purposes. It is a blueprint, establishing the normative architecture, principles, standards mappings, and design specifications that define what an OATS-conformant traceability DPI must be. It is also a toolkit, providing the operational guidance, conformance levels, procurement scaffolding, and implementation workflows that enable that architecture to be deployed. This dual framing is intentional. In every jurisdiction where this work has been examined, the institutional teams responsible for normative design and the teams responsible for operational implementation are the same teams, typically housed within an Agriculture Department Delivery Unit or its equivalent. The Blueprint reflects that working reality. Where readers prefer to engage with only the normative or only the operational dimensions, the modular publication strategy and the audience-to-chapter map on the following pages enable that separation in practice.

The OATS architecture is jurisdiction-neutral, vendor-neutral, and technology-neutral. Every specification, identifier scheme, event schema, conformance level, and governance instrument it defines is structured to function in any regulatory context, at any level of digital maturity, and across any agri-food value chain. The Indian federal context, including India Stack, AgriStack, the Beckn-powered Open Network for Digital Commerce (ONDC) and VISTAAR, MahaVISTAAR, MahaAGX, and the APEDA traceability systems, is used throughout as the illustrative good-practice implementation model because these are currently among the most extensively documented DPI deployments globally. The OATS Blueprint is not a description of those systems and is not bound to them. It is a generalised reference architecture that draws on India Stack implementation experience alongside global precedents from the European Union, the United States, Brazil, Australia, the Republic of Korea, and elsewhere.

The Blueprint is published under a Creative Commons Attribution 4.0 International licence (***CC BY 4.0***). This is a deliberate stewardship design. Any government, multilateral agency, academic institution, standards body, private sector organisation, or implementing consortium may reuse, adapt, translate, extend, or improve the Blueprint without seeking centralised permission, paying licence fees, or maintaining alignment with any single authoring institution. This is consistent with the foundational DPI principle of Open by Default articulated in Chapter 2, and it ensures that the Blueprint remains a living resource, capable of evolving across geographies, languages, regulatory generations, and technological frontiers without dependence on any single steward.

Acknowledgements

This Blueprint is the product of a structured institutional collaboration between the World Bank , the Government of Maharashtra, and a consortium of technical institutions led by TrayamBhu Tech Solutions Private Limited.(TRST01)

The financing for this work has been provided through the Korea-World Bank Partnership Facility (KWPF), administered under the World Bank supported State of Maharashtra Agribusiness and Rural Transformation (SMART) Project. The grant has enabled the Blueprint to be developed, peer-reviewed, and published as an open knowledge product, available without licensing constraint to any government, multilateral institution, academic body, standards organisation, or implementing entity that wishes to adopt or adapt it.

The Blueprint has been produced under the leadership of the World Bank task team responsible for this engagement. The team has been led by Mr. Adarsh Kumar under the strategic guidance of Ms. Gayatri Acharya, Practice Manager. Technical direction for architectural and standards-mapping for the Blueprint has been provided by Mr. Vikas Kanungo, Senior Consultant for Artificial Intelligence and Digital Transformation.

The institutional demand that anchored this engagement was articulated by the Government of Maharashtra. The authoring team gratefully acknowledges the institutional leadership of Mr. Vikas Rastogi, Additional Chief Secretary, Government of Maharashtra, whose strategic direction shaped the scope and ambition of the work; and Mr. Parimal Singh, Principal Secretary, Department of Agriculture, Government of Maharashtra, whose articulation of the state's traceability requirements provided the operational evidence base against which the architecture has been developed. Substantive contributions on the side of the state government were provided by Mr. Srikant Andge, Managing Director of the AI and AgriTech Innovation Centre (AIAIC), who led the diagnostic study and the identification of priority crops; and by Mr. Parag Dabhade, Chief Technology Officer, AIAIC, who guided the team on the technical design and Digital Public Infrastructure architecture principles.

The Blueprint has been authored by the TRST01 Consortium, with TrayamBhu Tech Solutions Private Limited serving as the lead authoring entity. The authoring team gratefully acknowledges the leadership of Mr. Prabir Mishra, Founder and Chief Executive Officer of TRST01, whose stewardship of the consortium ensured the technical rigour and editorial coherence of the Blueprint. The consortium has been supported by its constituent member institutions: the Indian Council of Agricultural Research, Central Institute for Research on Cotton Technology (ICAR-CIRCOT); GS1 India, the Indian member organisation of GS1 Global; and Tetra Information Services Private Limited. Each constituent member contributed domain expertise and institutional knowledge that shaped the substantive content of the Blueprint.

The Blueprint has benefited from a formal peer review process conducted by recognised institutions in the field of Digital Public Infrastructure. External peer review was conducted by the Centre for Digital Public Infrastructure (CDPI), under the leadership of Mr. Vineet Bhandari, Chief Operations Officer; and by the World Economic Forum Centre for the Fourth Industrial Revolution (C4IR), under the joint leadership of Mr. J. Satyanarayana, Chief Advisor, and Mr. Shreejit Borthakur, Lead for AgriTech. Both institutions conducted a comprehensive peer review of the full Blueprint and accompanying Toolkit, and their observations have materially strengthened the architectural framework, the conformance specifications, and the implementation guidance.

This Blueprint is contributed to the global Digital Public Infrastructure movement as a public good, in the spirit of open collaboration that defines the field. It is offered to every government, institution, and practitioner working to build food systems in which traceability is universal, trust is built into the

architecture, and the farmer at the origin of every value chain stands to benefit, but is never asked to bear the cost.

Abbreviations and Acronyms

Abbreviation	*Full Form*
ABDM	Ayushman Bharat Digital Mission
ACS	Additional Chief Secretary
ADB	Asian Development Bank
AePS	Aadhaar-enabled Payment System
AgriStack	India's Federated Agricultural Data Architecture
AI	Artificial Intelligence
AIAIC	AI and AgriTech Innovation Center
ANSI	American National Standards Institute
API	Application Programming Interface
APEDA	Agricultural and Processed Food Products Export Development Authority
APMC	Agricultural Produce Market Committee
B2B	Business to Business
B2C	Business to Consumer
BCP	Business Continuity Plan
Beckn	Beckn Open Protocol
BIS	Bureau of Indian Standards
BoM	Bill of Materials
BRS	Business Requirements Specification
CA	Certificate Authority
CAGR	Compound Annual Growth Rate
CAP	Common Agricultural Policy (EU)
CBV	Core Business Vocabulary (GS1)
CC BY 4.0	Creative Commons Attribution 4.0 International
CDN	Content Delivery Network
CDPI	Centre for Digital Public Infrastructure
CFIA	Canadian Food Inspection Agency
CI/CD	Continuous Integration / Continuous Delivery
CIRCOT	Central Institute for Research on Cotton Technology (ICAR)
COA	Certificate of Analysis
CoC	Chain of Custody
CoO	Certificate of Origin
CSC	Common Service Centre
CSV	Comma-Separated Values
DBT	Direct Benefit Transfer
DGFT	Directorate General of Foreign Trade (Government of India)
DID	Decentralised Identifier (W3C)
DigiLocker	DigiLocker (India's federated document repository)
DLT	Distributed Ledger Technology
DNS	Domain Name System
DPDPA	Digital Personal Data Protection Act, 2023 (India)
DPI	Digital Public Infrastructure
DPIA	Data Protection Impact Assessment
DPP	Digital Product Passport (EU)
DR	Disaster Recovery
e-KYC	Electronic Know Your Customer
e-NAM	National Agriculture Market (electronic)
e-NWR	Electronic Negotiable Warehouse Receipt
EFSA	European Food Safety Authority
EOI	Expression of Interest

EPC	Electronic Product Code (GS1)
EPCIS	Electronic Product Code Information Services (GS1)
ERD	Entity-Relationship Diagram
ESG	Environmental, Social, and Governance
ETL	Extract, Transform, Load
EU	European Union
EUDR	European Union Deforestation Regulation
FAO	Food and Agriculture Organization of the United Nations
FBO	Food Business Operator
FCI	Food Corporation of India
FDA	Food and Drug Administration (United States)
FPC	Farmer Producer Company
FPO	Farmer Producer Organisation
FRS	Functional Requirements Specification
FSC	Forest Stewardship Council
FSMA	Food Safety Modernization Act (United States)
FSSAI	Food Safety and Standards Authority of India
GACC	General Administration of Customs of the People's Republic of China
GAP	Good Agricultural Practices
GDPR	General Data Protection Regulation (EU)
GeM	Government e-Marketplace (India)
GFSI	Global Food Safety Initiative
GHG	Greenhouse Gas
GI	Geographical Indication
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
GLN	Global Location Number (GS1)
GMP	Good Manufacturing Practices
GoI	Government of India
GoM	Government of Maharashtra
GS1	Global Standards 1 (international standards organisation)
GST	Goods and Services Tax (India)
GSTN	Goods and Services Tax Network (India)
GTIN	Global Trade Item Number (GS1)
HACCP	Hazard Analysis and Critical Control Points
HLD	High-Level Design
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IAS	Indian Administrative Service
IBRD	International Bank for Reconstruction and Development
ICAR	Indian Council of Agricultural Research
ICT	Information and Communications Technology
IDA	International Development Association
IDE	Integrated Development Environment
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFAD	International Fund for Agricultural Development

IFC	International Finance Corporation
IMD	India Meteorological Department
IoT	Internet of Things
IPM	Integrated Pest Management
IPPC	International Plant Protection Convention
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
JWT	JSON Web Token
KMS	Key Management Service
KPI	Key Performance Indicator
KYB	Know Your Business
KYC	Know Your Customer
LCA	Life Cycle Assessment
LDAP	Lightweight Directory Access Protocol
LLD	Low-Level Design
MahaAGX	Maharashtra Agri Exchange
MahaVISTAAR	Maharashtra VISTAAR Platform
MD	Managing Director
MeitY	Ministry of Electronics and Information Technology (Government of India)
MFA	Multi-Factor Authentication
MIGA	Multilateral Investment Guarantee Agency
MIS	Management Information System
MoA&FW	Ministry of Agriculture and Farmers' Welfare (Government of India)
MoCAFPD	Ministry of Consumer Affairs, Food and Public Distribution (Government of India)
MoCom	Ministry of Commerce and Industry (Government of India)
MoEFCC	Ministry of Environment, Forest and Climate Change (Government of India)
MOSIP	Modular Open Source Identity Platform
MoU	Memorandum of Understanding
MRL	Maximum Residue Limit
MSP	Minimum Support Price
mTLS	Mutual Transport Layer Security
NABARD	National Bank for Agriculture and Rural Development
NCDEX	National Commodity & Derivatives Exchange
NDA	Non-Disclosure Agreement
NFR	Non-Functional Requirements
NGO	Non-Governmental Organisation
NIC	National Informatics Centre (Government of India)
NoSQL	Not Only SQL
NPCI	National Payments Corporation of India
OATS	Open Agricultural Traceability System
OAuth	Open Authorization
ODA	Official Development Assistance
OECD	Organisation for Economic Co-operation and Development
OIDC	OpenID Connect
ONDC	Open Network for Digital Commerce
PaaS	Platform as a Service
PACS	Primary Agricultural Credit Society

PDS	Public Distribution System
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PM-KISAN	Pradhan Mantri Kisan Samman Nidhi
PMFBY	Pradhan Mantri Fasal Bima Yojana
PMU	Project Management Unit
PoC	Proof of Concept
PPP	Public–Private Partnership
QR Code	Quick Response Code
RBAC	Role-Based Access Control
RBI	Reserve Bank of India
REST	Representational State Transfer
RFC	Request for Comments (IETF)
RFI	Request for Information
RFID	Radio-Frequency Identification
RFP	Request for Proposal
RFQ	Request for Quotation
ROI	Return on Investment
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SDG	Sustainable Development Goals (United Nations)
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SECO	State Secretariat for Economic Affairs (Switzerland)
SGTIN	Serialised Global Trade Item Number (GS1)
SHG	Self-Help Group
SLA	Service Level Agreement
SLI	Service Level Indicator
SLO	Service Level Objective
SOAP	Simple Object Access Protocol
SOP	Standard Operating Procedure
SoW	Statement of Work
SPS	Sanitary and Phytosanitary (WTO Agreement)
SQF	Safe Quality Food
SQL	Structured Query Language
SRS	Software Requirements Specification
SSCC	Serial Shipping Container Code (GS1)
SSI	Self-Sovereign Identity
SSO	Single Sign-On
STQC	Standardisation Testing and Quality Certification (Government of India)
TBT	Technical Barriers to Trade (WTO Agreement)
TCO	Total Cost of Ownership
TLS	Transport Layer Security
ToR	Terms of Reference
TPS	Transactions Per Second
TRST01	TrayamBhu Tech Solutions Pvt Limited
UAT	User Acceptance Testing
UI	User Interface
UIDAI	Unique Identification Authority of India

UML	Unified Modeling Language
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNDP	United Nations Development Programme
UNFCCC	United Nations Framework Convention on Climate Change
UNIDO	United Nations Industrial Development Organization
UPI	Unified Payments Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USAID	United States Agency for International Development
USDA	United States Department of Agriculture
UUID	Universally Unique Identifier
UX	User Experience
VC	Verifiable Credential (W3C)
VISTAAR	Virtual Implementation of Skills, Tools, Agronomy, Advisory and Resources
VP	Verifiable Presentation (W3C)
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAF	Web Application Firewall
WBG	World Bank Group
WBS	Work Breakdown Structure
WFP	World Food Programme
WHO	World Health Organization
WOAH	World Organisation for Animal Health
WTO	World Trade Organization
XML	Extensible Markup Language
YAML	YAML Ain't Markup Language

About This Toolkit

The OATS Blueprint is a universal, jurisdiction-agnostic operational toolkit, a modular composition of specifications, frameworks, standards mappings, and implementation guidance from which any government, multilateral agency, or implementation consortium may select the modules relevant to its regulatory context, digital maturity, and agri-food value chains. The Indian federal context — India Stack, AgriStack, the Beckn-powered ONDC and VISTAAR, MahaVISTAAR, MahaAGX, and APEDA traceability systems — is used throughout as the illustrative good-practice implementation model, but the OATS architecture is designed for adoption in any jurisdiction, from a single subnational state to a multi-country regional bloc.

Each section of the Blueprint has been deliberately designed for a distinct audience, policymakers and government architects, procurement and legal teams, technical designers and system integrators, and regulatory and field-level implementation managers. The publication strategy is specifically designed to address this: each section will be released separately in a modular digital format, enabling every stakeholder to access the section appropriate to their role and requirement. A condensed version, comprising the most essential and universally applicable content, is being prepared for broader dissemination.

How to Use This Toolkit

Each chapter is a self-contained module and each Part is internally coherent. No reader is expected to engage with every chapter — most will engage with three to five. Greenfield implementations may deploy all modules; brownfield contexts may select specific modules for integration with existing infrastructure. Every chapter includes a Functional Requirement Specification defining what the system must do and a System Requirement Specification defining how it must be built, together forming the basis for procurement scope, vendor evaluation, and conformance testing. The Blueprint maps every component to authoritative global standards: GS1 EPCIS 2.0, ISO 22005:2007, Codex CXC 60-2006, W3C Verifiable Credentials, FSMA 204, EU 178/2002, and DPDPA 2023. Illustrative examples are drawn throughout from India, the EU, the USA, Brazil, and Australia, providing concrete implementation precedent.

To navigate the Blueprint efficiently, readers should identify their profile from the **eight listed below** and follow the **Audience-to-Chapter Map** on the next page, which lists the chapters relevant to each profile with a one-line summary of what each chapter contains.

Audience-to-Chapter Map

Each chapter of the Blueprint is a self-contained module; no reader is expected to engage with every chapter. Most readers will engage with **three to five** chapters most directly relevant to their role. Identify the profile below that best fits your responsibility, and treat the listed chapters as your primary reading path. The Blueprint may then be navigated laterally — through cross-references between chapters — as the depth of engagement increases.

Profile 1 — Policymakers & Government Sponsors

Ministers, Principal Secretaries, Heads of Agriculture Departments, NITI Aayog-equivalent strategy units. Need the public-policy case, governance architecture, and the upside on consumer trust and farmer outcomes.

Ch.	Chapter / Appendix Title	One-line summary
1	Vision, Mission & Strategic Framework	Why population-scale traceability must be Digital Public Infrastructure; the public-policy imperative.
2	Principles, Design Tenets & Governance Values	The 20 OATS P-Principles, governance values, and anti-patterns that anchor any compliant deployment.
3	Stakeholder Ecosystem & Actor Mapping	Six actor tiers, the OATS Multi-Stakeholder Governance Council (OMGC), and engagement sequencing.
15	Consumer Transparency & Market Access	The Four-Pillar Disclosure model and the premium-market upside for GI/Organic/Fair-Trade producers.
16	Financial Inclusion & Value-Chain Finance	Event chain as collateral-grade evidence; linkages to KCC, PMFBY, eNWR finance, and DBT/CBDC.

Profile 2 — DPI Architects & Government CTOs

AIAIC, NIC, MeitY-equivalent architects and Chief Technology Officers responsible for the cross-cutting technical design of state and national stacks.

Ch.	Chapter / Appendix Title	One-line summary
4	OATS Reference Architecture & System Design	The 5+1 layer hourglass; canonical building blocks for each layer; design rationale.
5	Identity, Trust, Registry & Credentialing	GS1 GLN/GTIN/SSCC, W3C DIDs and VCs, AgriStack / MOSIP linkage, Status List 2021.
6	Events & Anchoring (GS1 EPCIS 2.0)	Critical Tracking Events, Key Data Elements, FSMA 204 and EU 178/2002 mapping.
9	Blockchain & DLT Integration	Decision framework: when to use DLT; Hyperledger Fabric, Besu, IOTA, CORD compared.
10	APIs, Microservices & Integration	REST-first OpenAPI 3.1, GovStack Information Mediator (X-Road) federation pattern.
+1	Intelligence Layer (Ch. 4 §4.6)	Risk scoring, satellite phenology, mass-balance fraud detection — augmentation, not override.

Profile 3 — Procurement, Legal & Compliance Officers

Procurement leads, government counsel, and compliance officers responsible for tenders, RFPs, contracting, data-protection sign-off, and conformance certification.

Ch.	Chapter / Appendix Title	One-line summary
App. A	FRS / SRS Compact Matrix	Procurement-ready functional and system requirements, tier-mapped per chapter.
13	Regulatory Compliance & Legal Architecture	GI/PDO, NPOP, NOP, EU Organic legal scaffolding; per-regulation crosswalk.
14	Cybersecurity, Privacy & Data Protection	DPIA framework, Significant Data Fiduciary obligations, audit logging, non-repudiation.
12	OATS Consent Management System	DPDPA-aligned consent artefacts, ORGANS framework, Consent Manager architecture.
App. B	Standards Index & References	Authoritative standards catalogue for tender specifications and conformance language.

Profile 4 — System Integrators & Technical Designers

Solution architects, lead engineers, and integration teams building or extending the OATS stack inside government or for a prime vendor.

Ch.	Chapter / Appendix Title	One-line summary
4	OATS Reference Architecture	Layered architectural blueprint and design rationale for L1–L5 plus +1.
6	GS1 EPCIS 2.0 Event Model	Five EPCIS event types, sensor/cold-chain integration, transformation events.
7	Physical–Digital Linkage	GS1 Digital Link QR, Data Matrix, RFID, NFC; Sunrise 2027 transition guidance.
8	Open Network Layer (Beckn Integration)	OATS-Beckn interface, BAP/BPP roles, network lifecycle, network policies.
10	APIs, Microservices & Integration	Event-driven backbone, aggregation layer, ERP/TMS connector patterns.
App. C	Schema & API Reference Index	Implementable schemas and endpoint catalogue for direct build.

Profile 5 — Regulators, Standards Bodies & Auditors

FSSAI, APEDA, DGFT, BIS, NABL, NPOP accreditors, FBO/audit firms, and equivalent regulatory institutions across jurisdictions.

Ch.	Chapter / Appendix Title	One-line summary
2	Principles, Design Tenets & Anti-Patterns	Conformance baseline against which any OATS-conformant implementation is evaluated.
6	EPCIS, CTEs & KDEs	Canonical event-level conformance specification; KDE matrix; Birth-of-Lot Principle.
13	Regulatory Compliance Framework	Per-regulation crosswalk; Digital Sentinel design for HACCP and CCPs.
14	Cybersecurity, Privacy & Data Protection	Audit logging, non-repudiation, DPIA process, evidence retention.
App. A	FRS / SRS Compact Matrix	Conformance-tier framework for certification and audit testing.

Profile 6 — Implementation Managers & Agriculture Department Delivery Units

Programme managers and field-implementation leads inside state/national delivery units, plus FPO federations and aggregator/exporter PMOs running roll-outs.

Ch.	Chapter / Appendix Title	One-line summary
3	Stakeholder Ecosystem & Actor Mapping	OMGC governance council, multi-stakeholder engagement strategy, sequencing playbook.
7	Physical–Digital Linkage (smallholder bridge)	Mobile-first, offline-capable capture; device-bound keys; USSD fallback for feature phones.
11	Data Governance & Federated Data Model	Tiered access (Open / Shared / Restricted), retention, archival, and right to erasure.
15	Consumer Transparency & Market Access	Four-Pillar Disclosure, QR consumer journey, grievance and feedback mechanisms.
16	Financial Inclusion & Value-Chain Finance	Operational integrations with KCC, PMFBY, eNAM/WDRA, and gender-responsive design.

Profile 7 — AgriTech Vendors & ERP / TMS Integrators

Private-sector AgriTech, ERP, TMS, cold-chain, and IoT solution providers building products that interoperate with the OATS stack.

Ch.	Chapter / Appendix Title	One-line summary
5	Identity, Trust & Credentialing	VC issuance flows, wallet integration patterns, hash anchoring on the Fabric governance channel.
7	Carrier Stack & IoT Integration	FIWARE NGSI-LD, OGC SensorThings API, cold-chain monitoring, field-capture devices.
8	Beckn / OATS Protocol	BAP/BPP integration patterns, message semantics, cross-network traceability flows.
10	APIs, Microservices & Integration	Plug-in surface for ERP/TMS connectors; event-driven ingestion; aggregation layer.
12	Consent Management	Consent artefact handling, revocation hooks, and audit obligations inside vendor systems.

Profile 8 — Development Finance Institutions & Multilateral Donors

World Bank, ADB, IFAD, IFC, GIZ, USAID, FCDO, regional MDBs, and bilateral development partners financing traceability and food-systems programmes.

Ch.	Chapter / Appendix Title	One-line summary
1	Vision, Mission & Strategic Framework	Scale of opportunity; the export-rejection cost case; the public-good rationale.
3	Stakeholder Ecosystem & Actor Mapping	Governance models, donor-coordination architecture, public–private participation.
11	Data Governance & Federated Data Model	Sovereign federation; cross-jurisdiction data flows; alignment with DPI safeguards.
16	Financial Inclusion &	Investable financial primitives derived from OATS event chains; PPP-readiness.

Ch.	Chapter / Appendix Title	One-line summary
	Value-Chain Finance	
App. A	FRS / SRS Compact Matrix	Implementation cost and conformance benchmarks for results frameworks and M&E.

Table of Contents

Table of Contents

Preface 5
Acknowledgements 7
Abbreviations and Acronyms 9
About This Toolkit 15
How to Use This Toolkit 15
Audience-to-Chapter Map 17
Executive Summary 25
1. Vision, Mission, and Strategic Framework 31
1.1 Definitions 31
1.2 The Global Food Safety and Traceability Imperative 33
1.3 Why Traceability Must Be Digital Public Infrastructure (DPI) 34
..... 34
1.4 The OATS Design Philosophy: Open, Federated, Sovereign 35
1.5 Strategic Alignment with Global Frameworks 36
2. Principles, Design Tenets, and Governance Values 37
2.1 Introduction 37
2.2 Governance Values and Ethics for Traceability DPI 39
2.3 OATS Anti-Patterns: Common Violations to Reject 39
3. Stakeholder Ecosystem and Actor Mapping 41
3.1 Introduction and Actor Classification Framework 41
3.1.3 (Tier 5) - Regulatory, Standards, and Certification Bodies 42
3.1.4 Tier 6 - Technology Providers and AgriTech Ecosystem 43
3.2 The Port-of-Entry Data Validation Nexus: Government as Certifier 43
3.3 OATS Multi-Stakeholder Governance Council (OMGC): Composition and Mandate 45
3.4 Stakeholder Engagement Strategy and Implementation Sequencing 46
4. OATS Reference Architecture and System Design 49
4.1 Architecture Design Rationale: The 5+1 Layer DPI Model 49
4.2 Master Overview: The OATS 5+1 Layer stack 49
4.2.3 Layer 3: Interoperability, Open Protocol & Commerce 52
4.3 The Hourglass Protocol Model 55
5. Identity, Trust, Registry and Credentialing Standards 57
5.1 Entity Identification Framework: GLN, GTIN and National IDs 57
5.2 Decentralized identity: W3C DIDs and DID Methods 58
5.3 Verifiable Credentials for Certifications and Compliance 59
5.4 Farmer Registry: Architecture, APIs and AgriStack Integration 60
5.5 Business and Facility Registry 60
5.6 Product and Commodity Registry 61
5.7 Certification and Accreditation Registry 61
5.8 Identity Federation and Cross-Jurisdiction Interoperability 63
5.9 Federated Registry Resilience: Failure Handling, Degraded Operations and Reconciliation 63
6. Traceability Event Data Model and EPCIS2.0 Implementation 65

6.1 GS1 EPCIS 2.0: Architecture and Event Model....65
6.2 Critical Tracking Events (CTEs) Across the Agri-Food Value Chain....65
....65
6.3 Key Data Elements (KDEs): Detailed Field Specifications....67
6.4 The Five EPCIS Event Types: Functional and Technical Mapping....69
6.5 Sensor Data and Cold Chain Integration (EPCIS 2.0 'How' Dimension)....70
6.7 Transformation Event: Processing and Comingling....70
6.8 FSMA 204 Compliance Mapping to EPCIS KDE....71
6.9 EU 178/2002 and Farm-to-Fork Alignment....71

7. Physical-Digital Linkage: Identifiers, Carriers, and IoT Integration....73
7.1 Physical Identifier Standards: QR Code, Data Matrix, RFID, NFC....73
7.2 GS1 Digital Link: Web-Addressable Product Identifiers....73
7.3 GS1 Sunrise 2027: Transition to 2D Barcodes....73
7.4 RFID and EPC Gen2 for Automated Bulk Identification....75
7.5 IoT Integration: FIWARE NGSI_LD and OGC SensorThings API....75
7.6 Cold Chain Monitoring: Temperature, Humidity and Shock Sensor....76
7.7 Field-Level and Farm-Gate Capture Devices....76
7.8 Resolver Architecture and GS1 Digital Link Registry....76

8. Open Network Layer: Beckn Protocol Integration and the OATS-Beckn Specification. 79
8.1 Beckn Protocol: The Parent of the OATS Protocol....79
8.2 The OATS Protocol: A Beckn-Derived Traceability Protocol....79
8.3 The OATS Network Lifecycle: Seven Stages....80
8.4 OATS Network Policies....80
8.5 Beckn + Verifiable Credentials: Trust Layer Design....81
8.10 Cross-Network Traceability: Multi-Domain Beckn Flows....82

9. Blockchain and Distributed Ledger Integration....85
9.1 The Role of Blockchain in Traceability DPI: Principles and Boundaries....85
9.2 Decision Framework: When to Use DLT vs Traditional Database....86
9.3 Mapping DLT to the OATS Five-Layer Architecture....88
9.4 Permissioned DLT Architectures: Hyperledger Fabric and Hyperledger Besu....88
9.5 IOTA Tangle and Feeless IoT-Native Anchoring....88
9.6 W3C Verifiable Credentials Anchored on DLT....88
9.7 Smart Contracts for automated Compliance and Recall Orchestration....88
9.8 Governance of Shared Ledgers: Consortium Models and Node Roles....88

10. OATS API Architecture, Microservices, and Integration Framework....89

11. Data Governance Architecture and Federated Data Model....93
11.1 OATS Data Governance Philosophy: Federated, Sovereign, Auditable....94
11.2 Data Mesh Architecture for Agri-Food Traceability....94
11. 3-Tiered Data Access Model: Open, Shared and Restricted Tiers....97
11.4 DEPA Aligned Consent Architecture....98
11.5 Cross-Jurisdiction Data Flow Governance....100
11.6 Data Quality Standards and Audit Trail Requirements....100
11.7 Data Retention, Archival and Right to Erasure....101
.... 101

12. OATS Consent management System....103
12.1 DPDPA 2023 Consent requirements and OATS Alignment....103
12.2 The ORGANS Framework:....103
12.3 Consent Manager Architecture and Registration....104

13. Regulatory Compliance Framework and Legal Architecture....105

13.1 GI Tag and Protected Designation of Origin....105
13.2 Organic Certification Legal Framework: NPOP, NOP, EU Organic....106
....106

14. Cybersecurity, Privacy and Data Protection Architecture....107
14.1 OATS Security Architecture: Zero-Trust by Design....107
14.2 Identity and Access Management: Role-Based and Attribute Based....110
14.3 Key management and PKI Architecture....111
....111
14.4 Audit Logging and Non-Repudiation....111
14.5 Data Protection Impact Assessment (DPIA) Framework....111

15. Consumer Transparency and Market Access....115
15.1 Consumer Transparency: The Right to Know....115
15.2 GS1 Digital Link QR Code Consumer Journey Design....116
....117
15.3 SmartLabel and Open Food Facts Integration....117
15.4 Premium Market Access: GI, Organic and Fair-Trade Value Premiums....118
15.5 ONDC and D2C Commerce Integration for GI Products....119
15.6 Consumer Grievance and Product Feedback Mechanisms....120

16. Financial Inclusion and Value Chain Finance Module....121
16.1 Digital Credit Scoring from Supply chain Event data....122
16.2 Supply Chain Finance: Invoice Discounting and Factoring....123
16.3 Smart Contract Payment Triggers at Delivery Milestones....124
16.4 CBC and DBT Integration for Direct Benefit Transfer....125
16.5 Crop Insurance Integration with Traceability Events....125
16.6 Warehouse Receipt Finance: Integration with eNAM and WDRA....126
16.7 Gender-Responsive Finance Design for Women Farmer....127
16.8 Financial Sustainability and Private sector Participation....127
16.9 Integration with Bharat Trade Net (BTN): India's Trade Documentation and Financing DPI....129

APPENDICES & REFERENCES....131

APPENDIX A - CONSOLIDATED FRS / SRS COMPACT MATRIX....131
A.1 Conformance Tier Framework....131
A.2 Functional Requirement Specifications (FRS)....131
A.3 System Requirement Specifications (SRS)....136

APPENDIX B — STANDARDS INDEX AND REFERENCES....143

APPENDIX C — SCHEMA AND API REFERENCE INDEX....149
....150

Executive Summary

1. The Imperative

Investing in population-scale food traceability is no longer a technology choice; it is a public-policy obligation. It safeguards public health, defends export competitiveness, and upholds every citizen's right to safe, verifiable food. The **World Bank (2018)** estimate, updated by the joint **WHO–WBG Technical Review (February 2025)**, places the cost of unsafe food in low- and middle-income countries at **USD 110 billion per year** in lost productivity and medical expense. The **IFC–WHO 2024 report** estimates that scaled foodborne-disease surveillance could prevent up to **19 million illnesses annually**.

Three regulatory currents are simultaneously making digital traceability mandatory: in the EU — **Regulation 178/2002 (Article 18)**, Farm-to-Fork (2020), **EUDR 2023/1115**, and the forthcoming **Digital Product Passport under ESPR 2024/1781**; in the United States, **FSMA Section 204** requires a 24-hour traceability response; and global data-protection regimes (DPDPA 2023, GDPR, and equivalents) make the lawfulness of data handling as material as the data itself.

For export-dependent economies, the cost of inaction is already visible. India exported **USD 48.9 billion** of agricultural and allied goods in FY 2023-24 (APEDA); yet **2–8% of shipments are rejected or detained at EU ports and 3–6% at US ports** — predominantly for traceability gaps, residue evidence, or certificate-of-origin failures. Solving this through a patchwork of proprietary vendor solutions is fiscally and architecturally unviable at national scale. Traceability must be treated as **Digital Public Infrastructure (DPI)**: an open, interoperable, sovereign-governed shared utility.

2. What OATS Is — and What It Is Not

The **Open AgriTrace Stack (OATS)** is a jurisdiction-neutral, vendor-neutral, technology-neutral *reference architecture* for food-traceability DPI, published as a global public good under **CC BY 4.0**. Every specification, identifier scheme, event schema, conformance level, and governance instrument is structured to function in any regulatory context, at any level of digital maturity, and across any agri-food value chain. The Indian DPI ecosystem — India Stack, AgriStack, the Beckn-powered ONDC, BharatVISTAAR, MahaVISTAAR, MahaAGX, and APEDA traceability systems — is used throughout as an illustrative good-practice model, drawing on global precedents from the EU, the United States, Brazil, Australia, and the Republic of Korea.

OATS is a **modular composition** of specifications, frameworks, standards mappings, and implementation guidance from which any government, multilateral, or implementing consortium may select the modules relevant to its context. It is not a product, not a platform, and not a single vendor's stack.

3. Vision, Mission and Strategic Objectives

Vision: A globally interoperable, open, and inclusive agri-food traceability infrastructure that protects consumers, enables sovereign data governance, and unlocks premium market access for producers of every scale.

Mission: Operationalise the public right to safe, verifiable food at population scale by binding identity, event, certification, consent, and commerce primitives into a single open protocol stack.

Strategic objectives:

- Achieve population-scale coverage — usable by feature-phone smallholders in low-connectivity areas and by enterprise ERP processors alike.
- Satisfy major export-market regulations through a single integrated chain (EU 178/2002, EUDR, FSMA 204, GDST, UFLPA, BCI), eliminating duplicate parallel submissions.
- Establish sovereign data governance compliant with DPDPA 2023, GDPR, and federated data-residency rules.
- Unlock premium market access for smallholders through verified, machine-readable provenance; compress recall-response time from days to hours via live event streams to regulators.
- Convert verified event chains into collateral-grade evidence for Kisan Credit Card, PMFBY, and supply-chain finance.

- Maintain technology neutrality and prevent vendor lock-in through open standards, modular adoption, and a protocol-not-platform discipline; reusable under CC BY 4.0 without licence.

4. Design Philosophy

OATS is anchored in five non-negotiable design tenets, synthesised from eight external framework families — the G20 DPI Declaration (DEWG, India Presidency 2023), GovStack v2.0, CDPI, InDEA 2.0, OECD & GDS, DPDPA 2023, GFTC, and ISO 22005:2007 with Codex CAC/GL 60-2006 — and codified into **20 OATS P-Principles** grouped in four categories, each translated to an enforceable design rule and an explicit anti-pattern.

- **Open by Default —** no proprietary identifier, schema, or protocol is permitted at any registry layer.
- **Federated by Architecture —** data remains at source nodes, referenced rather than centralised.
- **Sovereign by Design —** the Data Principal (farmer, FPO, exporter) is always at the centre; consent rests in human hands.
- **Inclusive by Architecture —** feature phones, USSD, offline-first capture, and vernacular voice are first-class participants.
- **Trustworthy by Construction —** transparent, layered mechanisms (identity, event integrity, claim verification, DLT-anchored evidence for high-value claims).

5. Reference Architecture — the 5+1 Layer Hourglass

OATS specifies a five-layer DPI architecture with an explicit **hourglass waist**, plus a +1 augmentation layer. All sectors, actors, commodities, and regulators pass through a single shared protocol layer (Layer 2) — **GS1 EPCIS 2.0 (ISO/IEC 19987:2024)** — so that one cotton bale, one turmeric lot, and one shrimp consignment are interoperable on the same rails.

Layer	Function	Canonical Building Blocks
L1 — Identity, Trust, Registry	Authoritative identity for actors, locations, lots, devices, certifiers.	GS1 GLN / GTIN / SSCC; W3C DID Core v1.0; W3C VC 2.0; AgriStack / MOSIP linkage; Status List 2021.
L2 — Events & Anchoring (waist)	Single shared event protocol; selective DLT anchoring for high-value claims.	GS1 EPCIS 2.0 (ISO/IEC 19987:2024); GS1 CBV 2.0; GS1 Digital Link; Hyperledger Fabric v2.5.
L3 — Open Protocols	Decentralised commerce and traceability discovery.	Beckn Open Specification; OATS-Beckn Interface; ONDC / VISTAAR / MahaVISTAAR networks.
L4 — Consent & Governance	Sovereign consent, federation, audit, dispute resolution.	DEPA Account Aggregator (FIP/FIU); ORGANS principles; consent artefacts; Network Policies NP-01 to NP-11.
L5 — Applications	Consumer transparency, export compliance, regulator portals, finance.	Brand QR; APEDA / FSSAI / DGFT integrations; ERP/TMS connectors; D2C corridors.
+1 — AI / ML Intelligence	Probabilistic augmentation; risk scoring; anomaly detection.	Intelligence Events (versioned, explainable, contestable); satellite phenology; mass-balance fraud detection.

6. Three Deployment Frameworks

All three are commodity-agnostic and converge on the same Layer-2 EPCIS waist:

- **Greenfield National Deployment —** a complete L1–L5 stack deployed by a sovereign or sub-sovereign government with no incumbent traceability infrastructure.
- **Brownfield Augmentation —** selected modules integrate with existing AgriStack, NABL, APEDA, FSSAI, and ERP/TMS investments; OATS rides on top without replacing them.
- **Sectoral Vertical —** a single commodity (cotton, soybean, coffee, shrimp) deployed against a specific regulatory anchor (EUDR, BCI, GDST, NPOP). The same Blueprint serves a Maharashtra-scale pilot and a multi-country regional bloc.

7. Identity, Trust and Chain of Custody

Every person and organisation in OATS carries a globally unique, persistent, standards-based identifier. Farmers and FPOs anchor to **AgriStack / MOSIP**; locations carry GS1 GLNs; products carry GTINs; lots carry LGTINs and SSCCs. Certifications are issued not as PDFs but as **W3C Verifiable Credentials** held in wallets controlled by the human actors themselves, with hash anchors on a Hyperledger Fabric governance channel. Chain of custody is captured as signed, timestamped EPCIS 2.0 events through **10 Critical Tracking Events (CTE-01 to CTE-10)**, a 45-element Key-Data-Element matrix, and a Birth-of-Lot Principle that prevents silent merging, unrecorded splitting, or unattested transformation.

8. Physical–Digital Linkage and the Smallholder Bridge

A digital event chain has no value unless it is unambiguously tied to the physical lot. The carrier stack — **GS1 Digital Link QR** (the GS1 Sunrise 2027 default), Data Matrix for small-format packaging, RFID for high-throughput logistics, and NFC for consumer-tap — is paired with a **smallholder bridge**: mobile-first, offline-capable capture, device-bound keys, and USSD fallback for feature phones.

9. Open Network and Selective DLT Anchoring

OATS does not invent a new commerce protocol. The **Beckn Protocol**, operating at population scale through ONDC and MahaVISTAAR, is the parent: every OATS message is a syntactically valid Beckn message. Blockchain is *not* the default data store — routine events remain in scalable EPCIS repositories, while only high-value, compliance-critical events (certification issuance, cross-border attestations) are cryptographically anchored on Hyperledger Fabric. Fabric, Besu, IOTA, and CORD are evaluated against deployment-context fitness with explicit decision criteria.

10. APIs, Federation and the Intelligence Layer (+1)

The API surface is **REST-first, OpenAPI 3.1**; federated exchange uses the GovStack Information Mediator (X-Road) pattern so data remains at source. The **+1 Intelligence Layer** consumes standardised L2/L3 inputs to generate risk signals — mass-balance fraud detection, satellite phenology, residue outliers, complaint clusters — that feed back as Intelligence Events. Every output is versioned, explainable, auditable, and contestable; it augments but never overrides the canonical record.

11. Federated Governance, Consent and Compliance by Architecture

OATS is a federated **data mesh**. Three access regimes apply: **Open** (public-good data), **Shared** (peer-to-peer with consent), and **Restricted** (personal or commercially sensitive under explicit licence). Consent is a system-level control, not an application feature: no personal data enters the event chain without a valid consent artefact or lawful basis, governed by the **DEPA AA FIP/FIU** pattern and **ORGANS** principles. Compliance is delivered *by architecture*: EU due-diligence statements, FSMA 204 submissions, GI

attestations, phytosanitary VCs, NPOP transaction certificates, and export certificates are auto-derived from canonical Layer-2 events.

12. Cybersecurity and Privacy by Construction

OATS security is **zero-trust by design**. Every API call, credential retrieval, and event submission is authenticated (DID-based), authorised (RBAC + ABAC), and cryptographically validated. **Selective-disclosure VCs (BBS+ signatures)** allow a farmer to prove EUDR-compliant geo-coordinates to a regulator without exposing them to the buyer. Population-scale Significant Data Fiduciary (SDF) obligations are codified as Network Policies binding any operator handling personal data of millions of farmers.

13. Onboarding, Certifications and the Digital Sentinel

OATS specifies a streamlined **single-API onboarding** for all participants — farmers, exporters, operators — linking directly to trusted registries (AgriStack, MahaAGX). Each step generates a tamper-evident, verifiable event. Certifications across NPOP, NOP, GLOBALG.A.P., and equivalents are upgraded to **W3C VCs with a six-state lifecycle**; every state change triggers an EPCIS event anchored on the Fabric governance channel. HACCP is transformed into a **Digital Sentinel System**: every Critical Control Point becomes event-driven and regulator-visible, shifting the regulator from after-the-fact auditor to an active system subscriber.

14. Consumer Transparency and Premium Market Access

The consumer-side promise is codified as a **Four-Pillar Disclosure Model**: Origin & Provenance; Certifications & Quality; Handling & Journey; and Food-Safety & Alerts — surfaced via GS1 Digital Link QR with a progressive-disclosure UI conforming to **WCAG 2.2 Level AA**. Five premium categories share a single credential-stack architecture: GI, Organic (NPOP / EU / NOP), Fair Trade, Sustainability (Rainforest Alliance, BCI, EUDR), and ODOP — each anchored by a core W3C VC and geo-verified where applicable.

15. Financial Inclusion and the Value-Chain Finance Layer

OATS treats the event chain as **collateral-grade evidence**. A smallholder's farming activity — seeding, area, inputs, yield, lot sold, price received, warehouse tonnage, invoices against registered buyers — becomes a verifiable, tamper-evident, machine-readable history rather than a stack of unverifiable affidavits. Four financial primitives derive directly: an **Agri-Credit Score**; supply-chain finance via co-signed **Invoice VCs**; smart-contract milestone escrow against verified custody events; and DBT–CBDC integration patterns.

16. The Call to Action

OATS is offered as a public good to every government, multilateral, standards body, and implementing consortium working to build food systems in which traceability is universal, trust is built into the architecture, and the farmer at the origin of every value chain stands to ***benefit, but is never asked to bear the cost***. The Blueprint is jurisdiction-, vendor-, and technology-neutral, and published under **CC BY 4.0** so that any jurisdiction may adopt, adapt, translate, or extend it without permission, licence fees, or single-steward alignment. The remainder of this document operationalises this vision into a coherent, deployable architecture.

PART I

STRATEGIC RATIONALE & POLICY FOUNDATIONS

- *The case for traceability as DPI - vision, mission, and strategic objectives of OATS*
- *The OATS Unified Principles Framework - governance values, ethics, and anti-patterns to reject*
- *The OATS design philosophy - Open, Federated, Sovereign, Inclusive, Trustworthy*
- *8-tier stakeholder ecosystem - from sovereign architects to consumers*
- *The Pre-Export Verification Certificate (PEVC) and the six-stage Port-of-Entry validation workflow*
- *The OATS Multi-Stakeholder Governance Council - composition, mandate, voting rules*



1. Vision, Mission, and Strategic Framework

1.1 Definitions

1.1.1 Traceability

Traceability (Authoritative Definition ISO 22005:2007 and Codex CAC/GL 60-2006)

The ability to follow the movement of a food through specified stage(s) of production, processing, and distribution. In the feed and food chain, traceability encompasses the ability to trace and follow a food, feed, food-producing animal or substance intended to be, or expected to be, incorporated into a food or feed, through all stages of production, processing and distribution.[1]

Traceability is a multidimensional concept encompassing three operational planes, each of which must be addressed within any population-scale DPI implementation:

- **Internal Traceability:** The capacity of a single enterprise to trace the flow of goods and information within its own operations linking inputs received, processing steps performed, and outputs dispatched. This represents the minimum operational requirement for compliance with ISO 22005:2007 and forms the foundational data collection layer of OATS.
- **Chain Traceability:** The capacity to link internal traceability systems across multiple enterprises along a value chain enabling 'one step forward, one step backward' product tracing as mandated by Codex CAC/GL 60-2006 and EU Regulation (EC) No 178/2002, Article 18. Chain traceability is the primary level of regulatory compliance in most jurisdictions.
- **Full Supply Chain Traceability:** End-to-end visibility from the point of primary production (farm gate, aquaculture pond, livestock holding) through all processing, transformation, logistics, and distribution stages to the point of consumption. This is the aspirational standard of GS1's Global Traceability Standard 2.0 and the population-scale operational target of OATS.

1.1.2 Digital Public Infrastructure (DPI)

Digital Public Infrastructure

Systems that serve as foundational, digital building blocks for public benefit. Systems built as DPI can comprise a variety of digital software, platforms, APIs, and services, along with their related legal and regulatory frameworks, standards, policies, and processes.[2]

Public denotes public benefit, not government ownership. The G20 DEWG (August 2023) established eight DPI principles (inclusivity, interoperability, modularity and extensibility, scalability, security and privacy, collaboration, governance for public benefit, and grievance redressal).

[1] ISO 22005:2007, Clause 3.8 | Codex Alimentarius CAC/GL 60-2006 (Principles for Traceability/Product Tracing)

[2] World Bank, 'Digital Public Infrastructure and Development: A World Bank Group Approach,' Digital Transformation White Paper, Volume 1, March 2025

1.1.3 Open Stack

Open Stack (OATS Contextual Definition)

A composition of software components, protocols, APIs, data standards, and governance frameworks in which all interface specifications are publicly available, no single vendor controls critical interoperability points, and any compliant implementation may participate in the network regardless of the underlying technology choices made by individual actors.[3]

Three dimensions: open specifications (GS1 EPCIS 2.0, GS1 Digital Link, W3C VC, W3C DID, Beckn, GovStack), **open access** (no central gatekeeper or prohibitive access fees), **open governance** (multi-stakeholder process; no single government, corporation, or vendor holds unilateral control — mirroring IETF, W3C, GS1, DPGA governance models).

1.1.4 India Enterprise Architecture (IndEA / InDEA 2.0)

India Enterprise Architecture (Official Definition - NeGD / MeitY, 2023)

IndEA provides a generic framework, based on The Open Group Architecture Framework (TOGAF), comprising a set of architecture reference models that can be converted into a Whole-of-Government Architecture for India, Ministries, States, and Government Agencies. The framework is based on a federated architecture approach and recognizes the need to accommodate both greenfield and brownfield e-Governance initiatives. India Digital Ecosystem Architecture (InDEA) 2.0 harmonizes and builds upon prior frameworks, recommending a value-driven approach, a focus on capability building, and above all a preference for enabling rather than building.[4]

1.1.5 Additional Foundational Definitions

The following terms are defined here to avoid ambiguity throughout the Blueprint:

Critical Tracking Event (CTE)

A specific point in the supply chain at which traceability data must be captured such as harvesting, packing, shipping, receiving, or transformation. CTEs are the operational units of traceability, mandated under FSMA Section 204 (USA) and mapped to GS1 EPCIS 2.0 event types in Chapter 6.[5]

Key Data Element (KDE)

A specific piece of information that must be recorded and maintained at each Critical Tracking Event. KDEs include identifiers (Traceability Lot Code, location identifiers), dates, quantities, and reference documents. Specific KDEs required vary by CTE and regulatory jurisdiction.[6]

[3] Derived from: DPGA Digital Public Goods Standard v1.0 (2020) | CDPI Architecture Principles | GovStack Building Block Specifications | Open-Source Initiative (OSI) definitions

[4] National e-Governance Division (NeGD), Ministry of Electronics and Information Technology (MeitY), Government of India. InDEA 2.0 Framework Document (2023).

[5] GS1 Global Traceability Standard 2.0 | FDA FSMA 204 Final Rule (87 FR 70910, November 2022)

[6] GS1 Global Traceability Standard 2.0 | FDA FSMA 204 | EU Regulation (EC) No 178/2002

Digital Public Good (DPG)

Open-source software, open data, open AI models, open standards, or open content that adhere to privacy and other applicable international and domestic laws, standards, and best practices, and do no harm by design.

Verifiable Credential (VC)

A tamper-evident, cryptographically verifiable digital representation of claims made by an issuer about a subject. In OATS, VCs represent certifications (organic, GI tag, GLOBALG.A.P.), compliance attestations, and chain of custody proofs, enabling portable, cross-platform trust without requiring a central verification authority.[7]

Data Fiduciary

Under India's Digital Personal Data Protection Act 2023 (DPDPA 2023), any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data. A Significant Data Fiduciary (SDF) is one whose processing is likely to pose high risk owing to volume, sensitivity, national security implications, or systemic risk to the rights of data principals. Equivalent concepts exist under GDPR (Data Controller) and other national data protection frameworks.[8]

1.2 The Global Food Safety and Traceability Imperative

The decision to invest in population-scale food traceability DPI is not a technology choice. It is a public health imperative, an economic necessity, a trade competitiveness obligation, and an expression of a state's commitment to the fundamental right of its citizens to safe food. This section establishes the evidence base for that investment case across four dimensions.

WHO FERG 2015 baseline: The global burden of foodborne disease demands systemic, infrastructure-level response. The WHO's landmark global burden (FERG 2015) estimates, the following baseline statistics[9]:

600M	**420K**	**33M**	**200+**
People fall ill from unsafe food annually	Premature deaths per year	Disability-Adjusted Life Years (DALYs) lost	Diseases caused by unsafe food

The WHO Global Strategy for Food Safety 2022-2030 (adopted 75th WHA, May 2022) positions traceability as a core instrument of national food safety systems.

Economic dimension: Unsafe food costs LMIC economies **USD 110 billion annually** in lost productivity and medical expenses. IFC-WHO (2024) investment case: investments in foodborne disease surveillance could avert up to 19 million illnesses, prevent 13,092 premature deaths, and

[7] W3C Verifiable Credentials Data Model v2.0, W3C Recommendation, May 2025

[8] Digital Personal Data Protection Act 2023, Section 2(i) and Section 10, MeitY, Government of India | GDPR Article 4(7), European Parliament and Council, 2016

[9] WHO GERG 2025 Baseline

generate USD 23 billion in health benefits across 17 countries over a decade at a total cost of USD 492 million — ROI ratio approximately 47:1. US recall costs total USD 7 billion annually. EU food fraud is estimated at EUR 30-40 billion annually by the European Parliament.

Trade and market access dimension: Three concurrent regulatory movements drive global traceability convergence: (i) **EU regulatory architecture** — Regulation (EC) 178/2002 Article 18 mandates one-up-one-down traceability for all food businesses operating in or exporting to the EU; EU Farm to Fork (2020) and EU Digital Product Passport (ESPR) progressively intensify requirements; (ii) **USA FSMA §204** — FDA Food Traceability Final Rule (87 FR 70910, November 2022; revised compliance deadline July 2028) mandates electronic lot-level traceability records for high-risk foods, with FDA authorised to demand records within 24 hours; (iii) **emerging global frameworks** — Japan's Food Labelling Act, Australia's NLIS, Canada's Safe Food for Canadians Act, Saudi FDA traceability requirements. For export-dependent agricultural economies, the absence of national food traceability DPI constitutes a structural trade-competitiveness deficit. Digital traceability with cryptographic verification — as provided by OATS's W3C VC architecture — is the most effective systemic deterrent against high-value-category fraud (organic, GI, premium origin).

1.3 Why Traceability Must Be Digital Public Infrastructure (DPI)

Proprietary traceability platforms are architecturally incapable of serving a multi-stakeholder, multi-jurisdiction, multi-scale food supply chain: interoperability requires expensive bilateral integration; data sovereignty is compromised; network effects are captured privately; recall response averages 5–6 weeks; smallholders are excluded. DPI repositions foundational components (identifiers, registries, event exchange, consent management) as shared, open, public utilities, analogous to the internet (shared communication protocol), mobile telephony (shared spectrum/numbering), and payment rails (shared clearing).

Proprietary Platforms	DPI (OATS)
Each participant pays individually for integration	Integration cost socialised; shared once, used by all
Interoperability requires bilateral negotiation and custom code	Interoperability guaranteed by open protocol specifications
Recall response depends on voluntary competitor data sharing	Recall accesses a common event ledger within hours, not weeks
Smallholder farmers excluded by cost and technical complexity	Farmers participate via low-cost, offline-capable mobile interfaces
Data sovereignty rests with platform operators	Data sovereignty rests with the data principal; consent is sovereign
Network effects benefit the platform owner	Network effects benefit the entire supply chain ecosystem
Regulators must negotiate access to private databases	Regulators access traceability data through standard public interfaces
International interoperability requires complex bilateral agreements	International interoperability enabled by shared open standards
Switching platforms requires full data migration and re-integration	No lock-in; any OATS-compliant application can read and write to the shared layer
Innovation is gated by the platform owner's roadmap and API policies	Innovation is permissionless; anyone can build on open protocols
Governance decisions made by platform shareholders for commercial return	Governance is multi-stakeholder, public-interest, principle-bound

Audit trails controlled and editable by the platform operator	Audit trails are immutable, timestamped, cryptographically verifiable
License fees, per-transaction charges, upgrade costs compound over time	Marginal cost of participation approaches zero as the network scales
Separate platform required for each commodity or sector	Single protocol framework adaptable across commodities (cotton, coffee, paddy, dairy)
Deforestation checks run by individual buyers, often overlapping and duplicative	Shared GeoJSON polygon registry with jurisdiction-wide deforestation monitoring
Carbon credits tied to proprietary MRV systems; farmers rarely see the revenue	dMRV built into the protocol; credits traceable to farm, revenue shareable with the data principal

1.4 The OATS Design Philosophy: Open, Federated, Sovereign

The **Open AgriTrace Stack (OATS)** is designed from five foundational philosophical commitments that permeate every technical, governance, and implementation decision in this Blueprint. These commitments are not aspirational values; they are hard design constraints that must be satisfied by any implementation claiming OATS conformance.

1.4.1 Open by Default

Every interface specification, data model, API contract, governance rule, and protocol definition is publicly available, royalty-free, implementable by any party. 'Open by default' applies to the *infrastructure layer*.

1.4.2 Federated by Architecture

- **Data federation:** events generated and owned at source, retained in custody of the generating actor; OATS Core stores routing, identifiers, ACLs;
- **Governance federation**: national standards plus subnational implementation autonomy;
- **Infrastructure federation** — each state or country operates its own OATS node, connected through shared open protocols. No single jurisdiction's decisions can disrupt another's operations.

1.4.3 Sovereign by Design

- **Data sovereignty**: Personal, commercial, and strategic data remains under the relevant sovereign's jurisdiction; cross-border transfers require bilateral legal agreement;
- **Technology sovereignty**: Any component replaceable at any layer by any conformant alternative implementation without losing interoperability;
- **Governance sovereignty** — international interoperability through bilateral or multilateral treaty frameworks (Chapter 28), not subordination to a central global authority.

1.4.4 Inclusive by Architecture

Inclusion encoded as technical constraints, not aspirational goals: offline-first operation; voice, USSD, and multilingual interfaces; **zero participation cost for smallholder farmers at point of use**; onboarding workflows that accommodate actors without formal business registration through national ID systems (Aadhaar, MOSIP, civil registration) or community-level verification.

1.4.5 Trustworthy by Construction

Trust constructed at four levels: **identity trust** (cryptographically verified actor identity via GS1 GLN + W3C DID; impersonation detectable); **event integrity** (every event timestamped, digitally signed by the reporting actor, immutable once submitted; DLT-anchored for high-value claims); **claim verifiability** (certifications, GI, organic, fair-trade as W3C VCs; cryptographic verification without trusting the intermediary); **audit transparency** (all data access logged in an immutable audit trail satisfying DPDPA 2023, GDPR, FSMA 204 non-repudiation).

1.5 Strategic Alignment with Global Frameworks

- **SDGs.** Primary contributions to six: SDG 1 (No Poverty), SDG 2 (Zero Hunger), SDG 3 (Good Health), SDG 8 (Decent Work and Economic Growth), SDG 12 (Responsible Consumption), SDG 17 (Partnerships).
- **G20 DPI Consensus Principles (August 2023).** Eight principles endorsed by all G20 members under India's G20 Presidency: Inclusivity, Interoperability, Modularity and Extensibility, Scalability, Security and Privacy, Collaboration, Governance for Public Benefit, Grievance Redressal.
- **Codex Alimentarius and WTO SPS Agreement.** Codex CAC/GL 60-2006 (joint FAO/WHO) provides the normative legal foundation for OATS. Codex standards are recognised under the **WTO SPS Agreement (1994)** as the international reference point for food safety

2. Principles, Design Tenets, and Governance Values

2.1 Introduction

OATS is governed by eight framework families of principles — G20, GovStack), CDPI, InDEA 2.0, OECD and GDS , DPDPA 2023 GFTC , and ISO 22005:2007 with Codex CAC/GL 60-2006 (§2.9). These are synthesised into the OATS Unified Principles Framework (20 P-principles in four categories) which is the normative baseline against which any OATS conformant implementation is evaluated.



The OATS Unified Principles Framework

The eight framework families above collectively define the normative foundation. This section synthesises those individual principles into a consolidated framework of 20 OATS principles in four categories. These 20 are the primary design authority for all OATS specifications and the normative baseline for any OATS-conformant implementation. Source attributions identify the framework provenance of each.

OATS Unified Principles Framework

Category I: Architecture Principles (8 Principles)

Code	Principle
P-1	**Open by Default:** All OATS interface specifications, data models, governance rules, and protocol definitions are publicly available, royalty-free, and implementable by any party without restriction.
P-2	**Federated and Decentralized:** Data stays where it is collected. Central OATS infrastructure maintains routing, identifiers, and access control; does not hold copies of supply chain data.
P-3	**Modular and Composable:** OATS components are independently deployable, replaceable, and composable. No module creates dependencies that prevent other modules from functioning.
P-4	**Interoperable by Specification:** All inter-component communication through published open standards. No proprietary protocol or format at any interoperability boundary.
P-5	**Scalable from Corridor to Continent:** Architecture supports operation from single commodity corridors to national population-scale systems without redesign.
P-6	**Security and Privacy by Design:** Controls embedded at the first design decision, not added as compliance layers after deployment.
P-7	**Technology Sovereignty:** Any OATS component may be replaced by any alternative compliant implementation without losing interoperability. Government retains the right to replace any vendor at any time.
P-8	**API-First Design:** Every OATS function is exposed as a documented, stable API before being embedded in any user interface.

Category II: Data Governance Principles (5 Principles)

Code	Principle
P-9	**Lawful Purpose and Explicit Consent** : Personal data processed only for specific, lawful purposes with free, specific, informed, unconditional, and unequivocal consent.
P-10	**Data Minimisation and Purpose Limitation:** Only data strictly necessary for the specified function is collected. Data collected for one purpose may not be used for another without separate consent.
P-11	**Data Sovereignty:** Supply chain actors own and control the data they generate. Consent architecture enables data sharing without transferring ownership.
P-12	**Storage Limitation and Data Lifecycle Management:** Data retained only for the period required by the specified purpose or applicable regulatory mandate. Automated lifecycle management enforces this at the architecture level.
P-13	**Accountability and Rights:** Every data principal has enforceable rights to access, correct, port, and erase their personal data. Every data fiduciary is accountable for compliance with all data governance obligations.

Category III: Traceability Practice Principles (4 Principles)

Code	Principle
P-14	**End-to-End by Design: T**raceability spans the full supply chain from primary production to consumer, regardless of the number of organisational or jurisdictional boundaries crossed.
P-15	**Event-Based Data Model:** Traceability captured as a structured stream of events using the CTEKDE framework, implemented through GS1 EPCIS 2.0. No static inventory snapshot or document based traceability is OATS conformant.
P-16	**Proportionate and Risk-Based:** Traceability granularity and mandatory participation thresholds calibrated to documented food safety risk levels; not applied uniformly across all products and actors.
P-17	**Verifiable and Auditable:** All traceability claims verifiable through audit, inspection, or automated testing. Cryptographic verification through W3C Verifiable Credentials provides the highest assurance level.

Category IV: Governance and Inclusion Principles (3 Principles)

Code	Principle
P-18	**Inclusive by Architecture Not by Exception:** Inclusion of smallholder farmers, digitally excluded populations, and low-connectivity contexts is a hard architectural requirement, not an optional feature.
P-19	**Multi-Stakeholder Governance:** OATS governance exercised by a multi-stakeholder council; not controlled by any single government, vendor, or interest group.
P-20	**Continuous Improvement and Adaptive Learning:** OATS architecture, governance rules, and specifications continuously reviewed and improved based on operational evidence, stakeholder feedback, and evolving standards.

2.2 Governance Values and Ethics for Traceability DPI

- **Value 1: Primacy of Public Benefit.** Every OATS governance decision evaluated against impact on public benefit, specifically food safety, smallholder welfare, consumer access to safe food, and national food security. Commercial considerations are legitimate inputs to governance but may not override public benefit as the primary objective.
- **Value 2: Protection of the Vulnerable.** Explicit priority to actors with the least bargaining power — smallholder farmers, informal market operators, migrant workers in food processing, communities dependent on subsistence food systems. OATS must not be used as a tool to exclude, exploit, or disadvantage these populations.
- **Value 3: Transparency as Default.** Governance decisions, performance data, audit reports, and standards development processes are publicly available unless a specific, documented exception applies. Opacity in governance is a governance failure, not a security practice.
- **Value 4: Accountability Without Exception.** Every OATS operator, data fiduciary, and governance council member is accountable for their obligations under OATS governance rules and applicable law. No actor — including the government itself — is exempt from accountability for misuse of OATS infrastructure or data.
- **Value 5: Non-Harm by Design.** OATS is designed so that normal operation does not harm any supply chain actor. Farmer data must not enable unauthorised surveillance; traceability records must not be weaponised against farmers in debt recovery; consumer data must not be monetised without explicit consent. The UNDP DPI Safeguards "Do No Harm" principle is a foundational OATS design constraint.

2.3 OATS Anti-Patterns: Common Violations to Reject

Anti-patterns are recurrent design 'solutions' that appear reasonable in isolation but systematically violate OATS principles. The OATS governance council and procurement teams must explicitly identify and reject the following anti-patterns during system design, procurement evaluation, and conformance assessment:

Anti-Pattern (What to Reject)	Principle Violated and Correct Approach
'Traceability portal' a single government web application that all supply chain actors must use for data entry	Violates P-1 (Open), P-3 (Modular), P-5 (Scalable), P-7 (Tech Sovereignty). Correct: Publish open APIs and allow any certified application to submit events.
'Blockchain-first' mandatory blockchain for all traceability data regardless of use case	Violates P-3 (Modular), P-5 (Scalable), P-16 (Proportionate). Correct: Use blockchain only where multi-party trust and immutability requirements justify the cost.
'Proprietary QR code' QR codes that only resolve within the implementing vendor's ecosystem	Violates P-1 (Open), P-4 (Interoperable), P-7 (Tech Sovereignty). Correct: All QR codes must implement GS1 Digital Link URI standard.
'Farmer registration as data harvest' collecting extensive farmer PII at registration for future commercial use	Violates P-6 (Security/Privacy), P-9 (Consent), P-10 (Minimization), DP-1 and DP-3. Correct: Collect only minimum data required for entity identification.
'Centralized all-data repository' routing	Violates P-2 (Federated), P-11 (Data Sovereignty), CDPI

all supply chain event data through a central government database	C-4. Correct: Implement data mesh with federated storage and central metadata only.
'Excel-based KDE collection' collecting KDEs as spreadsheet submissions without structured event schema	Violates P-15 (Event-Based), GFTC GT-2. Correct: Mandate EPCIS 2.0 JSON event format with CSV as a transitional import format only.
'Compliance-only mindset' designing for minimum regulatory compliance without food safety utility	Violates P-14 (End-to-End), P-17 (Verifiable), Codex CA-1. Correct: Design for food safety emergency response as the primary use case.
'English-only interface' designing OATS interfaces in English without multilingual support	Violates P-18 (Inclusive), G20 P-1, GDS Principle 6. Correct: All farmer-facing interfaces must support vernacular languages and voice.

3. Stakeholder Ecosystem and Actor Mapping

3.1 Introduction and Actor Classification Framework

Tier	Actor Category	Primary OATS Relationship
1	Government Actors (Agriculture Dept, FSA, Customs, CIO, Finance, Export Promotion Bodies)	Sovereign architects and primary financiers: government is the primary stakeholder, not a peripheral regulator
2	Primary Supply Chain Actors (Individual Farmers, FPOs, Cooperatives)	First-mile data originators: their participation or non-participation determines OATS traceability completeness
3	Post-Harvest and Processing (Aggregators, Processors, Manufacturers)	Transformation event recorders: critical chain-continuity actors responsible for EPCIS Transformation Event capture
4	Logistics, Cold Chain, Distribution (Transporters, Cold Store Operators, Warehouses, Port Facilities)	Transport and storage event recorders: cold chain integrity data directly determines FSSAI risk profile at port of entry
5	Regulatory, Standards, Certification Bodies (FSSAI, APEDA, GS1, NABL, EU EFSA, US FDA, Codex)	Normative authority actors: define compliance rules, issue certifications, enforce standards
6	Technology Providers and AgriTech Ecosystem (SIs, App Developers, IoT Vendors, Certification Bodies)	Application and innovation layer: build on OATS open APIs under government-enabling, private-innovation-delivering model
7	DFIs and Donor Partners	Capital mobilisers and technical assistance providers: critical for early-stage DPI financing
8	Civil Society, Academia, Consumer Organisations (Farmer Orgs, Research Institutions, Consumer Bodies)	Accountability, innovation, and public benefit verification actors: independent monitors of OATS outcomes

3.1.1 (Tier 1) - Government Actors: The Sovereign Architects of OATS

Government occupies the central role across four dimensions no private actor can or should perform:
Primary Financier — CapEx and OpEx for the shared infrastructure layer that the private ecosystem builds upon;
Sovereign Architect — legal mandate, conformance standards, participation enforcement;

- **Data Validator** — only Agriculture Departments and Food Safety Authorities have the regulatory authority and institutional credibility to certify that OATS data is accurate, legally defensible, and recognised at destination ports;
- **DPI Steward** — long-term sustainability, security, and governance beyond any commercial investment cycle. The World Bank AgriConnect Senegal Compact (February 2026) validates this precisely: *"governance entrusted to the Ministry of Agriculture's Delivery Unit, with a joint steering committee for coordination."*

3.1.2 (Tiers 2 - 4) - Supply Chain Actors

- **Farmer:** Farmers are the first-mile originators of every traceability record in the agri-food value chain. They register in the system through a national digital identity at no cost and with no recurring fees and capture their harvest events through accessible interfaces including basic mobile applications, USSD codes on feature phones, and vernacular voice interfaces. Each harvested lot is labelled with a zero-cost QR code from the Farmer Onboarding Kit, and the resulting record becomes the foundation on which every downstream traceability claim rests. Farmer Producer Organisations and cooperatives extend this role at the collective level, pooling member harvests into shared lots, managing group certifications such as organic, GLOBALG.A.P., and Geographical Indication on behalf of their members, and providing each member with an individual record of their contribution. Across the farmer tier, one principle remains absolute: farmers retain control of their data, exercise consent over how it is shared, and never bear the cost of the infrastructure they make possible.

- **Processors:** Processors occupy the most technically demanding position in the traceability chain. Every processing operation, including sorting, grading, drying, milling, packaging, and blending, transforms input lots into output lots, and the accuracy of this transformation determines whether the upstream farmer record retains its value. Processors are therefore responsible for recording every transformation with complete fidelity, including the input lots consumed, the output lots produced, the process parameters applied, and the facility, date, and time of the operation. They are also responsible for managing chain-of-custody certifications as digitally verifiable credentials, maintaining records in a format that satisfies the regulatory requirements of destination markets such as the United States and the European Union, and applying globally interoperable QR codes to every outgoing unit so that downstream actors and consumers can verify provenance.

- **Logistics:** The logistics tier safeguards traceability integrity, custody continuity, and product quality during the movement and storage of agri-food products between value chain actors. Transporters by road, rail, and air record the dispatch and receipt of every lot, capture real-time location data, and capture environmental telemetry including temperature, humidity, and shock where the product class requires it. Cold chain operators maintain continuous cold chain integrity, trigger automated alerts to food safety regulators in the event of a breach, and issue cold chain compliance credentials linked to the lots under their custody. Accredited warehouse operators issue electronic warehouse receipts that embed the underlying lot identifiers, thereby linking traceability integrity to financial inclusion by allowing farmers and aggregators to access collateral-backed credit against the produce in storage. Ports, inland container depots, and export container facilities form the final domestic node in the chain, recording the loading of export consignments and verifying the export credential at the point of final container sealing, the last domestic checkpoint before the consignment enters international markets.

3.1.3 (Tier 5) - Regulatory, Standards, and Certification Bodies

Regulatory and standards bodies are the normative authority actors of OATS. They define the compliance rules within which OATS operates, issue the certifications that give OATS data legal standing at ports of entry and in courts of law, and enforce compliance through inspection, audit, and penalty. Their engagement with OATS is bidirectional: they consume OATS event data for risk-based regulatory decisions, and they produce certification and compliance data as OATS Verifiable Credentials.

3.1.4 Tier 6 - Technology Providers and AgriTech Ecosystem

Technology providers and the AgriTech ecosystem constitute the application and innovation layer of OATS. The foundational OATS design principle derived from InDEA 2.0's 'enabling rather than building' orientation, CDPI Principle 3 (Diverse and Inclusive Innovation via Open Access), and GDS Principle 8 (Build digital services, not websites) is that government builds and operates the OATS core infrastructure layer, while the private sector AgriTech ecosystem builds value-added applications and services on top of open OATS APIs. This division prevents government from crowding out private innovation, ensures competitive supply of farmer-facing and processor-facing applications, and keeps the infrastructure layer strictly technology-neutral.

3.1.5 (Tier 7) - Development Finance Institutions and Donor Partners

Development Finance Institutions and multilateral donors are the capital mobilization and technical assistance actors of OATS. Their engagement is critical in the early deployment stages, when the public goods nature of traceability DPI and the long gestation period before commercial returns materialize makes purely commercial financing insufficient. The World Bank's AgriConnect initiative (October 2025), committing to double agribusiness investment to USD 9 billion annually by 2030 with explicit prioritization of shared digital public goods including farmer registries and traceability infrastructure, provides the primary DFI financing channel for OATS globally.

3.1.8 (Tier 8) Civil Society, Academia, and Consumer Organizations

Civil society, academic, and consumer organizations perform the accountability, independent research, and public benefit verification functions that neither government nor industry can perform for themselves. They are essential for three OATS outcomes that cannot be achieved through procurement: independent monitoring of whether OATS genuinely serves smallholder farmer welfare and public health objectives; research and innovation that extends OATS capabilities beyond what budget-bound government can commission; and consumer-facing transparency that creates market demand for OATS participation from the demand side of the supply chain.

3.2 The Port-of-Entry Data Validation Nexus: Government as Certifier

The Central Problem OATS Solves is Export Consignment Rejection at Destination Ports. A single rejected container represents lost export revenue (typically USD 50,000 to USD 500,000 per container); demurrage and destination storage costs; return freight or destruction costs; damage to exporter's market credentials; potential loss of APEDA/commodity board registration; reputational damage affecting future consignments. The root cause in the majority of cases is not product quality failure but **documentation failure**: incomplete, inconsistent, or unverifiable traceability records that cannot satisfy the destination authority's electronic verification requirements. OATS eliminates documentation failure as a cause of rejection by creating a pre-verified, digitally signed, cryptographically tamper-evident composite traceability record — the **Pre-Export Verification Certificate (PEVC)**, that the destination authority can verify in seconds rather than days.

The port-of-entry validation nexus involves at minimum six actors: Agriculture Department (finances and operates OATS, mandates participation); Food Safety Authority (inspects and certifies); Customs Authority (links traceability to shipping documentation); Export Promotion Body (issues sector-specific certifications); Exporter (compiles and presents PEVC); Destination-Country Regulatory Authority (verifies and decides).

3.2.1 The Six-Stage Pre-Export Verification Workflow

Stage	Responsible Actor(s)	OATS Mechanism and Output
Stage 1: Continuous Chain-of-Custody Event Capture (Farm to Port Staging)	All supply chain actors SC-01 through SC-08	Real-time EPCIS 2.0 event capture at every CTE from harvest through processing, grading, cold storage, and port staging. Every event is cryptographically signed with the recording actor's OATS digital identity certificate and timestamped on the OATS event ledger. No event can be retrospectively altered without detection, as the event chain is hash-linked. Output: complete OATS event chain for the specific consignment lot.
Stage 2: Pre-Export KDE Completeness Verification (72 hours before loading)	Agriculture Department OATS Delivery Unit (automated API)	Automated OATS API check against the destination-country specific KDE profile for the commodity and market: are all required CTEs present? Are all required KDE fields populated? Are all certifications (organic, GAP, phytosanitary) valid and unexpired? A OATS Completeness Score (0-100) is computed and flagged to the exporter via OATS portal notification 72 hours before scheduled loading. Deficiencies are flagged with specific remediation guidance. Under the current system, food safety risk-profiling and inspection for agricultural import consignments at Indian ports takes up to 72 hours for standard-risk categories (FSSAI FICS operational baseline). OATS's pre-verified PEVC is designed to reduce this to under 4 hours by enabling Green Channel treatment for consignments with verified traceability records a processing time target consistent with SWIFT Single Window objectives for low-risk food consignments.
Stage 3: FSSAI Pre-Export Physical Inspection and NOC Issuance	Food Safety Authority (FSSAI Authorized Officer)	For export consignments: FSSAI Authorized Officer conducts risk-profile-based inspection (OATS Completeness Score >85 may qualify for documentation-only review without physical sampling for specified low-risk commodities). Upon satisfactory review, FSSAI Authorized Officer issues the Pre-Export NOC as a W3C Verifiable Credential, digitally signed with FSSAI's OATS X.509 certificate, anchored to the specific OATS Master Lot ID of the consignment.
Stage 4: Export Promotion Body Certification Issuance	DPPQS Plant Quarantine Officer (Phytosanitary Certificate) and APEDA / Commodity Board Authorized Officer (all other certifications)	This stage involves two parallel certification streams that must both complete before PEVC assembly: **Stream 4A DPPQS/NPPO:** A Plant Quarantine Officer at the designated Plant Quarantine Station conducts pre-export phytosanitary inspection of the consignment. Upon clearance, the Phytosanitary Certificate (PC) is issued via PQMS (Plant Quarantine Management System) and transmitted via the ePhyto Hub as a W3C Verifiable Credential cryptographically linked to the OATS Master Lot ID. **Stream 4B APEDA/Commodity Board:** APEDA or the relevant commodity board issues destination-country specific documents: Health Certificate (HC), Certificate of Origin (COO), Organic Certificate where applicable (via NPOP TraceNet), and GI Certificate where applicable each as a W3C Verifiable Credential linked to the OATS Master Lot ID. NABL-accredited laboratory test results for pesticide residues, heavy metals, and microbial parameters are also issued as Verifiable Credentials. Both streams must be complete before Stage 5 (PEVC automated assembly) can proceed.

Stage 5: OATS PEVC Automated Assembly and Digital Signing	OATS Platform (Agriculture Department operated)	OATS platform automatically assembles all Verifiable Credentials FSSAI NOC, APEDA certificates, cold chain compliance attestation from IoT sensor records, laboratory test results, entity verification records into the OATS Pre-Export Verification Certificate (PEVC). The PEVC is digitally signed by the Agriculture Department as the sovereign DPI operator, stored in the OATS event ledger, and rendered as a QR code embedded in the Shipping Bill.
Stage 6: Destination-Country Electronic Verification	Destination Regulatory Authority (EU EFSA TRACES NT, US FDA PREDICT, etc.)	Destination authority scans the PEVC QR code at import gate or reviews the pre-submitted PEVC via OATS API. The OATS Verification API returns the full structured PEVC in a format compliant with the destination system's import notification requirements. The authority's risk management system scores the consignment based on OATS completeness and certification status. OATS-verified consignments with score above defined threshold are directed to Green Channel (documentation review only, no physical inspection). Outcome: clearance within 4 hours vs. standard 72-hour baseline.

3.2.2 OATS Pre-Export Verification Certificate: Structure, Legal Standing, and Destination Integration

The OATS Pre-Export Verification Certificate (PEVC) is the terminal credential in a chained-issuance trust graph that runs the full length of the supply chain. Each credential in the chain is itself a W3C Verifiable Credential that cryptographically references its parent, producing a single verifiable graph rather than a bundle of parallel documents linked by a platform service. The graph runs from the Farm Foundational VC, to the Lot Declaration VC issued at the harvest event, to the Aggregation VC at the first pooling point, to a Processing VC where applicable, to the suite of Certification VCs (FSSAI NOC, APEDA, phytosanitary, NABL lab reports, organic, GI), to the Commercial Invoice VC at the export transaction, and terminates in the PEVC itself. The PEVC's legal standing derives from three sources: the single verifiable chain of co-signed VCs back to the sovereign root; the sovereign digital signature of the Agriculture Department as OATS DPI operator on the terminal PEVC; and the OATS event ledger's non-repudiable, hash-linked, timestamped record of every event in the chain. This makes the trust chain intrinsic to the document structure rather than gateway-mediated, and directly enables financial-services composability for invoice financing, trade credit, and warehouse receipt finance applications that require single-presentation verification of provenance and commercial commitment.

3.3 OATS Multi-Stakeholder Governance Council (OMGC): Composition and Mandate

The OATS Multi-Stakeholder Governance Council (OMGC) is proposed as the apex governance body of the OATS DPI ecosystem. Its design reflects G20 DPI Principles 6 and 7 that shared public infrastructure must be governed through multi-stakeholder collaboration, not controlled unilaterally by any single actor including government. The OMGC exercises governance authority over four decision categories that affect all ecosystem participants: changes to core data schemas and EPCIS event specifications; changes to conformance requirements and certification criteria; major architecture decisions affecting interoperability; and allocation of the OATS InnovEx Enhancement Fund. Day-to-day operational decisions are delegated to the Agriculture Department's OATS Delivery Unit and are not subject to OMGC deliberation.

3.4 Stakeholder Engagement Strategy and Implementation Sequencing

Stakeholder engagement in OATS is a design prerequisite, not a communication activity appended to implementation. The research literature on digital traceability systems consistently identifies stakeholder resistance particularly from smallholder farmers, who face data capture burden without visible short-term benefit, and from SME processors, who perceive compliance costs exceeding benefits as the primary cause of traceability system failure after technically successful deployment. OATS's engagement strategy is structured around three implementation phases.

Phase	Timeframe and Focus	Key Activities by Actor Category
Phase 1: Foundation and Co-Design	Months -18 to -6 before first deployment (18 months pre-launch)	**Government:** Convene OMGC founding session; establish Agriculture Department Delivery Unit; secure multi-year OATS budget commitment; issue legal mandate notification with 24-month implementation grace period. Farmers and FPOs: Conduct ethnographic user research with farmer cohorts in 3 target commodity corridors; co-design farmer registration flow and harvest CTE interface in vernacular language with iterative prototype testing; pilot with 5 to 10 self-selected FPOs. Technology Providers: Publish OATS API specifications 12 months before compliance deadline; open OATS Certification Programme; populate OATS Vendor Registry. DFI Partners: Conduct World Bank-aligned OATS DPI Readiness Assessment (Chapter 22); submit Project Concept Note for DFI co-financing.
Phase 2: Pilot and Validation	Months 0 to +12 (first deployment year)	**Agriculture Department:** Deploy OATS-Core in 1 to 2 priority export commodity corridors (e.g., Alphonso Mango from Konkan Maharashtra; Basmati Rice from Haryana-Punjab); operate OATS Delivery Unit with real-time monitoring dashboard. **FSSAI:** Integrate FICS with OATS PEVC API; train Authorized Officers on PEVC verification workflow; measure first PEVC-enabled consignment clearance time at destination port vs. pre-OATS baseline. **Exporters:** Enrol 50 to 100 exporter entities; issue first batch of PEVCs; document export rejection rate change. **Farmers and FPOs:** Enrol 10,000 to 50,000 farmers in OATS-Core registration; measure data capture compliance rate at 3 and 6 months; conduct farmer satisfaction survey and remediate top 5 friction points. Civil Society: Publish first OATS Public Performance Dashboard; launch OATS Fraud Reporting Portal.
Phase 3: Scale and Institutionalization	Months +12 to +60 (years 2 to 5)	**All Actor Categories:** Roll out OATS-Standard across additional commodity corridors; integrate bilateral destination-country systems (EU TRACES, US FDA PREDICT); expand PEVC to all APEDA-registered commodity categories. Technology Ecosystem: Open OATS Innovation Challenge for Fund allocation; publish OATS Open Research Programme grants.

PART II

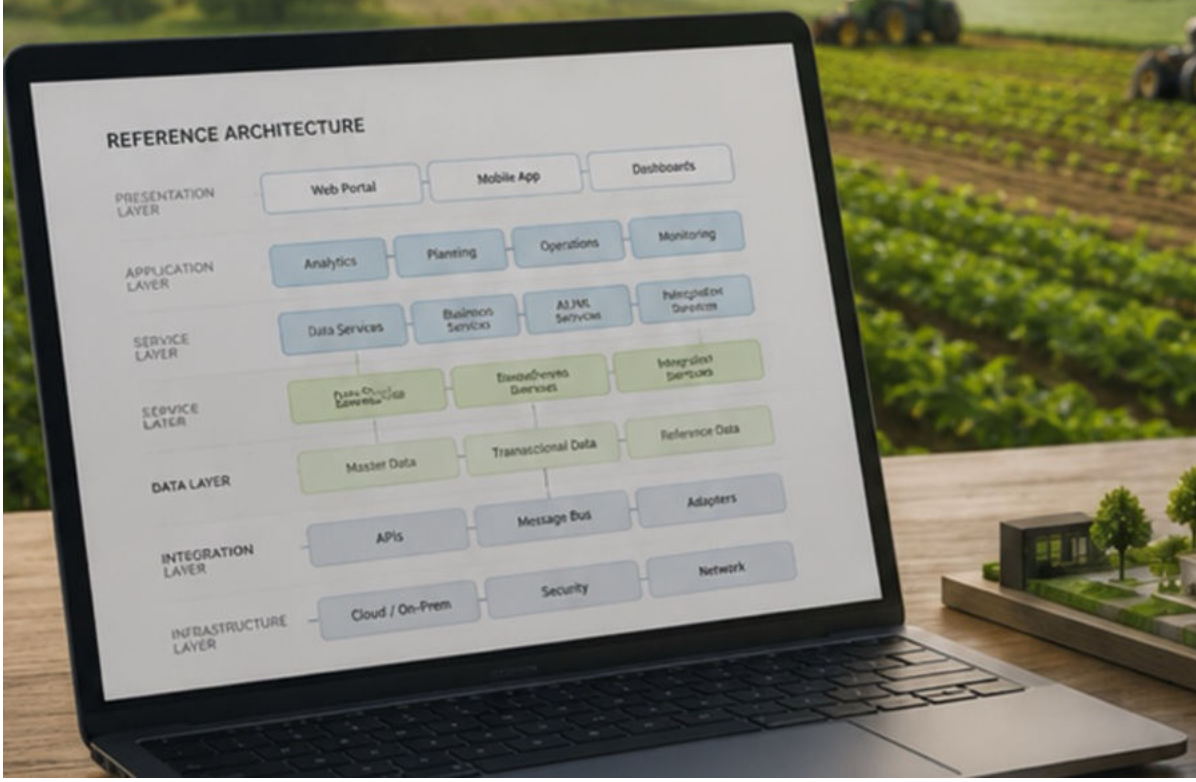
OATS

TECHNICAL ARCHITECTURE & STANDARDS

CHAPTERS 4-10

- *The 5+1 layer DPI stack (Identity · Event · Interoperability · Consent · Application + Layer 6: Verification / AI / Intelligence) and the Hourglass Protocol Model*
- *Identity & registry - GS1 GLN/GTIN, W3C DIDs, Verifiable Credentials, federated registries integrated with AgriStack*
- *EPCIS 2.0 event grammar - Critical Tracking Events, Key Data Elements, FSMA 204 + EU 178/2002 mappings*
- *Physical-digital carriers - QR, DataMatrix, RFID, NFC, GS1 Digital Link, IoT/cold-chain sensors, GS1 Sunrise 2027 transition*
- *The OATS Protocol - Beckn-derivative network layer; blockchain anchoring on Hyperledger Fabric / Besu / IOTA*
- *OATS API architecture - OpenAPI 3.1, microservices, GovStack X-Road, and the integration framework*

ANCHORED TO: GS1 EPCIS 2.0 · W3C VCS · BECKN · HYPERLEDGER FABRIC · GOVSTACK · CDPI · INDEA 2.0 · DPDPA 2023 · FSMA 204 · EUDR



4. OATS Reference Architecture and System Design

4.1 Architecture Design Rationale: The 5+1 Layer DPI Model

The OATS reference architecture is formally specified as a **5+1 layer Digital Public Infrastructure stack** — a layered digital common, not a monolithic platform, capable of serving all agri commodity sectors from a single shared infrastructure base. The same foundational infrastructure serves horticulture, cereals, oilseeds, fibre crops, spices, and plantation crops; commodity-specific configurations apply as modular extensions at the Standards Registry level. A ginning centre in Vidarbha recording cotton bale custody transfer uses the same Traceability chain code, the same Beckn-derived protocol event flow, and the same EPCIS 2.0 event structure as a pomegranate FPO in Nashik recording a harvest lot declaration.

Three cross-cutting technologies thread through multiple layers. **Blockchain** provides tamper-evident anchoring for identity credentials, event hashes, consent artefacts, and compliance evidence. **Beckn-derived protocols** operate as the open decentralised commerce and traceability discovery network. Beckn itself is a commerce protocol covering catalogue, order, fulfilment, and post-fulfilment flows, it does not natively generate traceability events; OATS introduces the **Beckn Network Adapter**[10] as the architectural bridge, translating each Beckn commerce transaction into the corresponding EPCIS 2.0 event so commerce and traceability are recorded as a single atomic action with no double data entry. **GS1 EPCIS 2.0 (ISO/IEC 19987:2024)**[11] is the universal event grammar.

4.2 Master Overview: The OATS 5+1 Layer stack

The table below presents the full 5+1 layer architecture in a single view, showing for each layer its core responsibility across all Agri commodity sectors, key building blocks, and the specific integration role of Hyperledger Fabric and Beckn Protocol.

Table 4.2 OATS 5+1 Layer DPI Architecture: Master Overview

Layer	Name	Core Responsibility	Key Building Blocks	Hyperledger Fabric & Beckn Role
L1	Identity, Trust & Registry	Establishes persistent, portable, verifiable identifiers for every participant & asset across all Agri chain; maintains authoritative entity registries; enforces zero-trust access control and DPDPA 2023 consent at the network perimeter.	AgriStack DID; MOSIP[11] (for jurisdictions without a national farmer registry - foundational identity fallback); Farmer /FPO /Lot/Facility Registries; GS1 GLN/GTIN; Commodity Standards Registry; Fabric CA; RBAC	Fabric CA issues X.509 certs linked to W3C VCs; VC hashes anchored on governance-channel at issuance
L2	Event, Traceability & Blockchain Anchoring	The hourglass waist of OATS. Records all Agri supply-chain events in GS1 EPCIS 2.0 standard; anchors event hashes to Hyperledger Fabric for tamper-evident immutability.	GS1 EPCIS 2.0; Event Anchor Microservice; Traceability Chaincode; Commodity Extension Schemas	SHA-256 event hashes anchored on Fabric with a target SLA; 7-channel Fabric architecture (farmer, fpo, trade, processing, logistics, export, governance); see Section 4.13

[10]

[11] Modular Open Source Identity Platform (MOSIP)." International Institute of Information Technology Bangalore (IIIT-B), 2018.

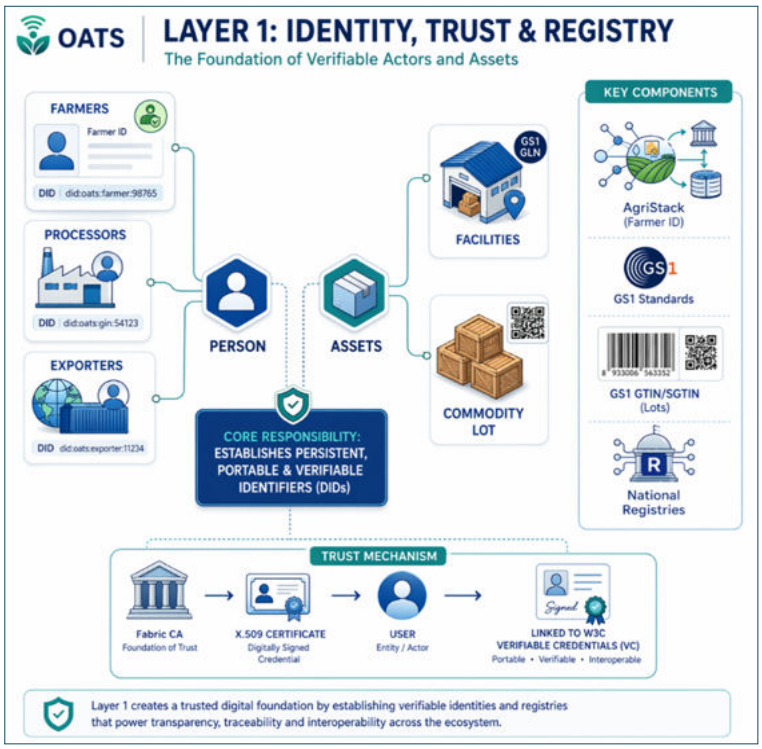
L3	Interoperability, Open Protocol & Commerce	Defines how systems interact across organizations and jurisdictions for all Agri commodity sectors; implements Beckn Protocol as the open decentralized commerce and traceability discovery network; standardizes API contracts.	OATS-Beckn Gateway; BAP/BPP; ONDC Agriculture; Open API 3.1 Gateway; Commodity Standards Registry	Beckn confirm calls trigger Fabric transferCustody(); Gateway is the anti-duplication bridge between Beckn commerce events and EPCIS traceability records
L4	Consent, Credentialing & Data Governance	Governs data rights across all Agri commodity sectors who holds which credential, who may access which data, for what purpose and duration; manages W3C VC lifecycle; enforces DEPA-aligned consent architecture.	DEPA Consent Manager[12]; W3C VC 2.0 Issuance; Selective Disclosure; RBAC Audit Trail; Commodity Certification VC Registry	VC hashes & revocation events anchored on governance-channel; consent artefacts structured as W3C VC objects; certification VCs for all commodity types
L5	Application & Ecosystem Layer	The competitive, innovative application space where public and private actors consume OATS infrastructure. Explicitly separated from infrastructure layers so no single application or vendor monopolizes the ecosystem across any commodity sector.	Consumer / Trade Transparency Portal; Export Compliance (APEDA); ONDC/APMCs; Commodity Recall Management; Regulatory Dashboards; MahaVISTAAR, State Data Exchanges like MahaAgx	Fabric hash verified before serving any provenance claim; compliance evidence assembled via queryLotHistory() across all commodity channels
L6 (+1)	Verification, AI & Intelligence	Autonomous cross-cutting intelligence layer consuming the trusted data foundation of Layers 1–5 to generate automated verification, predictive intelligence, and actionable insights across all agri-commodity sectors and value chains.	Autoencoder Anomaly Detection; MRL/Contaminant Prediction; OCR/NLP Document Validation; Edge AI; LLM/SLM Advisory; Satellite Imagery Analytics (deforestation, crop area); EUDR Due Diligence	AI anomaly alerts trigger Fabric flagging events on governance-channel; deforestation risk models consume satellite data and anchor compliance attestation hashes on export-channel

4.2.1 Layer 1: Identity, Trust & Registry

[12] Data Empowerment and Protection Architecture (DEPA): Draft for Discussion." NITI Aayog, Government of India, 2020. Operationalized by the Sahamati Collective

Layer 1 is the foundational trust infrastructure. It establishes persistent, portable, globally unique identifiers for every participant and asset across all agri commodity sectors. OATS adopts a **federated registry approach**, reusing national and institutional registries: AgriStack for farmer identity; Bhulekh and state land records under DILRMP; GS1 GLN for facility identification; GS1 GTIN/SGTIN for product and lot identification; livestock national identification systems where applicable. No new identity silo is created; OATS acts as the DID-based identity overlay linking existing authoritative registries.

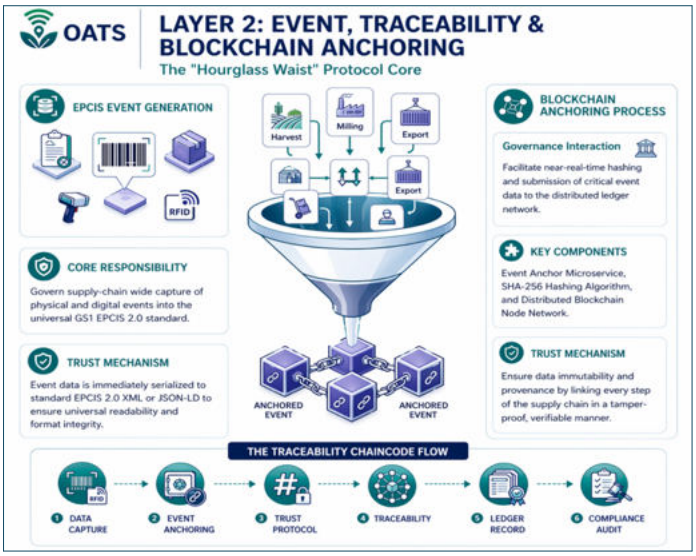
Commodity-Inclusive Registry Architecture.



- **Farmer and Producer Registry** — integrated with AgriStack Farmer ID. Covers all farmer types (horticulture, grain, cotton, spice).
- **Commodity Lot and Batch Registry** — GS1 SGTIN-based lot identifiers assigned at the Declare event. Commodity type and sector recorded at lot creation. Lot lineage tracks across aggregation, processing, packing, export using the parent-child world-state model.
- **Organisation Registry** — FPOs, mandi operators, ginning centres, cotton textile mills, oil mills, spice processing units, exporters, certification bodies. Each assigned a GS1 GLN and W3C DID.
- **Commodity Standards Registry** — a Layer 1 service maintained by the OATS Governance Council. Registers commodity-specific EPCIS extension schemas, KDE specifications, applicable regulatory rule sets (FSMA 204, EU 178/2002, EUDR, GDST, UFLPA, BCI), certification types. The configuration layer that makes OATS commodity-agnostic at core while commodity-specific in execution.
- **Certification and Accreditation Registry** — NABL-accredited laboratories, organic certifiers, GI tag authorities, BCI-licensed auditors, Rainforest Alliance certifiers, MSC chain-of-custody certifiers, APEDA-registered exporters. All certification events issue W3C VCs at Layer 4.

4.2.2 Layer 2: Event, Traceability & Blockchain Anchoring

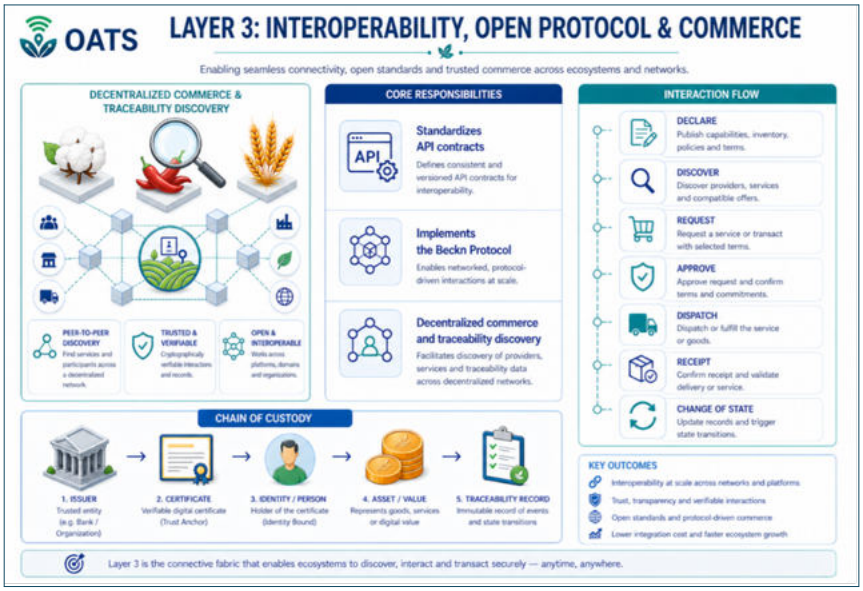
Layer 2 is the hourglass waist of OATS the single shared protocol layer through which all Agri commodity supply-chain actors, regulators, IoT devices, and destination authorities must pass, across every commodity sector. It is structured around the GS1's common foundation for business by uniquely Identify, accurately Capture and automatically Sharing vital information about product, location, assets and more. The globally recognized three-pillar model for end-to-end supply-chain traceability, underpinning FSMA 204 (US), EU Regulation 178/2002, ISO 22005:2007, and the EU EUDR. Hyperledger Fabric v2.5 provides the tamper-evident blockchain anchoring thread running through all three pillars.



4.2.3 Layer 3: Interoperability, Open Protocol & Commerce

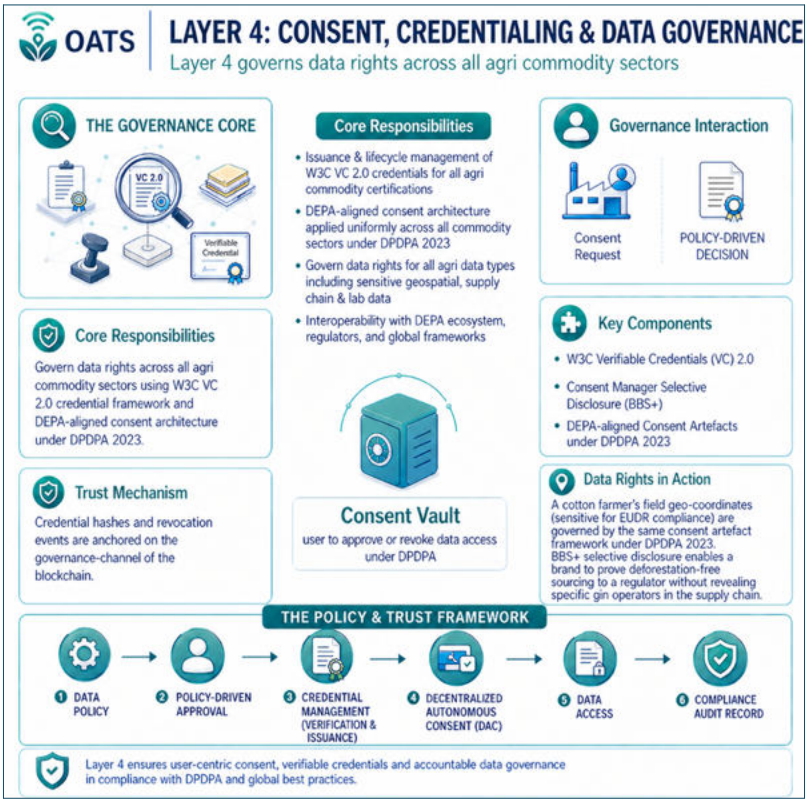
Layer 3 defines how systems interact across organizational and jurisdictional boundaries for all Agri commodity sectors like grain mandis, cotton exchanges, spice trading platforms and plantation commodity exchanges. It is explicitly protocol-driven: any compliant system operating in any commodity sector must emit and consume traceability records using the same common protocol semantics defined at this layer.

Beckn Protocol is implemented at Layer 3 as the open decentralized commerce and traceability discovery network spanning all Agri commodity sectors. A cotton textile mill (BAP - Buyer-side Application Platform) can discover BCI-certified cotton bale lots from gin operators (BPP - Seller-side/Provider Platforms) using the same Beckn search/on search flow as a spice buyer discovering NABL-tested turmeric lots, or an edible oil manufacturer discovering GMO-free soybean lots with EUDR deforestation attestation. The Beckn Registry Extension enables search by commodity-specific attributes, BCI certification, deforestation-free status, GI tag, organic certification creating direct commercial incentives for maintaining verifiable, up-to-date traceability records across all sectors



4.2.4 Layer 4: Consent, Credentialing & Data Governance

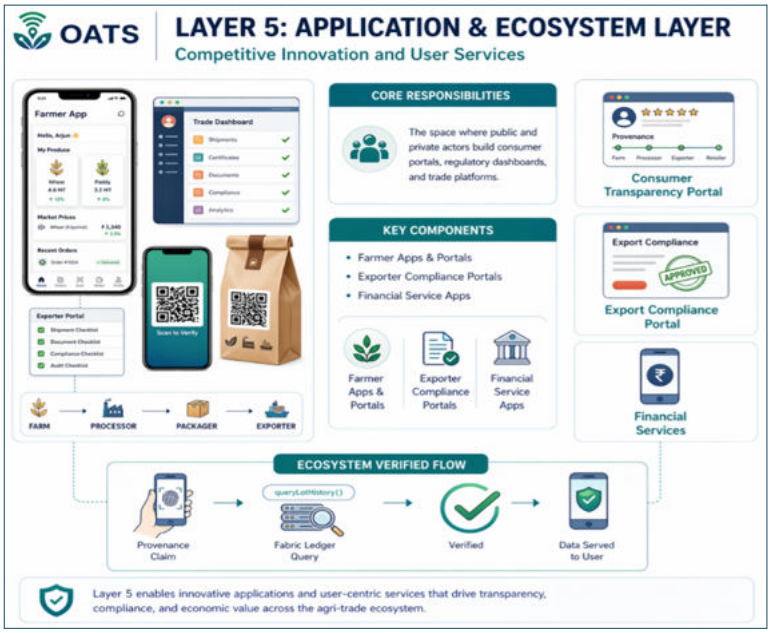
Layer 4 governs data rights across all agri commodity sectors. The W3C VC 2.0 credential framework at this layer issues and manages credentials for the full spectrum of agricultural commodity certifications - organic produce, GLOBALG.A.P., GI tags, Better Cotton Initiative, Fairtrade, Rainforest Alliance, GMO-free declarations, deforestation-free attestations, NABL laboratory accreditation, and APEDA export eligibility.



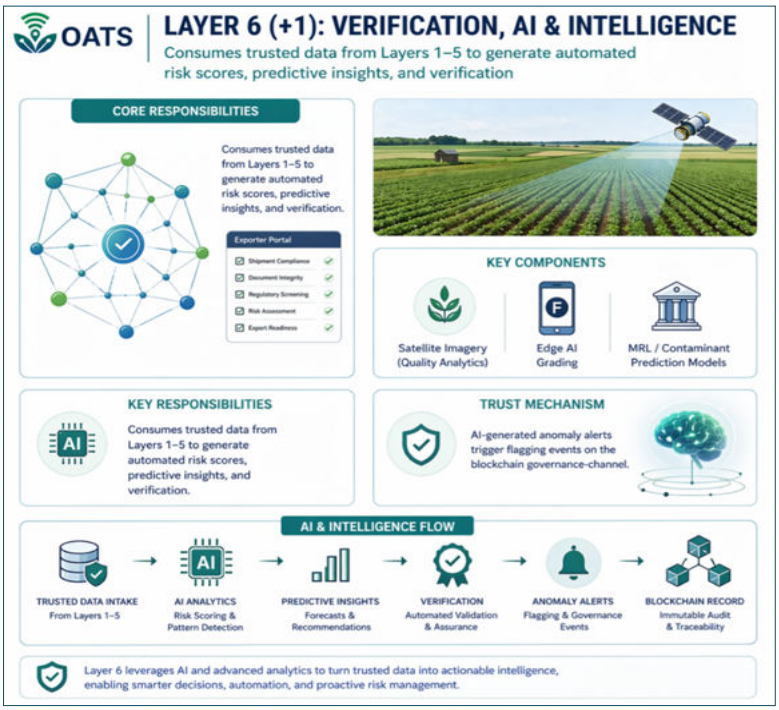
The DEPA-aligned consent architecture applies uniformly across all commodity sectors. A cotton farmer's field geo-coordinates (sensitive for EUDR compliance) are governed by the same consent artefact framework under DPDPA 2023 principles. The BBS+ selective disclosure capability is particularly important for fiber and plantation commodities where supply chain geography is commercially sensitive: a cotton textile brand can prove deforestation-free sourcing to a regulator without revealing the specific gin operators in their supply chain.

4.2.5 Layer 5: Application & Ecosystem layer

Layer 5 is the competitive application space where public and private actors consume OATS infrastructure to deliver operational services across all Agri commodity sectors. Applications are explicitly separated from infrastructure so no single application monopolizes ecosystem in any commodity sector.



that the

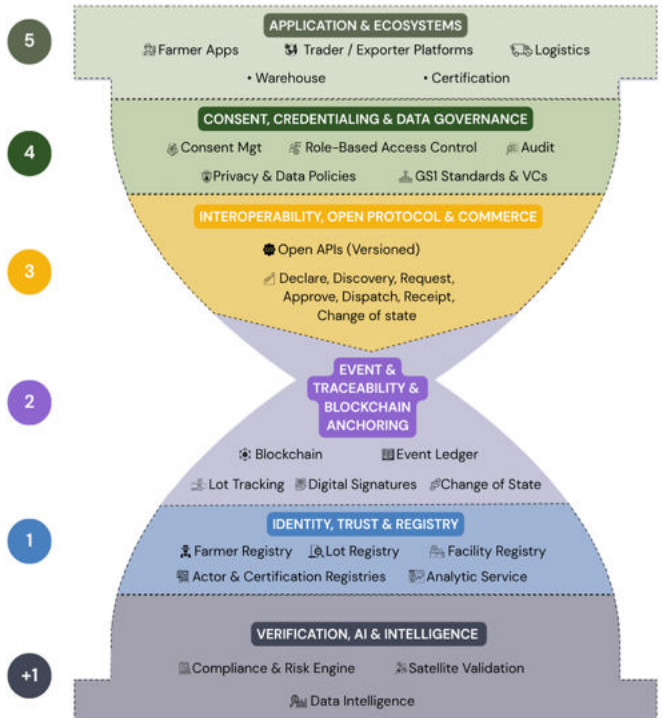


4.2.6 Layer 6 (5+1) (Verification, AI & Intelligence)

Foundational intelligence layer enabling trust across all commodity sectors compliance & risk engines, satellite validation, and data intelligence. Powers verification before and after transactions. Sector-agnostic and extensible.

4.3 The Hourglass Protocol Model

The hourglass model applies uniformly across all Agri commodity sectors. In the OATS hourglass, a narrow waist of shared open protocols sits between diverse sector-specific technology implementations below and diverse commodity-sector applications above. The waist Layer 2 (Event, Traceability & Blockchain Anchoring) is the same for a pomegranate FPO, a cotton ginning centre and a soybean crushing plant. Only the KDE schemas registered in the Layer 3 Standards Registry differ.



Below the waist

- **Layer 1 (Identity, Trust & Registry)**
  Diverse identity and registry systems across commodity sectors AgriStack, GS1 facility and actor registries. Competitive and technology neutral.

- **Layer +1 Verification, AI & Intelligence** Foundational, sector-agnostic intelligence layer for compliance, risk, satellite validation, and data-driven verification before and after transactions.

The Waist

- **Layer 2 (Event Traceability, Open Protocol Core & Blockchain Anchoring):**
  GS1 EPCIS 2.0 and blockchain (e.g., Hyperledger Fabric) as the shared open protocol that ALL actors across ALL commodity sectors must use event ledger, lot tracking, digital signatures, and state changes. Open, non-competitive, publicly governed. Closed infrastructure here risks platform capture: open infrastructure enables an agri commodity commons.

Above the waist

- **Layer 3 (Interoperability, Open Protocol & Commerce):**
  Standardized interoperability layer open, versioned APIs and Beckn-based commerce flows (discover, request, approve, dispatch, receipt). Enables seamless interaction across platforms.
- **Layer 4 (Consent, Credentialing & Data Governance):**
  Trust and governance framework for all interactions consent management, role-based access control, privacy & data policies, GS1 standards, verifiable credentials, and audit mechanisms.
- **Layer 5 (Applications & Ecosystems):**
  Diverse and competitive application layer across commodity sectors farmer apps,

Cross-Sector Interoperability Principle: Because all commodity sectors use the same EPCIS 2.0 waist, cross-sector traceability queries are natively possible. A processed food manufacturer sourcing turmeric (spice), soybean oil (oilseed), and packaging cotton (fibre) can assemble a unified supply chain compliance picture EUDR attestation, GI verification, and MRL clearance from a single OATS queryLotHistory() call per lot, regardless of the commodity sector

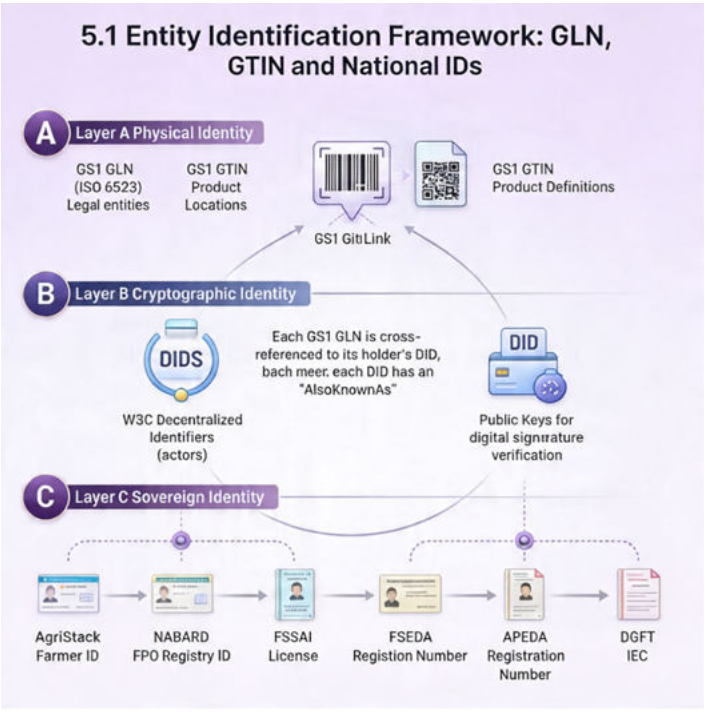
trader/exporter platforms, logistics, warehousing, certification systems, and sector-specific solutions.

5. Identity, Trust, Registry and Credentialing Standards

A strong agricultural digital ecosystem needs a standardized way to identify supply chain actors, including farmers, organizations, processors, logistics providers, and exporters. Using global standards like GS1's GLN and GTIN makes entity and product identification easier. W3C Decentralized Identifiers enable actors to manage their own digital IDs for privacy and trust. Certifications and compliance can be verified with Verifiable Credentials for secure, portable proof. Linking this system with national databases like AgriStack strengthens authenticity and connects it to government services. These measures support a scalable farmer registry architecture for secure onboarding, identity validation, and traceability across the value chain.

5.1 Entity Identification Framework: GLN, GTIN and National IDs

Every entity participating in OATS farmer, FPO, processor, exporter, warehouse, laboratory, certification body, and government authority must carry a globally unique, persistent, and standards-based identifier. The integrity of every traceability event recorded on the immutable event ledger depends on the ability to unambiguously resolve the identity of every actor and location referenced in that event. A harvest event that cannot be linked to a verified farm parcel, or a dispatch event that cannot be linked to a licensed transporter, carries no evidential weight regardless of how accurately the underlying physical event was captured.



OATS adopts a tiered identifier architecture that uses the most appropriate identification standard for each entity class, links those identifiers to authoritative national registries, and bridges commercial and sovereign identity systems through a unified OATS identifier resolution service. The governing principle is that no OATS-proprietary identifier format is permitted at any registry layer. Every OATS entity identifier must be either a GS1 global identifier standard, a W3C DID, or a recognized national government identifier that maps to one of these two anchor systems.

5.1.1 The Three-Layer Identifier Taxonomy

- **Layer A Physical Identity** - uses GS1 GLN (ISO 6523) for all legal entities and physical locations, and GS1 GTIN for all product definitions. These globally unique, commercially recognized identifiers enable interoperability with any GS1-compliant supply chain system worldwide and are encoded in GS1 barcodes and GS1 Digital Link QR codes at the consumer endpoint.

- **Layer B Cryptographic Identity** - uses W3C Decentralized Identifiers (DIDs) for every OATS-registered actor. DIDs carry the public keys that enable digital signature verification for events anchored on the immutable event ledger and for Verifiable Credential issuance and presentation, independent of any central authority.

- **Layer C Sovereign Identity** - uses national government identifiers: AgriStack Farmer ID, FSSAI License Number, APEDA Registration Number, and DGFT IEC. These identifiers anchor OATS entities within their regulatory jurisdiction and enable federation with government registries without replicating registry data in OATS.

The three layers are linked within the OATS Registry: each GS1 GLN is cross-referenced to its holder's DID; each DID carry an alsoKnownAs reference to the relevant sovereign identifier; and each sovereign identifier is verified against its authoritative national registry at enrollment and kept current through publish-subscribe synchronization. All three must be present for an entity to participate fully in OATS event recording and PEVC issuance.

5.1.2 GS1 Global Location Number (GLN)

The GS1 Global Location Number (ISO 6523) is the canonical identifier for all legal entities and physical locations registered in OATS. Every event anchored on the OATS event ledger references the GLN of the business location and read point where the event occurred the GLN is the geographic and organizational anchor that makes event records interpretable and verifiable across jurisdictions and systems.

5.1.3 GS1 GTIN and SGTIN

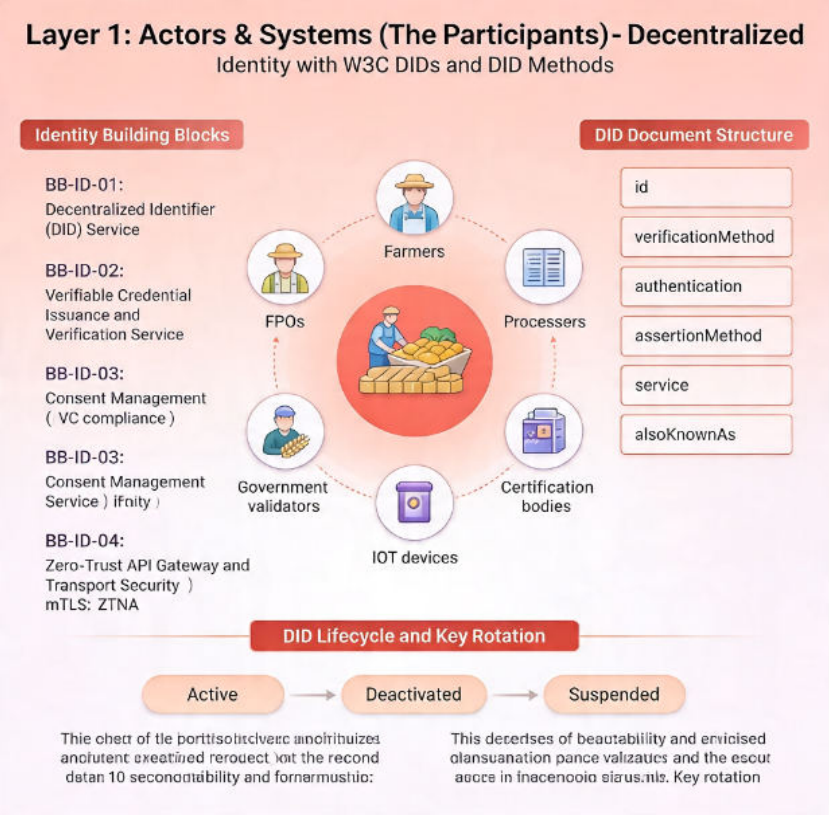
The GS1 GTIN is the standard identifier for all OATS-registered agricultural products in the Product Registry, defining product variety, grade, packaging, and certification for clear identification from farm to consumer. Each registered product must have a valid GS1 GTIN from GS1 India. The SGTIN adds serialization to the GTIN to pinpoint specific lots, is recorded in every EPCIS event, and is encoded in the GS1 Digital Link QR code scanned by consumers and authorities to view provenance.

5.1.4 National Identity System Integration

For individual farmers, GS1 identifiers are not the primary entry point. India's AgriStack programme provides the national farmer identity infrastructure, with the AgriStack Farmer ID as the canonical individual farmer identifier. OATS integrates with AgriStack through a consent-gated API that retrieves farmer identity attributes and farm parcel records without replicating AgriStack data in OATS persistent storage. In non-Indian OATS deployments, MOSIP (Modular Open Source Identity Platform) provides the equivalent open-source identity anchor, with the MOSIP UIN serving the same function as the AgriStack Farmer ID. OATS Layer 1 supports both did:agristack and did:mosip DID Methods, enabling the same cryptographic identity architecture regardless of the underlying national identity system.

5.2 Decentralized identity: W3C DIDs and DID Methods

Layer 1 (the foundational trust layer) enables three capabilities: authenticated identification of all participants (farmers, FPOs, processors, exporters, government validators, IoT devices, certification bodies) using standards-based decentralized identifiers; issuance and verification of cryptographically secure credentials proving compliance or certification status without relying on a centralised authority; and consent management aligned with the **DPDPA 2023**, ensuring that personal data is accessed and processed only with explicit, specific, and auditable user consent. Designed per InDEA 2.0 Privacy and Security by Design and Consent-Based Data Sharing, and per CDPI Principle C-1[55] which positions identity as foundational infrastructure rather than an application feature. Indian-context anchoring uses AgriStack for farmers, the APEDA Registry for exporters, and GS1 GLNs for commercial entities; for global deployments **MOSIP** is the scalable open-source alternative.



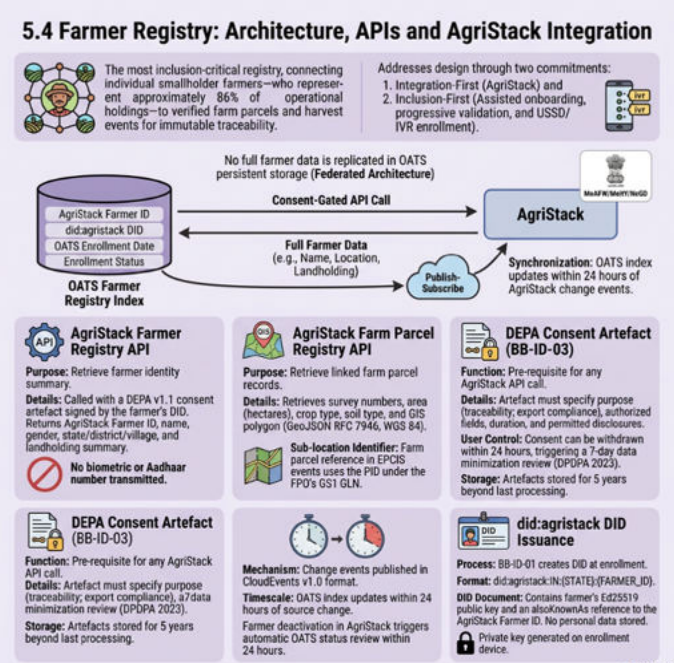
5.3 Verifiable Credentials for Certifications and Compliance

Verifiable Credentials (VCs) form the full trust-chain layer within the OATS ecosystem, covering identity assertions, foundational farm credentials, lot declarations, regulatory certifications, commercial transactions, and the terminal Pre-Export Verification Certificate. Each VC is a digitally signed claim issued by an authorised authority - for example, an AgriStack-issued Farm Foundational VC encoding farmer-plot-crop identity, a Lot Declaration VC issued by an aggregator at the birth-of-lot event, an FSSAI License VC, an APEDA Registration VC, a NABL Laboratory Test Report VC, or a Commercial Invoice VC issued by a seller at the transaction event. Every VC in the chain cryptographically references its parent VC, producing a chained-issuance trust graph that terminates in the PEVC.

Credential issuance is carried out by recognized certification bodies and regulatory authorities including FSSAI, APEDA, NABL-accredited labs, NPOP-accredited organic certifiers, and plant quarantine agencies, each operating through their own signing infrastructure linked to a registered DID-OATS issuer identity. Importantly, the full credential data remains with the issuing authority, while the OATS Certification Registry stores only minimal metadata: the credential hash, issuer DID, subject identifier, credential type, issuance date, and current status (valid, suspended, or revoked). This architecture avoids centralizing sensitive audit data while still enabling rapid, API-based verification of credential validity typically within milliseconds.
To ensure auditability and non-repudiation, the OATS immutable event ledger anchors cryptographic hashes of all certification lifecycle events such as issuance, renewal, and revocation as timestamped and digitally signed EPCIS ObjectEvents. The ledger records only proof of occurrence, not the credential content itself. For real-time revocation checks, OATS relies on issuer-maintained Status List 2021 bitstrings rather than querying the ledger, allowing high-frequency validation without impacting system performance. This design balances transparency, privacy, and scalability while maintaining strong compliance assurance across the ecosystem.

5.4 Farmer Registry: Architecture, APIs and AgriStack Integration

The Farmer Registry is the most inclusion-critical registry in OATS. Individual smallholder farmers represent the largest actor class in the Indian agricultural supply chain. Approximately 86 percent [13]of all operational holdings are below two hectares. Without reliable farmer identity anchored to verified farm parcels, harvest events on the immutable ledger cannot be linked to their production origin, lot-level lineage from farm to export gate cannot be established, and the entire upstream provenance record is unverifiable. The Farmer Registry design must therefore achieve both identity rigor and universal inclusion simultaneously.



OATS addresses Farmer Registry design through two commitments: integration-first building on AgriStack rather than creating a new farmer database and inclusion-first supporting assisted onboarding, progressive validation, and USSD/IVR enrolment pathways for farmers without smartphones or high-bandwidth connectivity. These commitments operationalize OATS Principle P-18 (Inclusive by Architecture) and InDEA 2.0 Consent-Based Data Sharing at the first-mile level.

5.4.1 AgriStack Integration Architecture

AgriStack (Ministry of Agriculture and Farmers Welfare / MeitY / NeGD) provides a unique Farmer ID for every Indian farmer linked to their Aadhaar-verified identity and cross-referenced to land holdings, crop declarations, and enrolled government schemes. The OATS Farmer Registry holds only a lightweight index: the AgriStack Farmer ID, OATS enrolment date, and enrolment status. Full farmer data is retrieved on-demand from AgriStack through consent-gated API calls and is never replicated into OATS persistent storage, in conformance with the federated registry architecture and DPDPA 2023 data minimization requirements.

5.5 Business and Facility Registry

This capability is also integral to Layer 1, as it reinforces the trust and identity foundation of the OATS ecosystem. Within this context, the registries define the authoritative record of all participants and the credentials associated with them, ensuring that every entity interacting within the system is uniquely identifiable, verifiable, and in a valid state. Aligned with the India Enterprise Architecture (InDEA) 2.0 Registry as a Service, these registries are exposed through standardized APIs, allowing any authorized system to validate entity identity and status without duplicating data. This design ensures that identity and credential verification remain a shared infrastructure service rather than being fragmented across applications.

[13] Agriculture Census, Ministry of Agriculture & Farmers Welfare, Government of India — agcensus.nic.in

By embedding registries within Layer 1, OATS strengthens the core trust layer and directly addresses the issue of isolated certification silos, where multiple agencies maintain disconnected and inconsistent records. Instead, a unified registry approach enables real-time verification of registration, licensing, and certification status through a single API call, while higher layers such as the event ledger reference entities by their identifiers rather than duplicating information. This integration ensures consistency, reduces redundancy, and establishes a reliable foundation for secure, interoperable, and scalable supply chain operations.

5.5.1 Facility Registry: Geospatial Functions

Geolocation data in the Facility Registry serves three supply chain functions. Supply chain route verification cross-checks the sequence of facility GLN locations in an EPCIS event chain on the immutable ledger against plausible geographic routing, flagging physically impossible transit claims before they propagate to a PEVC. Jurisdiction determination automatically identifies which State Food Safety Authority holds regulatory oversight for any event based on the facility's recorded GIS coordinates, enabling automated routing of compliance notifications and enforcement alerts. GI origin verification compares processing facility GPS coordinates against the GI registration's production area GeoJSON polygon in the Product Registry to confirm that GI-tagged lots were produced and processed within the registered geographic boundary, supporting the GI Attestation VC issued by the authorized Certification Body.

5.6 Product and Commodity Registry

The Product and Commodity Registry is a key Layer 1 component, providing standard definitions for all agricultural products and food commodities traceable in OATS. Each record includes the product’s species, variety, quality grade, certification schemes, destination-country regulations, and GS1 GTIN. Serving as the authoritative master data layer, it validates lot-level traceability events at data capture and enables compliance-by-design. The registry also supports the PEVC Compliance Engine, ensuring consistent and accurate compliance requirements for each product and destination throughout the supply chain.

Individual lots are identified at the event layer through GS1 SGTINs and SSCCs, not in the Product Registry itself. The SGTIN is the identifier recorded in every EPCIS event on the immutable ledger from initial harvest through final export shipment. GI product lots carry a GI Origin Attestation VC issued by the authorized Certification Body, confirming production within the registered geographic area by an authorized user. The cryptographic hash of this VC issuance event is anchored on the immutable event ledger, providing a timestamped, non-repudiable record of when the attestation was made and by which authority.

5.7 Certification and Accreditation Registry

The Certification and Accreditation Registry functions as the compliance intelligence layer within OATS Layer 1, maintaining the real-time status of all certifications associated with registered entities. It enables instant verification capabilities that are critical for the operation of the PEVC Compliance Engine. In line with privacy-by-design principles, the registry does not store full credential content; instead, it retains only essential metadata, including the Verifiable Credential (VC) hash, issuer decentralized identifier (DID), subject entity identifier, credential type, issuance date, and current status (valid, suspended, or revoked). The complete credential remains with the issuing authority, reducing the risk of centralizing sensitive audit reports or proprietary certification data and minimizing exposure to unauthorized access.

The OATS immutable event ledger complements this registry with a clearly defined and limited role. It anchors the cryptographic hash of each certification lifecycle event issuance, renewal, and revocation

as a timestamped and digitally signed EPCIS Object Event. This provides a non-repudiable audit trail confirming that a compliance-relevant action occurred at a specific point in time, without storing the credential content itself. For real-time validation, revocation checks are performed using the W3C Status List 2021 bitstring maintained by the issuing authority, rather than querying the ledger. This approach ensures high-frequency, low-latency verification during PEVC assembly while preserving system performance, scalability, and data privacy.

5.7.1 Certification Trust Chain

The OATS Certification Registry implements a chain of trust from the national accreditation authority at the apex through accredited Certification Bodies to the supply chain actors holding certifications. Every OATS VC issued by a Certification Body references that body's own accreditation VC hash in the Registry. This chain enables destination-country authorities to verify not just that a certification exists but that it was issued by a competent authority that was itself properly accredited at the time of issuance closing the fraud vector that characterizes paper-based certification systems where the standing of the issuer cannot be independently verified.

Certification Scheme	Issuing Authority and Accreditation Basis
FSSAI Central and State Licenses	Issued by FSSAI. Verified through direct FSSAI FBO Registry API. FSSAI is a statutory regulator under the Food Safety and Standards Act 2006; no separate NABL accreditation is required.
APEDA Registration	Issued by APEDA. Verified through APEDA registration database API. Statutory authority under the Agricultural and Processed Food Products Export Development Act 1985.
NPOP Organic Certification	Issued by NPOP-accredited Certification Bodies. Accreditation granted by APEDA under the National Programme for Organic Production. NABL ISO/IEC 17065 preferred but not mandatory for NPOP.
NOP (USDA) Organic Certification	Issued by USDA-accredited Certifying Agents. Accreditation granted by USDA Agricultural Marketing Service, National Organic Program.
GLOBALG.A.P. Certificate of Conformance	Issued by GLOBALG.A.P.-approved Certification Bodies. CB approval requires DAkkS (Germany), UKAS (UK), NABCB (India), or equivalent national accreditation body endorsement.
Spices Board Quality Certification	Issued by the Spices Board of India as a statutory authority under the Spices Board Act 1986. Covers cardamom, pepper, and 52 other notified spice commodities.
NABL Laboratory Accreditation	Issued by NABL (National Accreditation Board for Testing and Calibration Laboratories) under the Department of Science and Technology. NABL is the apex trust anchor for the OATS laboratory credentialing chain.
Halal Certification	Issued by APEDA-recognized Halal Certification Bodies accepted by GCC importing country authorities. OATS supports multiple recognized Halal bodies whose certifications are accepted by UAE, Saudi Arabia, and other GCC markets.
ISO/IEC 17065[14]	International standard for accreditation of bodies that certify products, processes, and services. Published by ISO and IEC. Referenced within the OATS Certification Trust Chain as the accreditation basis applied by national accreditation bodies (including NABCB in India) to Certification Bodies operating under OATS.

5.7.2 Certification Status Model

Every certification record in the OATS Certification Registry exists in one of four states. Active indicates the credential is valid and all revocation checks are passing. Warning indicates the credential is valid but natural expiry falls within 30 days the 30-day flag triggers entity notification through the registered channel and is visible to the PEVC Compliance Engine. Suspended indicates a

[14] iso.org

temporary hold by the issuing authority pending investigation this status is propagated to the Registry within 15 minutes and is immediately visible to any system querying the entity's certification status. Revoked indicates permanent revocation by the issuing authority or through an automated regulatory signal. No certification record is ever deleted; revoked and expired records are retained with their full state history for a minimum of 10 years, satisfying supply chain audit and food safety investigation requirements. All state transitions generate an audit event anchored on the immutable event ledger.

5.8 Identity Federation and Cross-Jurisdiction Interoperability

i. OATS operates as an identity federation node, not as a sovereign identity issuer. Three federation contexts: **India-Specific Federation**: AgriStack Farmer Registry is the foundational anchor; OATS federates with FSSAI FBO Registry, APEDA Registry, WDRA accreditation registry, NABL accreditation registry, NIC GI Cloud; central and state identity systems both supported through state-level OATS Identity Resolvers maintaining a unified identity framework across central and state levels.

ii. **MOSIP-Based Federation for Non-Indian Deployments** for deployments outside India, OATS adopts MOSIP as the equivalent national identity anchor; developed by IIIT Bangalore and supported by the international MOSIP community, providing scalable open-source identity infrastructure.

iii. **Cross-Border Identity Recognition** — for export-import contexts, OATS supports bilateral identity recognition through formal agreements under DPDPA 2023 cross-border transfer provisions; data-minimisation rules apply to cross-border payloads (SRS-2.9) — farmer identifiers, FPO member lists, and personal data are excluded from cross-border PEVC payloads unless required by regulations and covered by formal agreements under the DPDPA 2023.

5.9 Federated Registry Resilience: Failure Handling, Degraded Operations and Reconciliation

OATS operates as a federation node, not a sovereign issuer of identity - authoritative records remain in their source registries (AgriStack, APEDA), while OATS maintains only a lightweight index and credential-status pointers. This federation is the correct architecture, but it means OATS availability and freshness depend partly on systems OATS does not control, this section closes that gap.

Two non-negotiable principles govern:

- **Truth is never fabricated.** Cached values may be served when a source is unavailable but must be labelled cached and timestamped — never presented as live.
- **Trust-critical operations fail closed.** PEVC issuance, VC revocation checking, and consent verification refuse to proceed on stale data; they return a typed error rather than risk a clearance against a superseded fact.

5.9.1 Failure Taxonomy and Detection

Every federated-registry interaction is classified into one of five regimes — *Unavailable, Degraded-latency, Stale, Partial, Authoritative-conflict* — each with a defined detection signal, severity tier, and default response. Detection is continuous: each upstream is monitored by an active health probe and a passive observer of live traffic, with per-registry staleness clocks against the bounds in 5.9.2. Warning thresholds raise Sev-3 advisories; hard thresholds raise Sev-2 alerts.

5.9.2 Degraded-Operations Read Path

Each federated upstream sits behind a per-registry **circuit breaker** (closed / half-open / open) with configurable thresholds. When the breaker is open or latency exceeds SLO, OATS serves the last-known-good value from its index — annotated with mandatory fields: `registry_status` (live / cached / degraded), `source_registry`, `as_of` ISO-8601 timestamp, and `staleness_seconds`. A cached value not disclosed as cached is a conformance violation.

Each data class has a maximum-tolerable-staleness bound:

- **VC revocation status** — 15 min trust bound; trust-critical (fail closed beyond it).
- **Certification status** — 15 min; trust-critical.
- **Consent artefact status** — 15 min; trust-critical.
- **Entity / facility lookup** — 24 h hard bound; non-trust-critical (serve cached).
- **Product / GTIN reference** — 7 d hard bound; non-trust-critical.

Trust-critical operations exceeding the trust bound return an RFC 9457 `problem+json` error (`registry_unavailable` or `data_stale`) with a `Retry-After` hint. Downstream systems consuming OATS APIs must surface `registry_status` and `as_of` to end users.

5.9.3 Reconciliation on Recovery

When a breaker transitions back to closed, OATS runs a reconciliation pass for that registry; reconciliation also runs on a scheduled cadence and is driven by change notifications. **Authority rule:** the source registry is always authoritative; the index never overrides source; superseded index values are preserved as versioned history entries (SRS-2.6). Drift classes resolved: *missing-in-index* (create reference), *stale-in-index* (overwrite, version prior), *orphaned-in-index* (flag, suppress, escalate to Data Quality), *value-divergence* (source wins; signed reconciliation audit event).
Three complementary mechanisms bound worst-case index staleness: event-driven updates via CloudEvents pub/sub (SRS-2.7, <60 s; <15 min for revocation), scheduled delta sync (15-min default), and full reconciliation on upstream recovery. Every pass emits a signed, append-only audit event chained to the Section 11.6 audit architecture, with divergences beyond threshold raising a Data Quality Alert. Reconciliation is idempotent.

5.9.4 Cross-Cutting Considerations

Degraded mode bridges short upstream outages within the existing availability envelope (99.9%, SRS-1.9; RTO 4 h / RPO 15 min, SRS-10.14) — it is not a substitute for OATS's own disaster-recovery posture. Queries to external-jurisdiction registries (SRS-12.7) follow the same pattern, with one addition: **lawful-basis validation is itself trust-critical and fails closed.** The degraded-mode and reconciliation pattern defined here is the **canonical pattern for every external dependency** integrated through the Chapter 10 Information Mediator (X-Road v7), including the Bharat Trade Net adapter (Section 16.9).

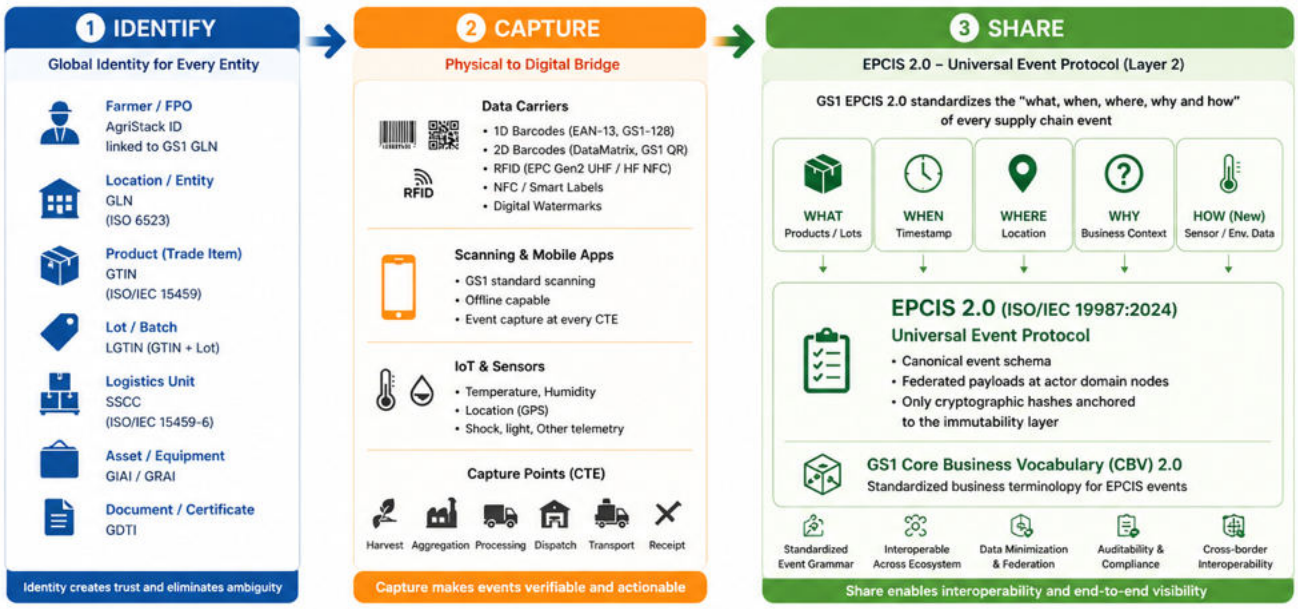
6. Traceability Event Data Model and EPCIS2.0 Implementation

This chapter sets the technical basis for the OATS Blueprint by defining a standard event data model for consistent capture, validation, and exchange of supply chain events. By adopting GS1 EPCIS 2.0 as the core schema, it ensures all supply chain actors and systems share a common, interoperable event structure.

OATS requires EPCIS 2.0 as the event standard, ensuring traceability data is recorded and shared in a consistent format across sectors and regions. The chapter explains how these events meet regulatory mandates like FDA FSMA Section 204 CTEs and EU Regulation 178/2002 Article 18 traceability rules. It also specifies the essential functional and system requirements for OATS-compliant engines, guaranteeing reliable generation, validation, and exchange of EPCIS events with compliance, auditing, and cross-border compatibility.

6.1 GS1 EPCIS 2.0: Architecture and Event Model

The GS1 system of standards organises supply-chain data into three pillars: **Identify** (unique identifiers — GTIN, GLN, SSCC, SGTIN), **Capture** (events at physical transition points — EPCIS), and **Share** (interoperable exchange — EPCIS REST API, GS1 Digital Link, CBV). EPCIS 2.0 is the **Share** standard mandated by OATS at Layer 3. It elevates JSON/JSON-LD to first-class formats (replacing the XML-centric design of EPCIS 1.x), enables REST API bindings, and introduces the sensor Element List for environmental conditions. It is fully backward-compatible with EPCIS 1.2 implementations through deterministic serialisation rules. The companion standards are **CBV 2.0** (Core Business Vocabulary, bizStep, disposition, and source/destination party URIs) and **GDSN** (Global Data Synchronisation Network) for master product data. Together they constitute the complete data model.



Every EPCIS event populates a **five-dimensional schema**. Every event must populate WHAT, WHEN, and WHY; WHERE is mandatory for Object Event, Aggregation Event, Transformation Event, and Association Event; HOW is optional in baseline EPCIS but **mandatory in OATS for any cold-chain-sensitive commodity** At Layer 3 validation, OATS extends EPCIS's baseline by making WHERE mandatory for all five event types.

6.2 Critical Tracking Events (CTEs) Across the Agri-Food Value Chain

A Critical Tracking Event is a supply-chain point at which traceability data must be captured for the lot to be traceable end-to-end. The concept originates in the GS1 Global Traceability Standard (GTS 2.0) and was made statutorily mandatory by the FDA Food Traceability Final Rule (87 FR 70910, November 2022). FSMA 204 identifies six foundational CTEs for all foods on the Food Traceability List. OATS extends the FSMA 204 baseline to **ten CTEs covering the complete agri-food value chain** from seed procurement to consumer retail scan, with each CTE mapped to a specific EPCIS 2.0 event type.

Table: The Five-Dimensional Event Schema

CTE#	CTE Name	EPCIS Event Type	Key Identifiers	Triggered by
CTE-01	Seed / Planting Material Procurement	ObjectEvent (ADD)	Seed Lot ID, Farmer ID, Dealer ID	Dealer sale or nursery purchase or Farmer or FPO agent Input
CTE-02	Farm and Plot Registration	ObjectEvent (ADD)	AgriStack Farmer ID, Plot ID (GeoJSON), Farm GLN	Registration onboarding
CTE-03	Input Application (Spray / Fertiliser)	ObjectEvent (OBSERVE)	Farmer ID, Plot ID, Input product, Date, Dosage	Farmer or FPO agent entry
CTE-04	Farm Harvest	ObjectEvent (ADD)	LGTIN (Harvest Lot ID), Farmer ID, Farm GLN, Date, Quantity, Variety	Farmer or FPO agent - birth of lot identity
CTE-05	Primary Aggregation / FPO Collection	AggregationEvent	Parent SSCC, child LGTINs (all farm lots), FPO GLN	FPO agent QR scan of each farm lot
CTE-06	Mandi / Market Arrival	ObjectEvent (OBSERVE)	LGTIN, Mandi GLN, eNAM Lot ID cross-reference, Weight, Date	eNAM gate scan or manual entry
CTE-07	Packhouse / Processing Transformation	TransformationEvent	Input LGTINs → Output LGTIN, Packhouse GLN, QC parameters	Packhouse or processor operator
CTE-08	Quality Testing and Certification Attachment	ObjectEvent (extension: certificationInfo)	LGTIN, Lab Sample ID, Test results, Certificate IDs (PSC/TC/GI/Agmark)	Lab upload; Certifier entry; PQ officer
CTE-09	Export Shipment	ObjectEvent (bizStep=shipping)	SSCC, Container ID, Port GLN, Consignee, DDS reference, AWB/BoL	Exporter or freight forwarder
CTE-10	Consumer / Retail Scan	ObjectEvent (bizStep=retail_selling)	GTIN, Retail GLN, GS1 Digital Link QR	Consumer QR scan or ONDC transaction

Birth-of-Lot Principle and Chain Continuity: Every OATS lot identity must have a single, unambiguous **birth-of-lot event** , the EPCIS event that creates a new LGTIN. New lot identities may be created only at **CTE-04 (Farm Harvest)** and **CTE-07 (Packhouse/Processing Transformation)**. CTE-05 (Aggregation) creates a parent SSCC but child LGTINs retain identity. Any system that creates lot identities outside CTE-04 and CTE-07 breaks the chain-of-custody invariant — and the FSMA 204

24-hour data provision requirement becomes architecturally unachievable. Chain continuity from farm to consumer is preserved through the parent-child world-state model: every LGTIN created at CTE-07 carries cryptographic references to its parent LGTINs at CTE-04 (via Transformation inputEPCList → outputEPCList), and every SSCC at CTE-09 carries references to the constituent LGTINs.

6.3 Key Data Elements (KDEs): Detailed Field Specifications

A Key Data Element is information that must be recorded at each Critical Tracking Event so that the supply chain can be fully reconstructed from event records. KDE requirements have been made statutorily mandatory by FSMA 204 (FDA Food Traceability Final Rule, 21 CFR Part 1 Subpart S), with specific KDE sets per FSMA CTE. OATS defines a canonical set of **45 KDEs spanning 9 value chain stages**, satisfying FSMA 204 in full and adding KDEs required by EU 178/2002 Article 18, EUDR, GLOBALG.A.P., GI attestation, and APEDA export compliance.

Table 6.3.1 — The OATS 45-KDE Specification by Value Chain Stage.

Stage	KDE	Format	Authoritative Source
1 – Seed / Planting Material Procurement	Seed Lot Number / Sapling Batch ID	Alphanumeric	SATHI Portal (India); seed dealer records; nursery records
	Seed Variety Code	Alphanumeric (ICAR code or equivalent)	National Seed Corporation; ICAR variety registry
	Seed Certification Tag Number	Alphanumeric	State Seed Certification Agency
	Source Entity ID (Dealer / Nursery)	GLN or national trader ID	Dealer registration; MAHA-TRACE or equivalent
	Procurement Date	Date (ISO 8601)	Farmer self-declaration; dealer invoice
2 – Farm Input and Sowing	Farmer ID	AgriStack Farmer ID (India) or MOSIP equivalent	AgriStack / National Farmer Registry
	Plot ID with GeoJSON Polygon	GS1 GLN + GeoJSON (RFC 7946, WGS 84)	Bhulekh / National Land Records; AgriStack Farm Parcel Registry
	Sowing / Transplantation Date	Date (ISO 8601)	Farmer entry via OATS mobile app
	Area Sown under Crop	Numeric (hectares)	AgriStack Farm Parcel Registry
	Crop Variety Sown	Alphanumeric (ICAR code)	Farmer entry; cross-referenced to seed lot
3 – Crop Management and Growth	Input Product (Pesticide / Fertiliser) Name and CIBRC Registration Number	Alphanumeric	CIBRC registered products list (India); MAHA-TRACE input product registry
	Active Ingredient and Concentration	Text and numeric	CIBRC label; product manufacturer data sheet
	Application Date and Time	Timestamp (ISO 8601)	Farmer or FPO agent entry via OATS mobile

			app
	Dosage and Quantity Applied	Numeric with unit of measure	Farmer or FPO agent entry
	Pre-Harvest Interval (PHI) Compliance Verification	Date or flag	System-computed from application date + label PHI
	Irrigation Event *(optional, for water-stressed commodities)*	Timestamp and volume	Farmer entry or IoT soil-moisture sensor
4 – Harvest and On-Farm Handling	Harvest Lot ID (Traceability Lot Code)	Harvest LOT ID as EPCIS event	OATS system-generated at harvest CTE
	Harvest Date(s)	Date or date range	Farmer or FPO agent entry
	Harvested Quantity per Plot	Numeric (kg or MT)	Farmer or FPO agent entry; weighbridge record where available
	Crop Variety Confirmation at Harvest (GI-relevant)	Alphanumeric	Farmer or FPO agent visual declaration; APEDA for export crops
	Post-Harvest Handling Method	Categorical (crate / bag / bin) + text	Farmer or FPO agent entry
	Farm-Gate Temperature (cold-sensitive crops)	Numeric (°C) + timestamp	IoT sensor at farm-gate cold storage; manual log
5 – Primary Aggregation and Trade	FPO or Trader ID	GS1 GLN linked to NABARD FPO Registry / APMC license	FPO Registry; APMC Secretariat
	Aggregation Lot ID	GS1 SSCC (parent) + LGTINs (children)	OATS system-generated at aggregation CTE
	Contributing Farm IDs and Quantities	Structured list	Derived from child LGTINs; reconciled against farmer records
	Mandi Arrival Weight and Date	Numeric + Date	eNAM API or mandi weighbridge record
	eNAM Lot ID Cross-Reference *(where applicable)*	Alphanumeric	eNAM platform API
6 – Processing and Transformation	Processor / Packhouse GLN	GS1 GLN linked to APEDA packhouse code and FSSAI license	OATS Facility Registry; APEDA HortiNet; FSSAI
	Processing / Transformation Batch ID	GS1 LGTIN (output)	OATS system-generated at TransformationEvent
	Input Lot IDs and Quantities	Structured list of Lots with quantities	OATS TransformationEvent input EPC list
	Output Lot IDs and	Structured list of	OATS

	Quantities (Mass Balance)	Lots with quantities	TransformationEvent output EPC list
	Processing Parameters (Commodity-Specific)	Numeric (various units)	Processor QC system; MAHA-TRACE or equivalent entry
	Cold Chain Records (Temperature, Humidity, Duration)	IoT time-series or manual log	IoT sensors via FIWARE NGSI-LD; manual log
7 – Quality Testing and Certification	Lab Sample ID	Alphanumeric (LIMS-generated)	NABL-accredited lab LIMS; APEDA HortiNet for export
	Test Parameters and Results (MRL / Residue)	Numeric + pass/fail against destination market limit	NABL lab; APEDA HortiNet for export
	Certification Type and Certificate ID	Verifiable Credential (W3C VC Data Model 2.0)	Certification body (NPOP, GLOBALG.A.P., GI Registry, Agmark, FSSAI)
	Certifier DID and Digital Signature	W3C DID + Ed25519 signature	Certification body's OATS-registered DID
	Certificate Validity Dates	Date range	Certification body records
8 – Export Packaging and Shipment	Export Consignment ID / SSCC	GS1 SSCC (18-digit)	OATS system-generated at palletisation
	APEDA Registration Number / IEC	APEDA Reg. No. / DGFT IEC	APEDA registration database
	Shipping Bill / AWB / BoL Number	Alphanumeric	ICEGATE (CBIC); airline or shipping line
	Container ID and Seal Number	ISO 6346 container ID + seal no.	Shipping line; Customs seal
	Destination Country and Importer Details	Text / structured	Exporter entry in OATS; export documents
	Due Diligence Statement (DDS) Reference (EUDR)	Alphanumeric	EU TRACES-NT DDS submission
	Phytosanitary Certificate (ePhyto)	Verifiable Credential	Plant Quarantine Authority
9 – End Consumer / Retail	Retail GLN	GS1 GLN	Retailer OATS registration
	GS1 Digital Link QR (Consumer-Facing)	GS1 Digital Link URI	Packhouse QR at packing; consumer scan
	GTIN of Final Product	GS1 GTIN (14-digit)	Product manufacturer / packer
	Retail Selling Date *(optional)*	Date	POS system integration (optional)

6.4 The Five EPCIS Event Types: Functional and Technical Mapping

EPCIS 2.0 defines five event types. OATS implements all five, each maps to specific Critical Tracking Events and specific business semantics.

- **Object Event** records an observation, transition, or addition of one or more objects with no aggregation or transformation: harvest, dispatch, arrival, observation. The most common event type — used at CTE-01, CTE-02, CTE-03, CTE-04, CTE-06, CTE-08, CTE-09, CTE-10. Three actions: ADD (new identity entering supply chain), OBSERVE (existing identity at new location), DELETE (identity leaving supply chain).
- **Aggregation Event** records the physical containment of child objects within a parent object — without changing any identities. The parent (typically an SSCC pallet or container) and all child LGTINs retain their identity. Used at CTE-05 (FPO aggregation). Two actions: ADD (children attached to parent) and DELETE (children separated from parent).
- **Transformation Event** records the consumption of input identities and creation of output identities — a complete identity transition in which old identities cease to exist as carriers of new business state and new identities are born. Used at CTE-07 (Processing/Packhouse Transformation). The single most critical event for chain continuity — failure to capture TransformationEvents correctly breaks the upstream-to-downstream link permanently.
- **Transaction Event** records a commercial or legal linkage between one or more objects and one or more business transactions (purchase orders, invoices, shipping bills) — separate from physical movement. Used to record Approve, Confirm, and Commercial Invoice VC linkages.
- **Association Event** *(new in EPCIS 2.0)* records the binding or unbinding of a physical or digital artefact to a primary object — most importantly, the linkage of an IoT sensor to a lot, or a QR code to a lot. Two actions: ADD (binding) and DELETE (unbinding). The carrier mechanism for the new HOW dimension.

6.5 Sensor Data and Cold Chain Integration (EPCIS 2.0 ‘How’ Dimension)

Sensor data integration matters because food safety and quality compliance increasingly depend on documented environmental conditions, not just identity and location. A pomegranate consignment may be perfectly traceable but commercially worthless on arrival if cold-chain breaches during transit were not detected and remediated. EU and FDA inspections increasingly require demonstrable cold-chain compliance evidence; cargo insurance claims require non-repudiable sensor records.

The **EPCIS 2.0 sensor Element List specification** consists of arrays for sensor Metadata (device ID, calibration reference) and sensor Report (type, value, uom, time, min/max/mean). OATS ingests IoT sensor data via two open standards: **FIWARE NGSI-LD v1.6** for context-broker-based and **OGC Sensor Things API v1.1** for OGC-compliant IoT deployments. The OATS IoT Gateway converts both into EPCIS 2.0 sensor Element List payloads. **Association Event for Physical-Digital Sensor Linkage** — every IoT device (registered with a GIAI device ID) is linked to a lot or SSCC via an Association Event at deployment, ensuring verifiable provenance.

Cold Chain Compliance Verifiable Credentials. At the end of a defined cold chain custody interval (typically a container journey or a storage period), the responsible logistics operator or cold storage facility issues a **Cold Chain Compliance VC** as a W3C VC, cryptographically linked to the specific lot IDs covered. The VC carries aggregated sensor statistics (min, max, mean, breach events) and is signed with the operator's OATS-registered DID. The VC is a machine-verifiable claim that the cold chain was **Compliant**, **Conditional** (minor breach within acceptable tolerance), or **Non-Compliant** for the specified interval — and is a required component of the PEVC for cold-chain-sensitive exports; its presence or absence determines PEVC Compliance Engine pass/fail.

6.7 Transformation Event: Processing and Comingling

Transformation events are the most complex and most error-prone component of the OATS traceability model, and the principal failure point in real-world traceability systems. Transformation

events break traceability chains because the input identities are consumed at the moment new identities are created; if the cryptographic linkage between input LGTINs and output LGTINs is not recorded, the chain is permanently severed. Once severed, no downstream event can restore the link — the upstream farm-to-lot record becomes orphaned and the consumer-facing provenance claim becomes unverifiable.

Commingling and Identity Loss. Where transformation involves commingling multiple input lots into a single output lot (rice mill aggregating multiple farmer paddy lots), all input LGTINs are preserved as cryptographic references on the output LGTIN, and downstream events carrying the output LGTIN inherit the commingled lineage. Where pure commingling occurs in bulk storage (a grain elevator without lot-level identity preservation), the lot identity is lost and is recorded as such in the OATS lineage record; downstream traceability claims acknowledge the commingled state rather than presenting a false single-source claim.

6.8 FSMA 204 Compliance Mapping to EPCIS KDE

The FDA Food Traceability Final Rule mandates electronic lot-level traceability records for high-risk foods on the Food Traceability List, with FDA authorised to demand records within **24 hours**. FSMA 204 is format-agnostic; **GS1 US has published the GS1 US EPCIS Recommendations for FSMA 204 Critical Tracking Events (2023)**, mapping each FSMA KDE to a specific EPCIS 2.0 field. **OATS adopts this mapping directly**, every FSMA-required record is producible from the OATS EPCIS event store with no transformation other than format export.

The 24-Hour Data Provision Architecture. The FSMA 204 24-hour data provision requirement is architecturally demanding: when the FDA initiates a traceability investigation for an outbreak, all supply chain records for the implicated lots must be producible within 24 hours. This is achievable only if records are maintained digitally and are searchable in real time. Paper records or spreadsheet-based systems cannot satisfy this in practice. OATS satisfies the requirement by combining the EPCIS event store (Apache Kafka[71] backbone with append-only storage, content-addressed and hash-chained), the Lot Registry & Lineage Service for chain-of-custody assembly, and the FDA Sortable Spreadsheet exporter.

6.9 EU 178/2002 and Farm-to-Fork Alignment

EU Regulation (EC) No 178/2002 Article 18 is the foundational mandate of EU food traceability law: every food business operator placing food on the EU market must be able to identify the supplier of each food ingredient and the immediate recipient of each food product, the one-step-back/one-step-forward principle. The regulation applies to all food businesses regardless of size or product category. **EPCIS Event Chain as Article 18 Compliance Mechanism:** Article 18 traceability is fully satisfied by the OATS EPCIS event chain — each Transaction Event and Association Event records the upstream supplier (the source party DID) and the downstream recipient (the destination party DID), with cryptographic linkage to the underlying lot identifiers.

EU Farm to Fork Strategy Alignment. The EU Farm to Fork Strategy (May 2020), part of the European Green Deal, intensifies traceability obligations across the entire EU food value chain, reduced pesticide use, expanded organic farming, mandatory sustainability labelling. Every OATS issued PEVC for EU-destined lots carries the Farm to Fork data dimensions (pesticide application records, sustainability attestations, animal welfare where applicable) as standard fields drawn from the relevant OATS KDEs.

EU Deforestation Regulation (EUDR) Integration. Regulation (EU) 2023/1115 imposes mandatory deforestation-free verification for cattle, cocoa, coffee, oil palm, rubber, soy, and wood products entering the EU market. OATS supports EUDR through: geo-polygon recording at CTE-02 (Farm Registration); satellite-based deforestation verification); DDS (Due Diligence Statement) reference recording at CTE-09 (Export Shipment) as an OATS KDE; PEVC Compliance Engine enforcement at PEVC issuance for EUDR-covered commodities destined for the EU.

EU MRL Regulation (EC) 396/2005 Integration. Maximum Residue Levels for pesticides are enforced through Laboratory Test Report VCs (CTE-08) issued by NABL-accredited laboratories. Each VC carries pesticide-by-pesticide MRL compliance verdicts evaluated against the destination market's MRL profile (held in the OATS Product Registry per Ch 5 §5.6); the PEVC Compliance Engine blocks PEVC issuance for any consignment failing any MRL on the destination market's enforced list.

7. Physical-Digital Linkage: Identifiers, Carriers, and IoT Integration

This chapter builds on the logical traceability foundation established in previous chapter by addressing the critical challenge of reliably linking physical products to their corresponding digital event records. In a traceability DPI, this physical-digital linkage is foundational: a digital EPCIS event chain has no regulatory or commercial value unless it can be unambiguously tied to the actual physical lot it represents. OATS solves this through a coordinated architecture combining standardized data carriers such as QR codes, DataMatrix, RFID, and NFC; globally unique, web-resolvable identifiers using GS1 Digital Link; and IoT-based environmental monitoring integrated via standards like FIWARE NGSI-LD and OGC Sensor Things API. These components together operationalize the “How” dimension of traceability, ensuring that identifiers, conditions, and physical states are continuously and verifiably linked to digital records.

The chapter is positioned within the context of the global transition to next-generation identification systems, particularly the GS1 Sunrise 2027 shift from traditional one-dimensional barcodes to 2D, Digital Link enabled carriers. OATS is designed to be fully aligned with this transition from inception, enabling seamless integration with emerging retail and regulatory ecosystems. At the same time, it addresses the practical realities of smallholder-driven supply chains by incorporating low-cost, mobile-first, and offline-capable capture mechanisms, ensuring that robust physical-digital linkage can be achieved even in low-connectivity environments.

7.1 Physical Identifier Standards: QR Code, Data Matrix, RFID, NFC

An OATS lot identifier is useful only insofar as it can be reliably read from the physical product unit at every Critical Tracking Event. The choice of physical carrier is therefore a first-order architectural decision, not a peripheral packaging concern. OATS adopts a technology-neutral carrier framework: no single carrier is mandated for all use cases. Instead, four internationally standardized carrier technologies are accepted QR Code, GS1 DataMatrix, RFID (EPC Gen2), and NFC each appropriate to a specific combination of product unit, read environment, and actor capability. This pluralism is directly derived from OATS Principle Open by Default and Federated by Design: supply chain actors choose the carrier that best fits their operational context, and OATS event schemas accept events originating from any conformant carrier.
The common technical thread across all four carrier technologies is that each must encode, or resolve to, a GS1 Digital Link URI as specified in Section 7.2. This means that the physical identifier is never proprietary to OATS, to any specific application, or to any specific vendor it is a globally unique, web-addressable identifier resolvable from any standards-compliant reader. The mapping between carrier and encoded data is summarized below:

7.2 GS1 Digital Link: Web-Addressable Product Identifiers

The GS1 Digital Link standard (ISO/IEC 18975, originally published as the GS1 Digital Link URI Syntax v1.0 in 2018 and now at v1.3, 2023) is the single most consequential development in product identification since the introduction of the EAN/UPC barcode in 1974. It is the technical foundation that transforms a product barcode from a point-of-sale identifier into a web-addressable digital asset, and it is the OATS-mandated identifier syntax for all physical carriers. Every QR code, Data Matrix, RFID tag, or NFC chip in the OATS ecosystem either encodes a GS1 Digital Link URI directly or resolves to one through a registered GS1 Digital Link resolver as described in Section 7.8.

A GS1 Digital Link URL is a standard HTTPS address that combines GS1 identifiers as path components. At minimum, it contains the Global Trade Item Number (GTIN), with optional additions like Lot Number, Serial Number, and Expiry Date. The domain resolver provides relevant links such as product details, traceability, and regulatory documents.

7.3 GS1 Sunrise 2027: Transition to 2D Barcodes

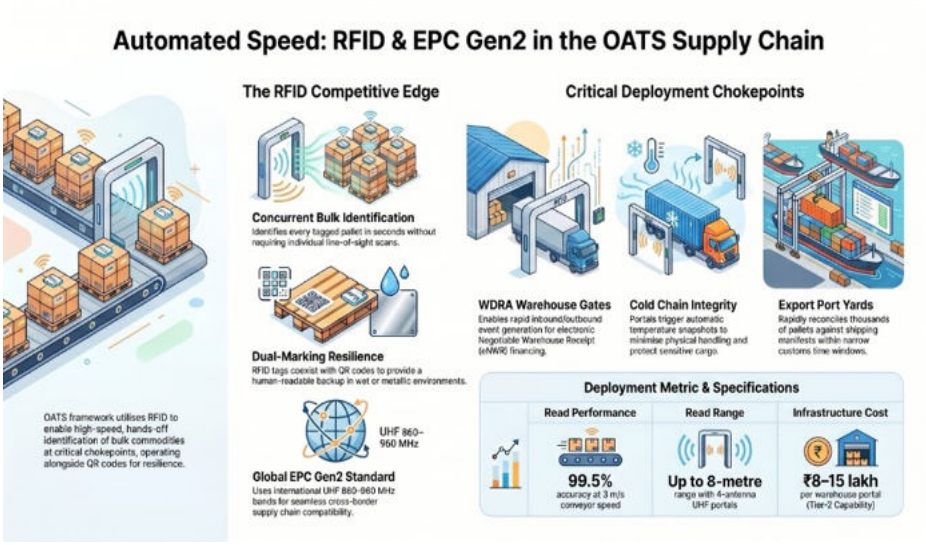
GS1 Sunrise 2027 is the global industry programme to transition worldwide retail point-of-sale systems from the legacy one-dimensional EAN/UPC barcode to 2D barcodes (QR Code and DataMatrix) by

2027. The transition matters for OATS because it makes consumer-facing traceability natively available at every retail checkout. Every OATS-compliant product becomes a smartphone scan away from verified government-anchored provenance.

Table 7.3.1 GS1 Sunrise 2027: Transition to 2D Barcodes

Actor Category	Pre-2027 State (Current)	Post-2027 OATS Target State
FPO / Packhouse / Processor	Manual paper-based lot labelling; occasional EAN-13 barcodes; QR codes only on premium product lines; no standardized lot number encoding	GS1 Digital Link QR code on every outbound carton and consumer pack; GTIN + Lot + Expiry + Serial (where applicable) encoded; thermal printer-based label print at FPO/packhouse; QR code pre-approved under OATS Labelling Conformance Test
Retailer (Modern Trade)	POS scanners read only 1D EAN/UPC barcodes; 2D scanners deployed only for specific use cases (pharma, electronics); no consumer-facing traceability access at shelf	POS scanners upgraded to omnidirectional 2D imagers (EAN/UPC backward compatible); shelf-edge digital signage displaying live OATS provenance data via Digital Link resolution; customer-facing app scan triggers full provenance display
Retailer (Traditional Trade / Kirana)	No POS scanning; paper-based sales; no digital product identification beyond manufacturer's pack	OATS Consumer App (Android PWA) enables any kirana customer to scan the QR code on any OATS-compliant product for provenance; no retailer-side investment required; OATS-anchored demand generation for traditional trade
Exporter / Port	Paper-based shipping manifests; EAN-13 on retail packs; SSCC labels on pallets; Shipping Bill linked manually to packing list	SSCC encoded as GS1 Digital Link on container and pallet labels; ICEGATE Shipping Bill auto-populated from SSCC scan; destination customs systems (TRACES NT, FDA PREDICT) query OATS resolver directly from the SSCC on the Customs Import Declaration
Consumer	Fragmented brand-specific QR codes; no standardized meaning; 5–20% scan rate at shelf; provenance data where available is marketing-driven, not verifiable	Every OATS-compliant product is a smartphone scan away from verified government-anchored provenance; scan rate target 60%+ for premium export commodities; provenance data is W3C Verifiable Credential-backed and legally admissible

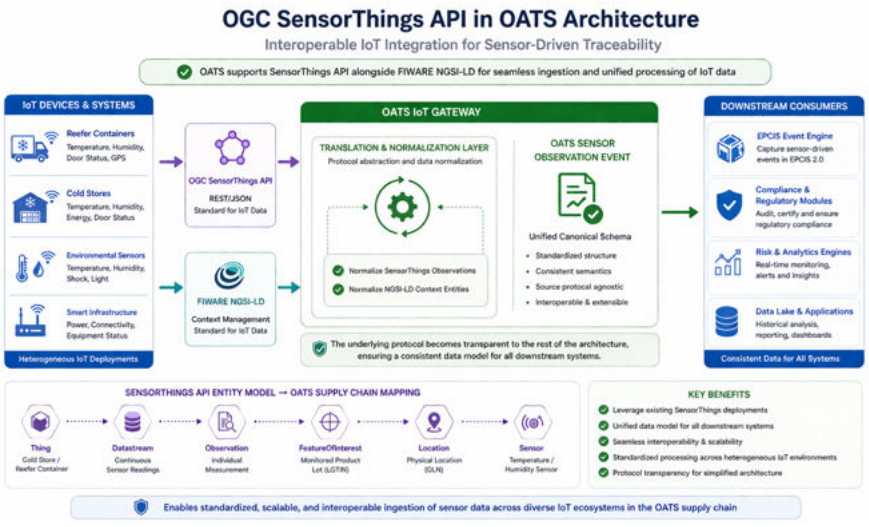
7.4 RFID and EPC Gen2 for Automated Bulk Identification



RFID complements 2D barcodes in OATS by enabling hands-off, bulk, and high-throughput identification at facility nodes where human scanning would be operationally prohibitive — WDRA warehouse gates, cold storage portals, and export port container yards.

The primary adoption barrier for RFID in Indian smallholder-dominated supply chains is not the tag cost (₹5–₹15 for passive SGTIN/SSCC tags is marginal against export-grade consignment values) but the fixed infrastructure cost of portals, antennas, and middleware — typically ₹8–15 lakh for a complete two-antenna warehouse portal. OATS positions RFID as a **Tier-2 conformance capability** applicable specifically to WDRA warehouses, large processing facilities, and port operators — not as a universal requirement. FPOs and smallholder-serving aggregators operate with QR-Code-only conformance at Tier-1 with no operational disadvantage.

7.5 IoT Integration: FIWARE NGSI_LD and OGC SensorThings API



This section addresses the dynamic dimension of traceability — how continuous environmental data (temperature, humidity, shock, GPS location, container access events) is captured, linked to specific OATS lots, and incorporated into the EPCIS event chain as the How dimension (Ch 6 §6.6). OATS supports two open IoT data standards. Both translate through the OATS IoT Gateway to the same canonical EPCIS AssociationEvent + sensor data extension — no canonical-output difference between the two ingress paths.

7.6 Cold Chain Monitoring: Temperature, Humidity and Shock Sensor

Cold chain integrity represents the most critical and high-impact IoT application within OATS, particularly for temperature-sensitive commodities — fresh horticulture, dairy, fisheries, meat, selected processed foods. Failures in maintaining prescribed environmental conditions during storage and transit are the leading cause of export rejections and consumer-side spoilage incidents. The OATS Cold Chain Commodity Registry maintains commodity-specific monitoring mandates; implementations must verify against destination-market regulations.

7.7 Field-Level and Farm-Gate Capture Devices

The most critical physical-digital linkage challenge in OATS occurs at the smallholder farm gate, where the first Critical Tracking Event is captured under constraints Limited connectivity, lack of infrastructure, and non-technical operators are the main ones. If traceability fails at this point, the entire downstream event chain loses integrity. OATS addresses this through a Farm-Gate Reference Implementation using low-cost, resilient, and user-friendly technologies organised around four architectural patterns as described in the table below:

Pattern	Specification	OATS Implementation
Smartphone Device	Android 8.0+ low-cost phones	QR scanning, GPS tagging, data entry, label generation
Offline Operation	Local encrypted storage	Sync with event engine when network available
QR Label Printing	Bluetooth thermal printer	Generates GS1 Digital Link-based lot labels
User Interface	Voice + vernacular UI	Guided data capture for non-technical users

7.8 Resolver Architecture and GS1 Digital Link Registry

All OATS identifiers resolve to GS1 Digital Link URLs). The resolver transforms these URLs into actionable responses for different actors (consumers, regulators, enterprise systems). It is not a simple redirection layer but a policy-driven, access-controlled gateway that determines what data is returned based on the identity and authorisation of the requesting party. The resolver orchestrates access to distributed data sources (product registries, EPCIS event chains, certification records), ensuring each request receives the appropriate view.

Resolver Functions and Architecture. Five core functions: URI parsing and normalisation; content negotiation based on request type; access policy enforcement; federated data retrieval from authoritative sources; response composition. Implemented as a stateless, horizontally scalable microservice deployed across multiple geographic regions with CDN support to ensure low latency and high availability. The resolver does not store product data — it dynamically fetches from OATS registries and EPCIS repositories, aligning with the federated architecture principle and avoiding duplication of authoritative datasets.

Requesting Actor	Authentication Method	Resolver Response Content
Consumer	None	Product provenance summary, certifications, cold chain status, recall flag
Supply Chain Actor	DID + OAuth / mTLS	Provenance plus role-specific commercial data
Regulatory Authority	Government DID + mTLS	Full EPCIS event chain, KDEs, VCs, IoT data access
Customs Systems	Cross-border credentials	PEVC record and compliance summary
Retailer Systems	OAuth client credentials	Structured product master data and integration feeds

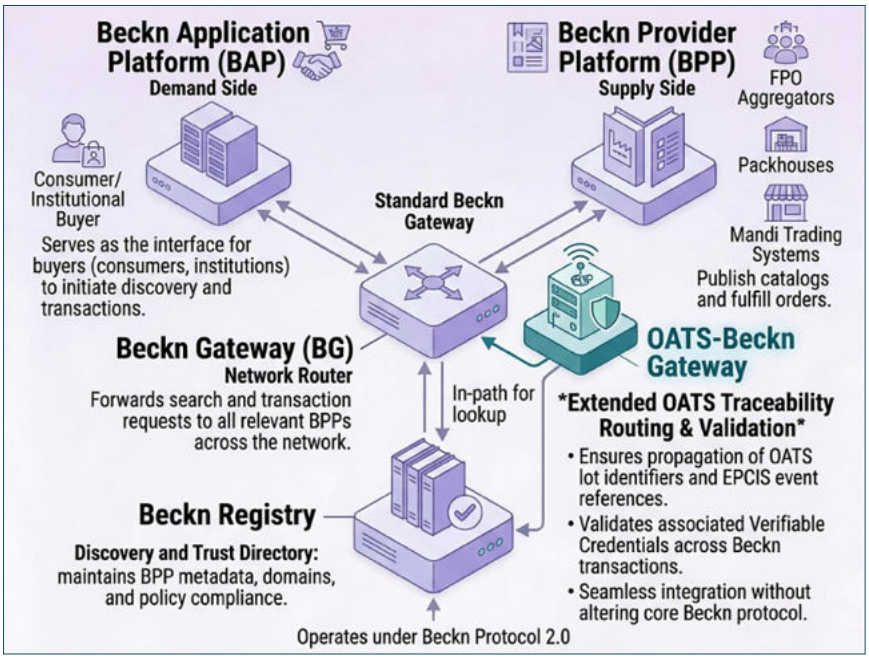
Digital Link Registry and Federation. The OATS Digital Link Registry maintains all resolvable URI patterns and associated access policies. It is populated through integration with product registration workflows and national GS1 systems, ensuring consistency of identifiers. For cross-border scenarios, the resolver federates with global GS1 resolver networks, enabling OATS-generated identifiers to resolve seamlessly in other jurisdictions without requiring duplication of infrastructure across countries.

8. Open Network Layer: Beckn Protocol Integration and the OATS-Beckn Specification

OATS does not invent a new commerce protocol. The decentralised, open-source, four-actor Beckn Protocol, already operating at population scale through ONDC and MahaVISTAAR, is the parent protocol from which OATS derives its open network layer. This chapter specifies the Beckn-derived **OATS Protocol**, the **OATS-Beckn Interface Specification** that embeds traceability into commerce messages without forking Beckn, the **seven-stage OATS Network Lifecycle** mapped to EPCIS 2.0 events, the **eleven OATS Network Policies (NP-01 to NP-11)** that govern operator conduct, and the production-grade reference networks (ONDC, VISTAAR / MahaVISTAAR) against which conformance is tested.

8.1 Beckn Protocol: The Parent of the OATS Protocol

The Beckn Four-Actor Model. A Beckn network has four roles: the **Beckn Application Platform (BAP)** is the consumer-facing or buyer-facing application; the **Beckn Provider Platform (BPP)** is the supplier-facing or seller-facing application; the **Beckn Gateway** is the network discovery layer that routes search requests to matching BPPs; and the **Beckn Registry** is the directory of all certified participants. There is no central commerce platform — every transaction is bilateral between a BAP and a BPP, mediated only by the discovery Gateway.



Beckn Transaction Primitives. Beckn defines eight commerce APIs paired as request-callback couples. The OATS Protocol maps each Beckn API to a specific traceability outcome — the carrier mechanism that allows traceability to be embedded inside commerce without duplicate data entry.

8.2 The OATS Protocol: A Beckn-Derived Traceability Protocol

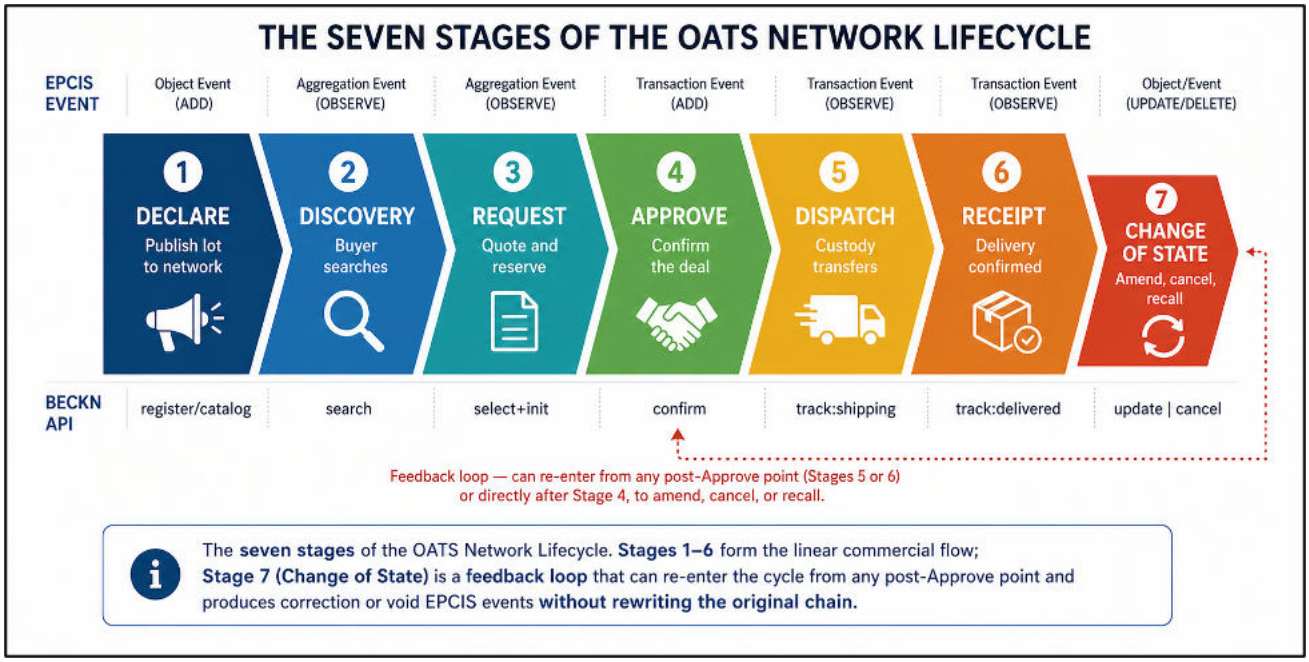
The **OATS Protocol is a superset of Beckn Core v1.1**, every OATS message is a syntactically valid Beckn message (Network Policy NP-04). The relationship is parent-child, not fork: OATS adds traceability semantics without modifying any Beckn field.

What the OATS Protocol Inherits from Beckn. The four actor model (BAP, BPP, Gateway, Registry); the eight transaction primitives and their callback structure (signed message envelopes with sender DID + payload + signature; the participant Registry with discovery semantics; the tag-group extension mechanism for domain-specific fields; the Online Dispute Resolution (ODR) framework).

What the OATS Protocol Adds to Beckn. A **Seven-Stage Network Lifecycle** (Declare, Discovery, Request, Approve, Dispatch, Receipt, Change of State); **traceability extension fields** carried in the Beckn tag-group mechanism); **deterministic EPCIS event derivation** from authenticated Beckn messages by the OATS-Beckn Gateway; the **OATS Operator License** as the participant credential;

eleven Network Policies governing operator conduct; **Verifiable Credentials embedded** in catalogue responses for compliance proof; **multi-domain coordination** for cross-network traceability.

8.3 The OATS Network Lifecycle: Seven Stages



Every OATS-traced commercial flow proceeds through seven stages as depicted in figure above. . Each stage corresponds to specific Beckn API calls and produces (or does not produce) specific EPCIS events. The seven stages are the universal vocabulary across all OATS participants regardless of commodity sector.

The transition from Approve to Dispatch is the shift from commercial commitment to physical fulfilment and may transfer custody to another network domain. Stage 7 is the only stage that can alter the EPCIS event chain post-Approve, and does so by appending new, referenced events without modifying the original chain.

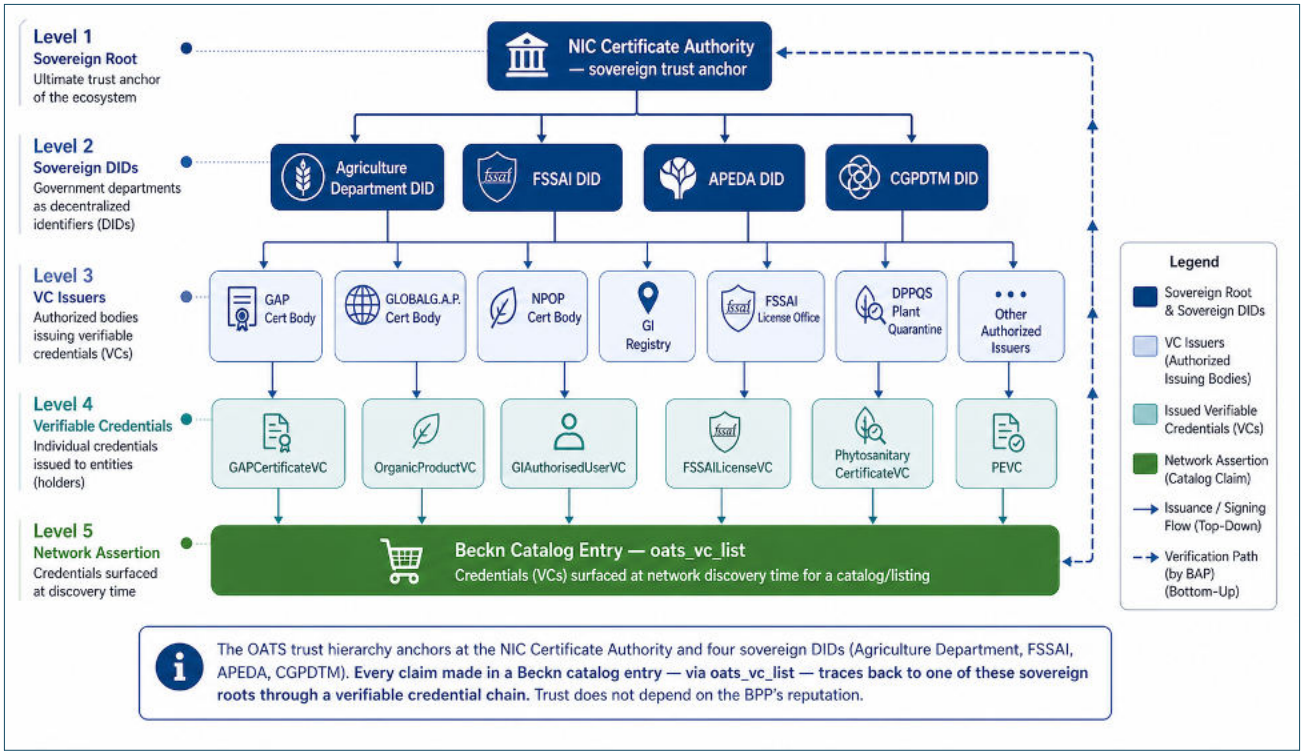
8.4 OATS Network Policies

The OATS Network Policy Framework is a deliberate inheritance from the ONDC Participant Policy and Beckn Foundation participant requirements. It does not replace those frameworks; it extends them with the specific obligations traceability-grade conformance demands. **A participant in good standing under ONDC and the Beckn Foundation is not, by virtue of that standing alone, an OATS Protocol participant.**

8.5 Beckn + Verifiable Credentials: Trust Layer Design

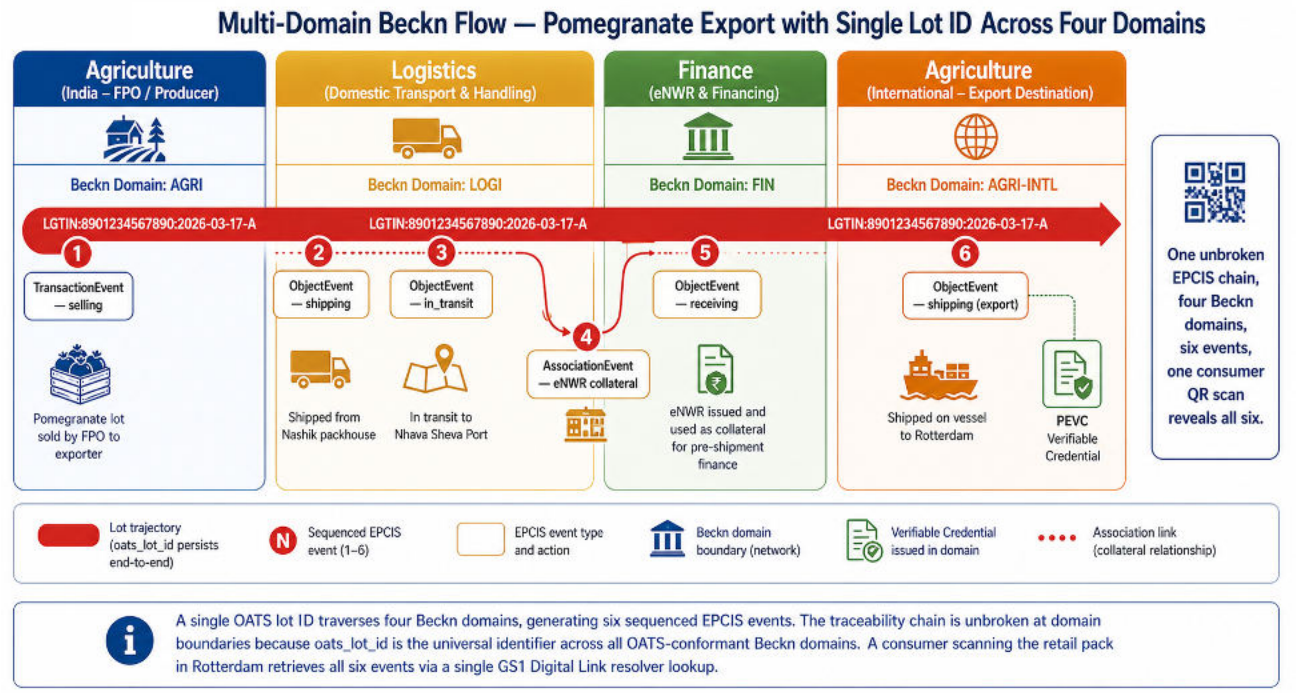
The OATS-Beckn Catalog Extension defines an oats_vc_list field that carries an array of Verifiable Credential references, each containing: VC type identifier; issuer DID; credential subject identifier; status list URI; expiration date. The full VC payload is not transmitted in the Beckn message, only the reference. The receiving BAP resolves the VC from the issuer's DID document or from the OATS VC registry, verifies the cryptographic signature, checks the revocation status via the issuer's Status List 2021 bitstring, and uses the validated VC content for compliance decisioning. This **resolution-not-transmission pattern** preserves issuer privacy, keeps Beckn payloads small, and ensures every BAP-side compliance check uses the freshest revocation state.

Selective Disclosure and the Minimum-Disclosure Principle. Where a destination market requires only a subset of credential fields (an EU retailer needs proof of GLOBALG.A.P. certification but not the auditor's specific identity), the OATS Wallet generates a **selective disclosure proof** using **BBS+ signatures** (per the W3C VC Data Integrity specification), revealing only the required claims while keeping the certification cryptographically verifiable. This satisfies NP-07 (minimum disclosure) and reduces commercial data leakage across supply chains. **Trust Chain to the Sovereign Root.** Every OATS VC is ultimately signed by an entity whose DID is registered in the OATS Layer 1 Registry, which is itself anchored by the Agriculture Department's sovereign root DID. A destination-country verifier can trace any leaf VC (a farmer's GAP certificate, an exporter's PEVC) back to the sovereign root through a single chain-of-signatures verification — eliminating the trust gap that has historically constrained mutual recognition of agri certifications across jurisdictions.



8.10 Cross-Network Traceability: Multi-Domain Beckn Flows

A complete agri-food commercial flow rarely lives within a single Beckn domain. A typical export transaction crosses four: Agriculture (primary commodity sale, FPO to exporter), Logistics (transport from packhouse to port), Finance (WDRA eNWR-backed working-capital lending against in-transit stock), and potentially Retail (domestic surplus not exported). The OATS Protocol solves the domain-crossing problem through a single invariant: the oats_lot_id is the universal traceability identifier across all Beckn domains. Every domain-specific confirm that references an OATS-traced lot carries the same oats_lot_id in its OATS-Beckn extension fields. The OATS event repository assembles the lot's full event chain by aggregating all EPCIS events keyed on thatlot ID, regardless of which Beckn domain produced them.



Consider a 5-tonne Bhagwa pomegranate lot, OATS lot ID LGTIN:8901234567890:2026-03-17-A, originating at an FPO in Nashik destined for an EU importer in Rotterdam.

Step	Beckn Domain	Lifecycle Stage	Commercial Transaction	EPCIS Event Generated
1	Agriculture	4. Approve	FPO-Nashik-Alpha (BPP) confirms sale to Export-House-Mumbai (BAP) on ONDC Agriculture.	TransactionEvent. Source GLN: FPO packhouse. Destination GLN: Export House aggregation facility. bizStep: selling.
2	Logistics	5. Dispatch	Export House (BAP) confirms transport with RefrigeratedTransport-Provider (BPP) on ONDC Logistics; pickup at FPO packhouse.	ObjectEvent bizStep=shipping at origin. oats_transport_sensors and oats_cold_chain_profile (5–8°C, 85–90% RH) declared.
3	Logistics	5. Dispatch (in-transit)	In-transit track events at 30-minute intervals, plus alert events on telemetry excursions.	ObjectEvent bizStep=in_transit with sensor reading windows. Cold-chain breach produces an OATS Alert Event independently.

4	Finance	7. Change of State (Associate)	Export House (BAP) confirms working-capital loan from NABARD-Refinanced-Bank (BPP) on ONDC Finance, collateralised by the in-transit lot.	AssociationEvent linking the lot to an eNWR financial instrument. eNWR reference validated against WDRA platform (Chapter 4 §4.4.1).
5	Logistics	6. Receipt	Delivery confirmation at Mumbai port; transporter BPP issues on_track with state=Order-delivered.	ObjectEvent bizStep=receiving at the port. Final telemetry window attached; oats_cold_chain_compliant=true if no breach.
6	Agriculture (international)	1. Declare → 4. Approve	Export House (BPP) issues PEVC-backed catalog listing to EU-Importer (BAP) on an international Beckn network or through APEDA TRACES-NT; confirm constitutes the export shipment event.	ObjectEvent bizStep=shipping with the PEVC Verifiable Credential embedded via oats_vc_list. Phytosanitary Certificate VC also attached; ePhyto Hub transmission triggered in parallel.

Consent and Authorisation Across Domains. Each domain crossing carries a DPDPA-aligned consent artefact) under DIF Presentation Exchange v2.0: Logistics receives lot ID, dimensions, weight, cold-chain profile; Finance receives lot ID, valuation, eNWR reference; Retail receives lot ID, certifications, origin claims; Agri-international receives the full EPCIS chain plus PEVC. A farmer who later withdraws consent triggers DPDPA-compliant retrospective minimisation across all domains that received the data. **Cross-Domain Dispute Resolution.** Disputes spanning multiple domains escalate to tier-2 (OATS Operator Registry) where the EPCIS chain is the authoritative evidentiary record; commercial disputes within a single domain remain at tier-1 (ONDC ODR for ONDC domains) — preserving the hourglass-waist invariant that regulatory traceability decisions are grounded in the same standardised event-chain evidence regardless of detection domain.

9. Blockchain and Distributed Ledger Integration

This chapter defines the role of Distributed Ledger Technology (DLT) within the OATS architecture as a trust-anchoring sub-layer, complementing but not replacing the canonical event and registry systems. OATS does not treat blockchain as a default data store; instead, it applies a principled decision framework to determine when DLT provides net value over traditional databases. The core principle is selective anchoring: high-value, compliance-critical events such as certification issuance, lot-level compliance milestones, and cross-border attestations are cryptographically anchored on a distributed ledger, while high-volume operational data such as EPCIS event payloads and IoT telemetry remain in scalable off-chain systems.

The chapter evaluates permissioned ledger platforms including Hyperledger Fabric, Hyperledger Besu, IOTA, and CORD, assessing their suitability for different OATS deployment contexts such as government-regulated supply chains, IoT-heavy environments, and financial settlement layers. It further specifies how W3C Verifiable Credentials Data Model 2.0 are anchored on DLT through hash commitments, enabling tamper-evident verification without exposing sensitive credential content. Smart contracts are introduced as automation mechanisms for compliance validation, recall triggers, and conditional workflows, while governance frameworks define node participation, consensus models, and access control for shared ledgers.

The chapter also draws lessons from existing implementations such as IBM Food Trust, TradeTrust, and Maha-TRACE, highlighting practical considerations in scalability, interoperability, and governance. It concludes with detailed Functional and System Requirement Specifications that define how blockchain integration must operate within OATS, ensuring that DLT enhances trust, auditability, and cross-border interoperability without introducing unnecessary complexity or performance constraints.

This chapter outlines DLT's role in OATS as a trust-anchoring layer, supplementing existing event and registry systems rather than replacing them. Blockchain is not used as a default data store; instead, only compliance-critical events—such as certifications and cross-border attestations—are anchored, while routine data stays off-chain in scalable systems.

The chapter reviews permissioned ledger options like Hyperledger Fabric, IOTA, and CORD for various OATS scenarios, explains how W3C Verifiable Credentials are anchored through hashes for tamper-evident validation, and describes smart contracts for automated compliance. Governance frameworks address node participation and access control.

It summarises lessons from projects like IBM Food Trust and Maha-TRACE, and provides Functional and System Requirements to ensure DLT integration supports trust, audit, and cross-border interoperability without causing complexity or performance issues.

9.1 The Role of Blockchain in Traceability DPI: Principles and Boundaries

Evaluated against OATS Unified Principles - interoperability, technology sovereignty, data sovereignty; **only four narrowly defined DLT use cases are legitimate in OATS**, all focused on trust anchoring and multi-party verification rather than data storage or transaction processing.

Event Hash Anchoring — cryptographic hashes of batched GS1 EPCIS 2.0 events are anchored on a shared ledger. Any participant or regulator can independently verify that an event existed at a specific point in time and has not been altered. Full event payload remains in federated repositories.

Verifiable Credential Lifecycle Anchoring — issuance and revocation states of licences, certifications, and compliance attestations are anchored. Cross-border authorities can validate credential authenticity and status without real-time access to the issuing authority.

Consortium-Governed Registry State — critical registry updates requiring multi-party trust (identifier assignments, system registrations) are recorded on the ledger, preventing unilateral modification by any single entity.
Automated Compliance and Recall Smart Contracts — deterministic rules (regulatory thresholds, traceability completeness, recall propagation) executed on-chain for verifiable enforcement.

9.2 Decision Framework: When to Use DLT vs Traditional Database

OATS adopts and extends the **NIST IR 8202** decision framework, adding governance, federation, and substitutability criteria aligned with OATS principles. The framework is **mandatory for all jurisdictions implementing OATS components** and must be formally evaluated and documented before any DLT adoption decision.

Table 9.2.1 — The OATS DLT Decision Framework.

Decision Criterion	Use DLT if…	Use Traditional Database if…
Multiple writers	Three or more independent parties must write to a shared record without a trusted arbiter	A single authority controls and maintains the record
Trust topology	Parties require independent verification and do not trust a central operator	A trusted central operator exists and is accepted by all
Immutability requirement	Tamper-proof history is essential and must be cryptographically verifiable	Records require legitimate updates, corrections, or deletion
Disintermediation value	Removing intermediaries reduces cost, latency, or dependency	Intermediaries provide trusted and necessary oversight
Data sensitivity	Only non-sensitive metadata or hashes are stored	Data includes personal, confidential, or regulated information
Transaction volume and latency	Throughput and latency constraints are compatible with ledger performance	High-frequency or real-time processing is required
Governance maturity (OATS-specific)	A multi-stakeholder consortium with defined governance exists	Governance is centralized or undefined
Federation compatibility (OATS-specific)	Anchoring supports distributed data ownership and federation	Use would centralize data unnecessarily
Substitutability (OATS-specific)	Implementation remains vendor-neutral and replaceable	Design depends on a specific vendor or platform

Within OATS, the validated DLT use cases satisfy all criteria, while non-approved uses fail one or more conditions. This ensures that DLT is applied only where it strengthens trust without compromising scalability, privacy, or interoperability. The assessment outcome must be documented and submitted to the OATS governance process before implementation.

9.3 Mapping DLT to the OATS Five-Layer Architecture

DLT in OATS is **not implemented as a standalone layer but as a trust-anchoring sub-layer embedded primarily within Layer 2**, with selective extensions into Layers 1 and 3. Layer 2 (the hourglass waist, Ch 4 §4.5) combines event traceability and blockchain anchoring, making it the natural integration point. The canonical traceability record remains the GS1 EPCIS 2.0 event; DLT operates alongside by anchoring cryptographic proofs rather than storing operational data.

9.4 Permissioned DLT Architectures: Hyperledger Fabric and Hyperledger Besu

OATS specifies two reference implementations for permissioned DLT deployments. **Hyperledger Fabric 2.5+** is the OATS DLT Reference Implementation A, the default choice for event anchoring, VC state, and registry updates. **Hyperledger Besu (QBFT or IBFT 2.0)** is OATS DLT Reference Implementation B, recommended where EVM smart-contract portability is required

9.5 IOTA Tangle and Feeless IoT-Native Anchoring

The IoT layer in OATS generates extremely high-frequency telemetry from cold-chain sensors, farm weather stations, and logistics trackers, hundreds of thousands of readings per day at production scale. Anchoring each individual reading on a permissioned ledger is technically feasible but operationally inefficient. OATS introduces **IOTA as a secondary, telemetry-specific anchoring layer**: IOTA's feeless architecture, scalability with network participation, and MQTT compatibility make it suitable for high-volume machine-generated data. **It complements, not replaces, the primary permissioned ledger.**

9.6 W3C Verifiable Credentials Anchored on DLT

OATS uses **W3C VC Data Model 2.0** as the foundation for representing certifications, licences, and compliance attestations. While VCs are inherently verifiable through cryptographic signatures, two requirements necessitate DLT anchoring: efficient and tamper-evident revocation checking; and timestamped proof of issuance acceptable across jurisdictions.

9.7 Smart Contracts for automated Compliance and Recall Orchestration

In OATS a smart contract is a **narrowly-scoped, deterministic program** executed on a permissioned ledger — Fabric chaincode or Besu Solidity. Smart contracts are permitted only where three conditions are satisfied: the governing rule is fully specified in machine-readable regulatory form; execution is deterministic across all nodes; outcomes must be independently verifiable by all consortium members, including destination-country authorities. **Smart contract scope is restricted to objective, rule-based validation** — functions involving discretionary judgement, AI inference, or dependence on private off-ledger state are not implemented on-chain. Such processing is performed by off-ledger systems (compliance engine, analytics layer), with their outputs anchored to the ledger for verification. The ledger remains a trust-verification layer, not a computation-heavy decision engine.

9.8 Governance of Shared Ledgers: Consortium Models and Node Roles

A permissioned ledger derives its trust not from technology alone but from transparent, multi-stakeholder governance. OATS operationalises this through a consortium model under the **Multi-Stakeholder Governance Council** defined in Chapter 3.

10. OATS API Architecture, Microservices, and Integration Framework

Chapter 10 defines the **implementation layer that operationalizes the five-layer OATS architecture from Chapter 4**, specifying how each building block is exposed, orchestrated, and integrated through standardized APIs and microservices. It does not introduce new functional components; instead, it provides the **execution framework** that binds Layer 1 (Identity, Trust & Registry), Layer 2 (Event, Traceability **O**pen **P**rotocol & Blockchain Anchoring), Layer 3 (Interoperability and Open Protocols), Layer 4 (Consent and Governance), and Layer 5 (Applications) into a cohesive, interoperable system.

The API architecture is **REST-first, based on OpenAPI 3.1**, forming the canonical interface surface across all layers. Each Layer 4 building block defined in Chapter 4 (e.g., DID Service, Registry Service, EPCIS Event Router, VC Service, OATS-Beckn Gateway) exposes standardized APIs that are consumable across jurisdictions and systems. Federated data exchange is implemented using the GovStack Information Mediator (X-Road pattern), ensuring that data remains at source nodes while being securely discoverable and queryable. This directly enforces OATS principles of federation and data sovereignty established in Chapters 2 and 4.

Microservices are structured **one-to-one with OATS building blocks**, ensuring strict separation of concerns and independent scalability. The EPCIS Event Router, IoT Gateway, Registry Services, and Compliance Engine operate as autonomous services, communicating through an **event-driven architecture using Apache Kafka**. This supports high-throughput ingestion of traceability events and IoT telemetry while maintaining consistency with the Layer 2 hourglass model. For Layer 5 applications and analytics, GraphQL is introduced as an aggregation layer that composes data from multiple services without duplicating underlying data.

Security and integration follow a **zero-trust model anchored at the API Gateway**, where every request is authenticated, authorized, and audited. Mutual TLS, OAuth 2.0, and policy-based access control are enforced consistently across all inter-layer interactions defined in Chapter 4 Section 4.9. Additional integration mechanisms include webhooks for asynchronous notifications, developer sandbox environments for onboarding, and standardized interface contracts that ensure interoperability across national and cross-border deployments.

The deployment model aligns with the **federated topology defined in Chapter 4 Section 4.8**, where microservices may be deployed across sovereign infrastructure, certified cloud environments, or hybrid configurations. Each jurisdiction operates its own service instances while remaining interoperable through shared API specifications and open protocols.

OATS

PART III

GOVERNANCE, DATA RIGHTS & REGULATORY COMPLIANCE

CHAPTERS 11-14

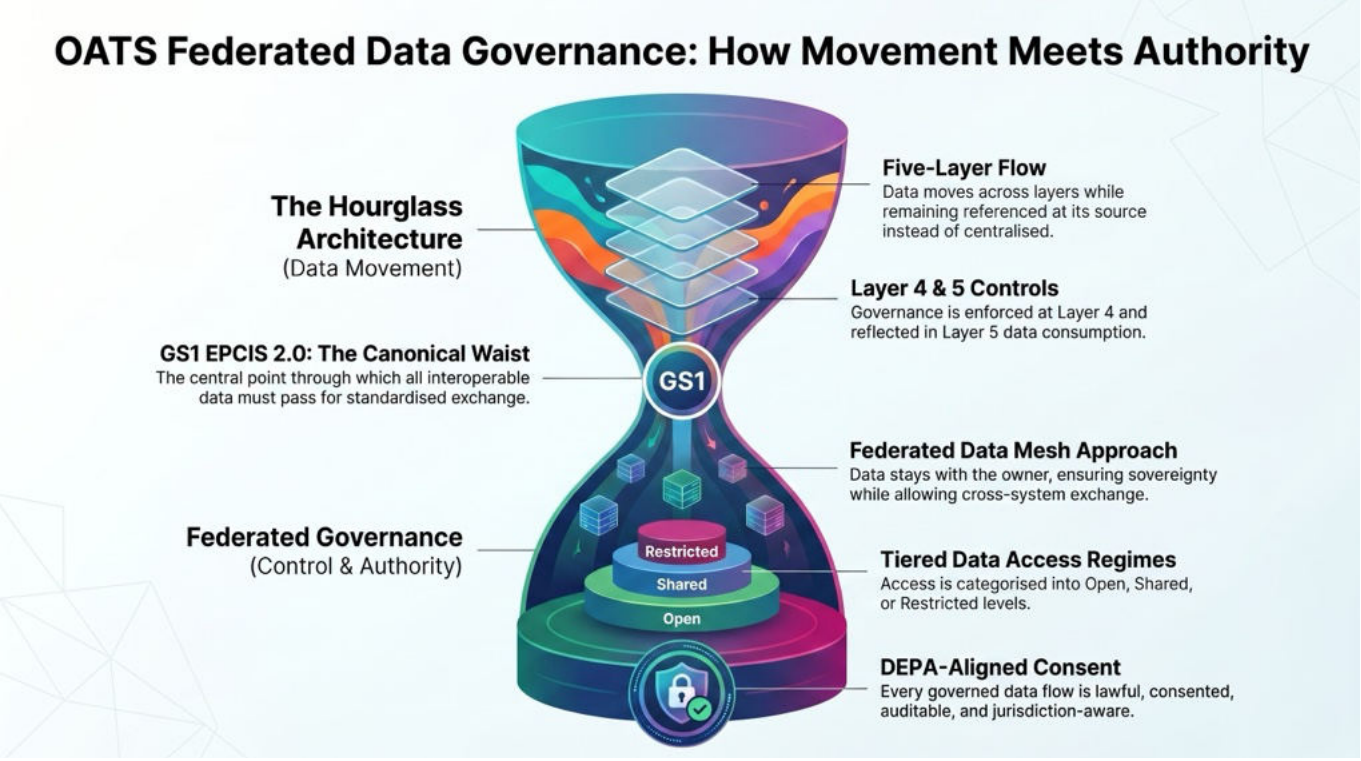


- OATS data governance philosophy - federated, sovereign, auditable; three governance pillars and data-mesh architecture
- Tiered data access - Open · Shared · Restricted; cross-jurisdiction data-flow governance; data retention and right-to-erasure
- The ORGANS consent framework - Open, Revocable, Granular, Auditable, Notice-based, Selective consent
- DPDPA 2023 alignment; Consent Manager architecture and consent-artefact lifecycle
- Regulatory framework - GI / Protected Designation of Origin and Organic certification
- Zero-trust cybersecurity — IAM (role + attribute-based), PKI hierarchy, audit logging & non-repudiation, DPIA framework

11. Data Governance Architecture and Federated Data Model

OATS is a commodity-agnostic, jurisdiction-neutral Digital Public Infrastructure in which data does not merely flow, it is governed. Chapter 4 established the five-layer architecture and the hourglass model, with GS1 EPCIS 2.0 as the canonical data exchange waist through which all interoperable data passes. Chapter 11 complements that foundation by defining the authority, control, and accountability structures that govern this flow. Where Chapter 4 specifies how data moves across layers, Chapter 11 specifies under whose authority it moves, under what permissions, and with what obligations. The hourglass remains intact: all cross-system exchange continues to pass through Layer 3, while governance controls are enforced through Layer 4 and reflected in Layer 5 consumption.

The OATS data governance model is explicitly federated. Data remains at its source in Layer 1 and Layer 2 systems, is referenced rather than centralized, and is exchanged through standardized interfaces without compromising ownership or sovereignty. This chapter formalizes the data mesh approach for agri-food traceability, defines tiered data access regimes (Open, Shared, Restricted), establishes data stewardship responsibilities, and embeds DEPA-aligned consent into every governed data flow. Together, Chapter 4 and Chapter 12 form a single load-bearing system: the hourglass architecture ensures interoperability and standardization, while the federated governance model ensures that every data movement is lawful, consented, auditable, and jurisdiction-aware.



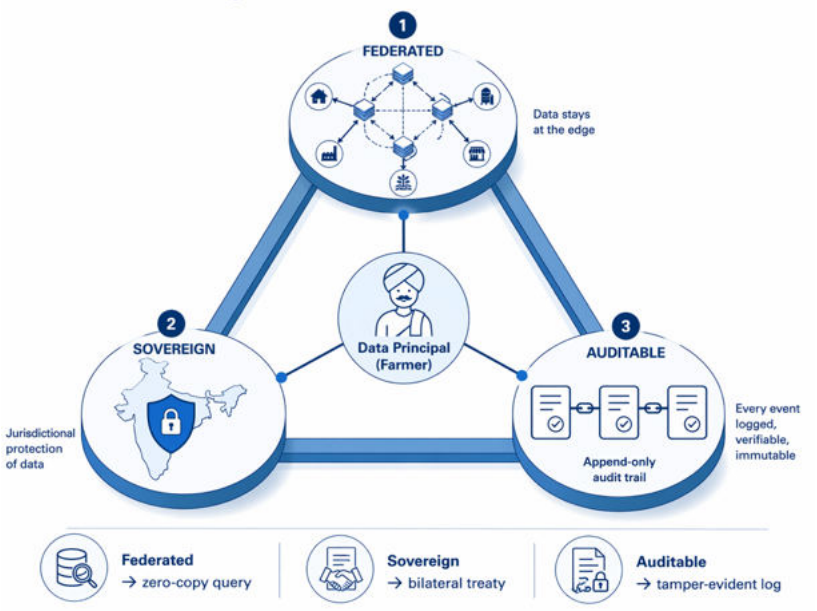
11.1 OATS Data Governance Philosophy: Federated, Sovereign, Auditable

11.1.1 The Three Governance Pillars

Federated: Event data is owned and stored at the originating domain node (Layer 1 / Layer 2) of the actor that generated it. The system does not centralize raw data. OATS Core Services maintain a minimal metadata index (event hashes, lot identifiers, actor DIDs, timestamps, credential status) enabling cross-actor discovery and verification through the Layer 3 hourglass interface (EPCIS) without replicating underlying records. Federation is not a deployment preference but an **architectural enforcement of data sovereignty**.

Sovereign: Every OATS deployment operates within the legal and regulatory jurisdiction of the implementing authority. Personal, commercial, and strategic agricultural data remain within jurisdictional boundaries, not exported in bulk. Cross-border interactions occur through federated query mechanisms over Layer 3 interfaces, transmitting only the minimum verifiable data required. Sovereignty extends to system control: jurisdictions retain the ability to replace, modify, or govern any OATS component without external dependency.

Auditable: All data interactions; queries, consent artefacts, credential exchanges, cross-border lookups, are recorded as tamper-evident, cryptographically signed records linked to the Layer 2 event chain. Logs are timestamped, non-repudiable, and retained per regulatory requirements. **Auditability is an always-on system property**, enabling both institutional oversight and data-principal-level visibility — individuals can inspect how their data has been accessed.

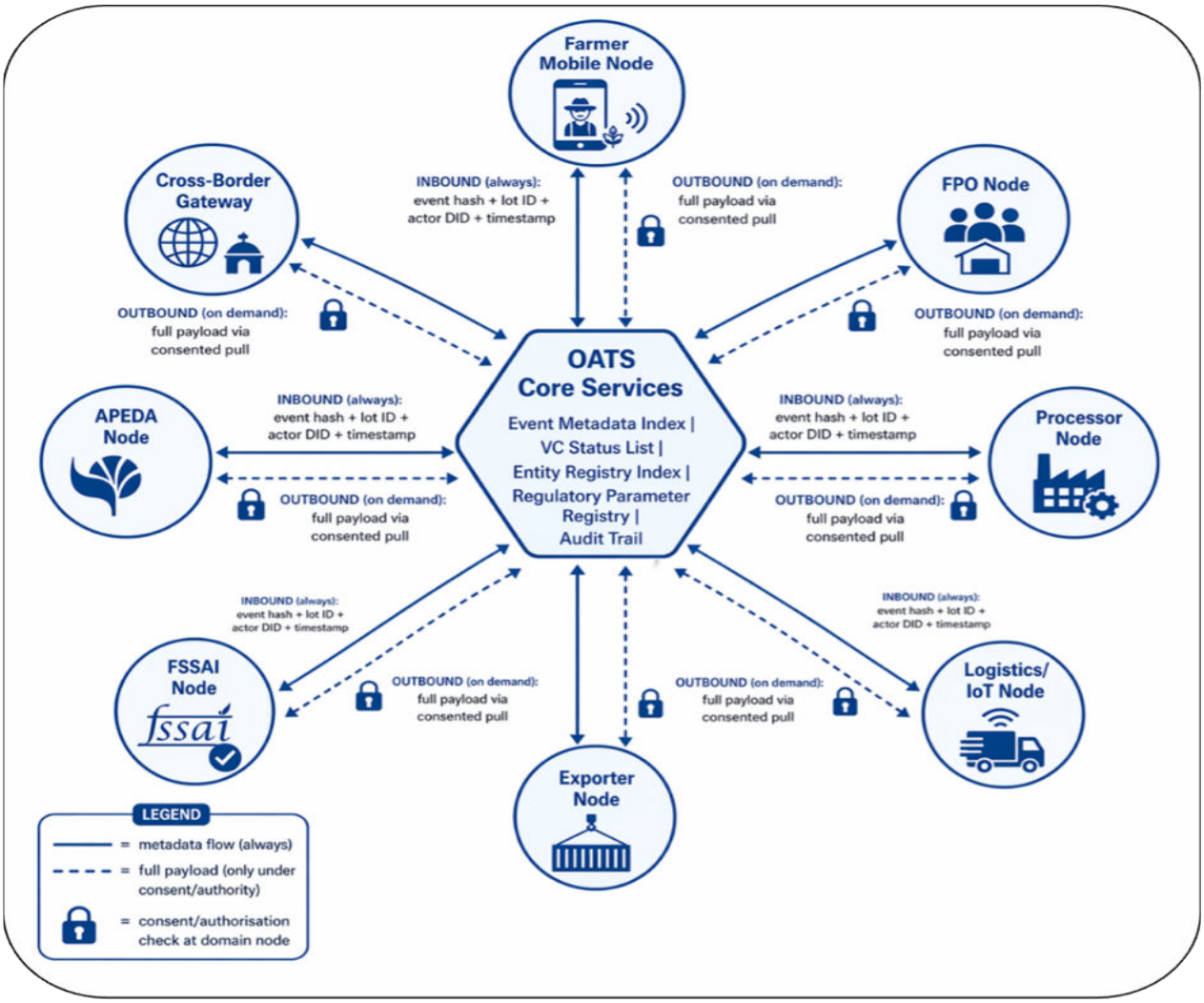


11.2 Data Mesh Architecture for Agri-Food Traceability

The data mesh is the mechanism by which federation is operationalised. Data is not centralised or aggregated into a single repository, it is treated as a **domain-owned data product**, where each

participant (farmer systems, FPO platforms, processors, logistics operators, exporters, regulators) maintains control over its own data and exposes it through standardised, policy-governed APIs.

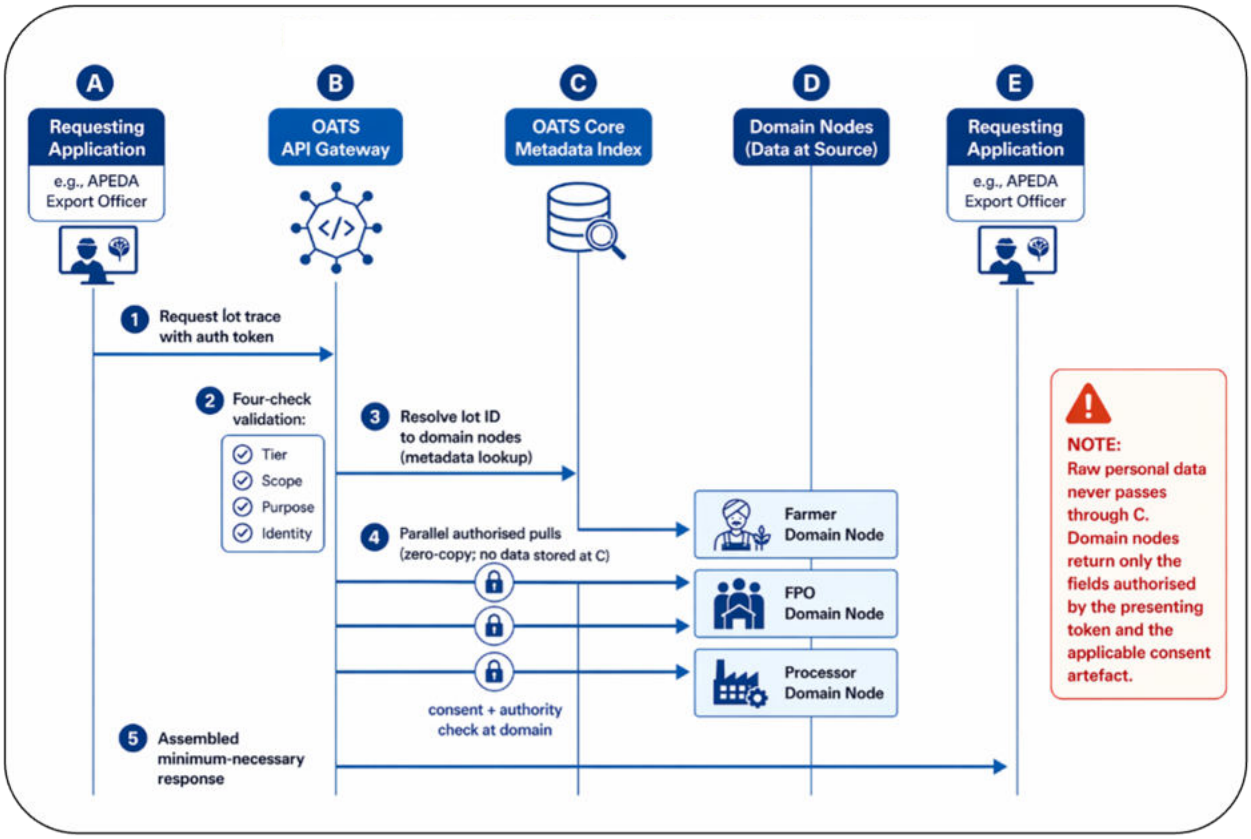
OATS Core operates as a lean metadata and orchestration layer, not a data warehouse maintaining only the minimum index required for discovery and verification (identifiers, hashes, timestamps, credential references) and enabling **zero-copy queries** across the network. Event payloads are stored exclusively at the originating domain node and are never persisted in OATS Core. Access control is evaluated locally by each domain using consent artefacts and policy rules. Each domain retains **portability rights** — it can migrate its data to any compliant infrastructure without dependency lock-in.



Zero-Copy Pull Model:

When an authorised actor initiates a query, OATS Core resolves the required identifiers through its metadata index and orchestrates authenticated requests to the relevant domain nodes; each node independently evaluates the request against consent artefacts, role-based access policies, and regulatory obligations before returning only the minimum required data. No bulk data is stored or replicated at Core. **Four concrete governance properties** a warehouse model could not provide: *fewer attack surfaces* (compromise of OATS Core does not expose farmer data because farmer data is not in OATS Core); *consent authenticity* (consent is evaluated at the point of data retrieval in real time, not against a stale central copy); *jurisdictional cleanliness* (data does not cross borders during query resolution unless explicitly permitted by the responding domain node); *replacement neutrality* (the Core layer can be replaced without migrating underlying data).

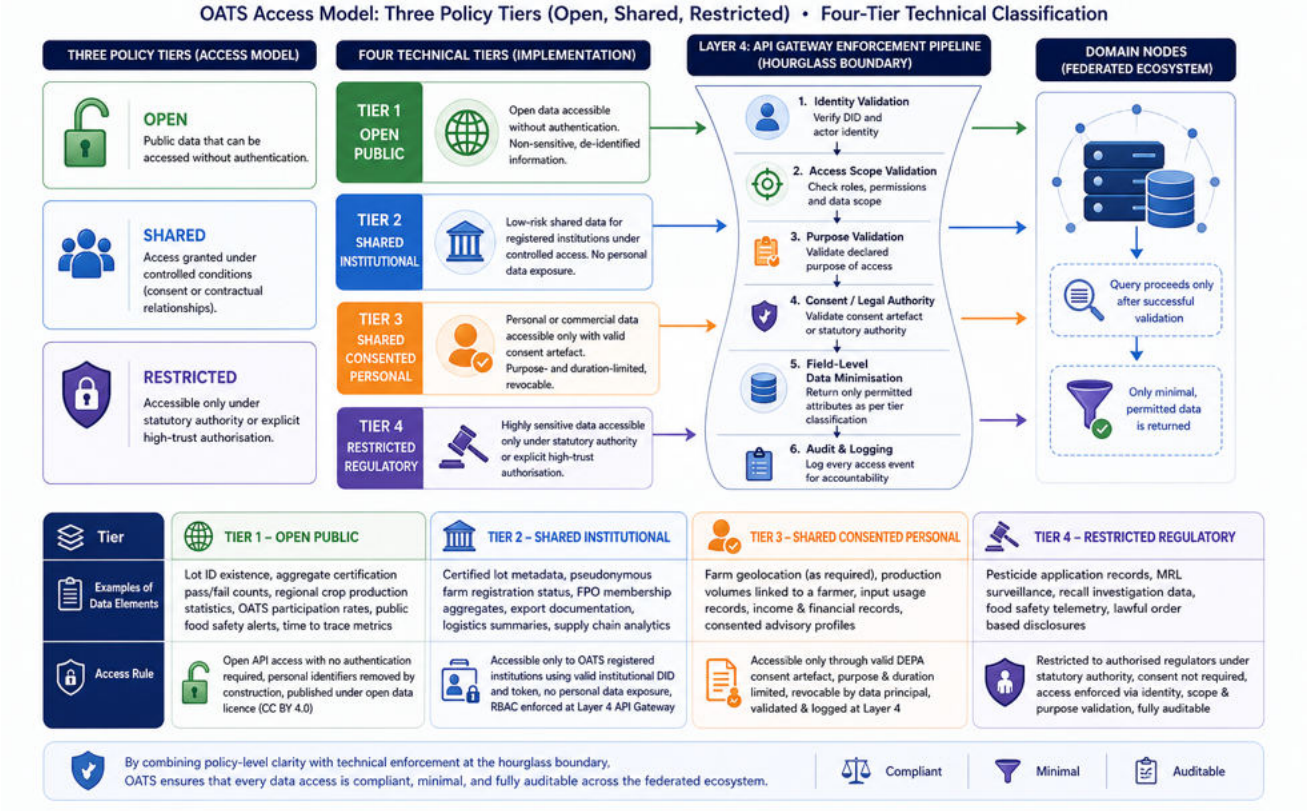
Zero-Copy Query Resolution Flow



11. 3-Tiered Data Access Model: Open, Shared and Restricted Tiers

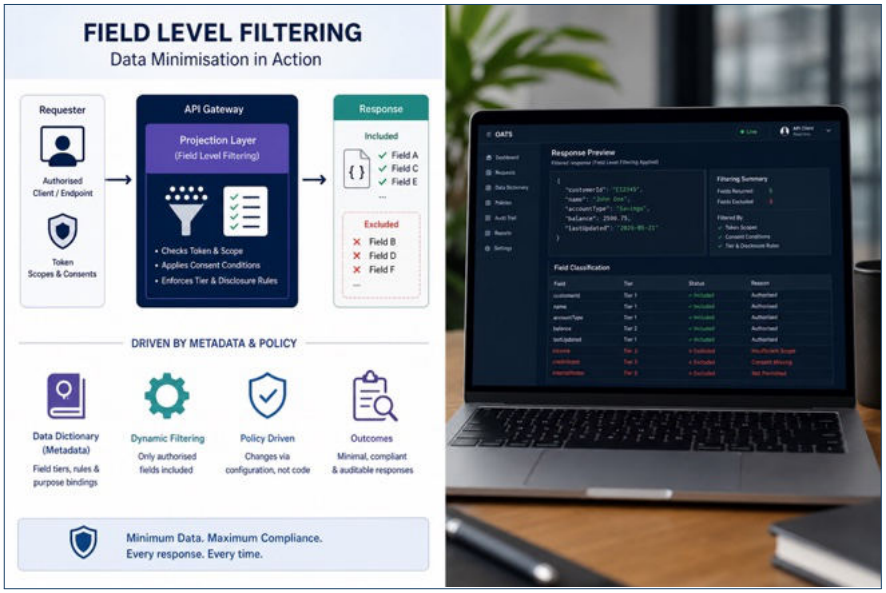
OATS presents the access model as **three policy tiers - Open, Shared, Restricted,** while implementing it as a **four-tier technical classification** aligned with API Gateway enforcement.

Three-Tier and Four-Tier Implementation



Technical Enforcement at the API Gateway:

Each participating entity is issued a cryptographically signed access token at registration, embedding claims defining the maximum permitted data tier, authorised API scopes, declared purpose of access, and token validity. The Gateway executes **four mandatory checks in sequence**: **Tier check** (requested endpoint's classification does not exceed token's permitted tier); **Scope check** (endpoint within token's authorised API set); **Purpose check** (declared purpose aligns with permitted use cases and, for consented data, matches an active consent artefact); **Identity check** (presenting DID matches token subject and cryptographic proofs are valid). Any failure → structured error response; denial recorded in audit trail. **Field-Level Filtering and Data Minimisation.** Endpoint-level tier enforcement is complemented by a projection layer at the API Gateway that dynamically filters fields based on the requester's token, permitted scope, and applicable consent conditions. Each data field in the **OATS Data Dictionary** carries an associated tier classification, disclosure rules, and purpose bindings — a single endpoint serves multiple access contexts without duplicating APIs.



11.4 DEPA Aligned Consent Architecture

The OATS consent architecture operationalises consent as a **first-class digital control**, where no statutory or contractual lawful basis exists, data access is contingent on explicit, informed, and revocable consent issued by the Data Principal. Consent is not a passive agreement but an **active, machine-readable artefact** governing how data can be accessed, by whom, and for what purpose. Consent enforcement is embedded into the same API Gateway and domain node validation flows that govern all other access decisions (

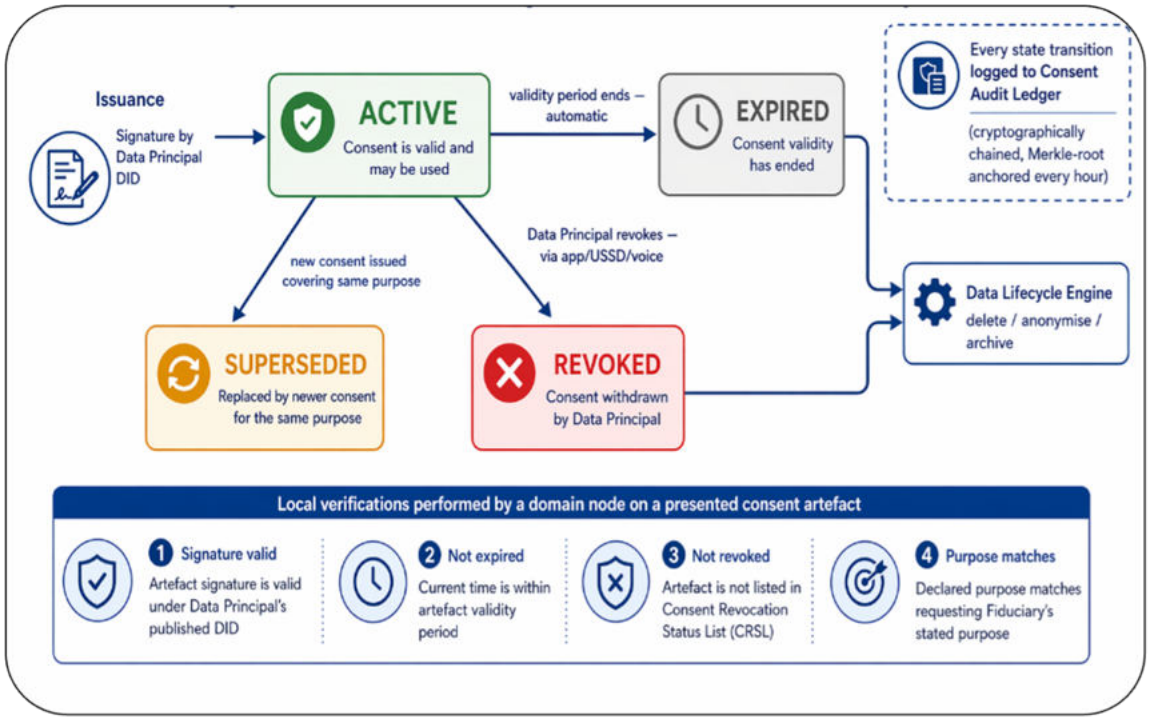
Consent as a Machine-Readable Artefact:

An OATS consent artefact is a **cryptographically signed credential** following the **DEPA Consent Artefact Specification v1.1 with OATS extensions** for agricultural data classification and commodity-level scoping. It specifies: Data Principal DID; requesting Data Fiduciary; exact data attributes or categories being requested; declared purpose mapped to the **OATS Purpose Code Registry**; validity period; renewal conditions; revocation mechanism. **Four validations** are executed locally at the domain node when a request is presented: signature verification against the Data Principal's DID; validity period check; revocation status against a continuously updated **W3C Status List 2021**; declared purpose matched against the requesting entity's stated use.

Pull and Push Consent Flows: Both flows generate identical consent artefacts and undergo the same validation checks. In the **Pull flow**, a Data Fiduciary initiates a request; the Data Principal reviews, modifies scope if required, and approves or rejects through any accessible interface (mobile, USSD, assisted centre, voice channel), appropriate for targeted bilateral interactions like lending, insurance underwriting, or buyer verification. In the **Push flow**, the Data Principal proactively issues consent for a predefined class of purposes or recipients — appropriate for broader market participation where repeated bilateral approvals would be infeasible (e.g., a farmer allowing any registered buyer within a commodity category to verify certification credentials).

Revocation and Consent Lifecycle: A Data Principal may revoke consent at any time through any supported interface; revocation propagates to the Consent Revocation Status List within a bounded window. All subsequent requests referencing the revoked artefact are rejected at the API Gateway before reaching domain nodes. The consent lifecycle is defined across **four states**: **active** (valid and enforceable), **expired** (validity period lapsed), **revoked** (explicit withdrawal by the Data Principal), **superseded** (replacement by a newer artefact covering the same purpose with modified parameters). Every transition is recorded in a cryptographically secured audit ledger. Data previously accessed under valid consent is governed by retention rules requiring deletion, anonymisation, or lawful retention.

DEPA-Aligned Consent Artefact Lifecycle



11.5 Cross-Jurisdiction Data Flow Governance

Agri-food supply chains are inherently cross-jurisdictional. A pomegranate grown in Solapur, traded in Nashik APMC, processed in Mumbai, and shipped to Rotterdam traverses at least two legal jurisdictions; three if the processing facility is in a different state with traceability data requested by actors in all three. Each jurisdiction has its own data protection regime, food safety statute, export documentation framework, and data localisation rules. OATS cannot wish this complexity away; it must make it legible and tractable.

The Jurisdictional Sovereignty Principle: All data remains anchored at Layer 1 and Layer 2 domain nodes within the originating jurisdiction and is never replicated or exported as bulk datasets across borders. Cross-border data movement is not a default capability but a controlled exception, permitted only when a legally recognised instrument exists between participating jurisdictions.

11.6 Data Quality Standards and Audit Trail Requirements

Data quality and auditability are enforced as **intrinsic properties of Layer 3 event processing and Layer 4 governance controls**, not downstream validation activities. Every data element entering the system originates at Layer 1 or Layer 2 domain nodes, passes through Layer 3 ingestion pipelines, and is validated before it becomes part of the traceability record. The six dimensions are as described in the table below:

Dimension	Definition	OATS Example
Accuracy	Data correctly represents the real world entity or event	GPS coordinates match actual farm polygon, lot quantity matches measured weight, harvest date reflects event
Completeness	All required key data elements are present and non empty	FSMA harvest event contains all mandatory KDE fields with no null values
Timeliness	Data is captured and published within required time window	Harvest events submitted within 24 hours, cold chain breach reported within minutes
Consistency	Data is internally coherent and aligns with related records	Transformation input quantities reconcile with output quantities within defined tolerance
Validity	Data conforms to syntactic and semantic standards	Lot IDs follow GS1 structure, dates follow ISO format, commodity codes exist in registry
Provenance	Data origin is cryptographically attributable to an actor	Event signed by actor DID, signature verifiable, actor credential valid at time of submission

Data Quality Enforcement in the Event Pipeline: Every submitted event is validated against EPCIS schema definitions, business vocabulary rules, commodity-specific extensions, and the credential status of the submitting actor; requests failing validation are rejected with structured error responses. Cross-event consistency checks, mass-balance reconciliation, and external-registry validations are executed asynchronously by the **Data Quality Engine**; failures generate a **Data Quality Alert** propagated through the system triggering remediation workflows for the originating actor and visibility for relevant regulators.

Audit Trail Architecture: Every operation — data access, consent validation, credential usage, cross-border interactions — is recorded in an **append-only log where each entry is cryptographically linked to the previous one**. Periodic cryptographic summaries of the audit log are **anchored to the permissioned distributed ledger** (Ch 9) — Merkle roots anchored hourly; 7-year retention (SRS-12.3). Audit access is stratified: Data Principals access their own personal-data history through accessible channels (mobile/voice/USSD/assisted centres) showing who accessed, when, for what purpose, under which consent artefact (every audit query itself is logged); Data Fiduciaries through their DPOs review audit records for their processing activities; regulators access under statutory authority with all access validated and logged; the Farmer Data Rights Ombudsman retains full access for grievance investigation.

11.7 Data Retention, Archival and Right to Erasure

Storage limitation is among **DPDPA principles**. OATS implements storage limitation **architecturally rather than procedurally**. The retention clock runs automatically against every personal data record, and expiration triggers an automated lifecycle action (deletion, anonymisation, or archival) according to the policy bound to the record at creation. Retention is a continuous background process, not a quarterly hygiene exercise.

12. OATS Consent management System

Within the Chapter 4 hourglass architecture, consent is a **Layer 4 core control mechanism** governing every movement of personal data originating from Layer 1 identity and Layer 2 registries and flowing through Layer 3 event exchange. It is **not an application-level feature but a system-level requirement** — a sovereign control exercised by the Data Principal, ensuring that data describing land, production, and supply-chain participation cannot be accessed, processed, or shared without explicit, verifiable authorisation. In agricultural ecosystems where the power imbalance between smallholder farmers and institutional actors necessitates enforceable mechanisms rather than declarative assurances, OATS treats consent as a foundational Digital Public Infrastructure component equal in importance to identity, traceability events, and interoperability protocols. The architectural mechanics — DEPA-aligned artefacts, Consent Manager (BB-ID-03), W3C Status List 2021 revocation, four-check API Gateway validation — are canonically specified in **Chapter 5 and Chapter 12. T**his chapter specifies the legal grounding, the **ORGANS framework**, the consent artefact schema, the Consent Manager registration regime, voice-first/vernacular operations for semi-literate populations, and audit/grievance procedures.

12.1 DPDPA 2023 Consent requirements and OATS Alignment

The **Digital Personal Data Protection Act 2023** (Act No. 22 of 2023), read together with the **DPDP Rules 2025** (published November 2025), is the controlling statute for any OATS deployment processing the personal data of any Data Principal located in India. Most provisions map directly to OATS architectural controls already specified in Ch 5 and Ch 12.

12.2 The ORGANS Framework:

Open, Revocable, Granular, Auditable, Notic based, Selective - The ORGANS Framework is the normative design lens introduced by this Blueprint for consent architecture in agricultural DPI. It distils the combined requirements of DPDPA 2023, GDPR, UNDP DPI Safeguards v2.0, and field-tested lessons from the DEPA Account Aggregator ecosystem into six design properties that every OATS-conformant Consent Manager must satisfy**. Each property is independently testable;** a Consent Manager that satisfies five out of six is non-conformant. **The acronym is deliberate: consent architecture should be to a DPI what organs are to a living body, not optional modules but load-bearing systems whose failure is systemic failure.**

O - Open	The Consent Manager's interface specifications, artifact schemas, and audit-log formats are published as royalty-free open standards. Any OATS-conformant implementation must be independently buildable from these published specifications. Proprietary extensions at the consent-artifact or interface boundary are prohibited. This operationalises OATS Principle P-1 (Open by Default)
R - Revocable	Every consent is revocable at any time through any channel the farmer can use. Revocation takes effect within 24 hours and propagates to all downstream data consumers within 7 working days.
G - Granular	Consent is never bundled across unrelated purposes. Each combination of (data category, purpose, recipient, duration) generates a distinct consent artifact. A farmer may consent to share plot geometry with the export certifier while refusing to share the same data with the credit bureau, and the Consent Manager will honour both decisions independently. Granularity is enforced at the schema level: the Consent Request object cannot enumerate more than one purpose per artifact. This operationalises DPDPA DP-2 (Purpose Limitation) and GDPR Art. 6(1)(a) specificity requirements.

A - Auditable	Every consent lifecycle event - request, grant, denial, view, update, revocation, expiry, archive is written to an append-only, tamper-evident audit log. The log is accessible to the Data Principal through the Farmer Data Dashboard and to the Data Protection Authority on lawful request. Audit entries are timestamped and signed using the issuing actor's DID key.
N - Notice-based	No consent is valid without a correspondent notice satisfying DPDPA Section 5 and GDPR Article 13. The notice is delivered in the Data Principal's chosen language, in plain language at a grade-5 reading level, with a voice rendering available on demand. The cryptographic digest of the notice shown at the time of consent is embedded in the artifact, so the exact text the farmer saw is provable and non-repudiable. Machine-translated notice text is prohibited for legally operative content; only human-translated, glossary-locked text is used for the notice.
S - Selective	Consent supports selective disclosure: a single consent may authorise sharing of some attributes of a credential while suppressing others.

12.3 Consent Manager Architecture and Registration

A Consent Manager (CM) is a **dedicated, user-empowering intermediary** whose sole function is to collect, store, notify, revoke, and audit consent artefacts on behalf of Data Principals. Following the DEPA design pattern from India's Account Aggregator ecosystem, **a CM is not a data consumer and not a data producer** — it stores no personal data beyond consent artefacts themselves and has no commercial interest in the data flows it mediates. This **structural neutrality** is what allows a CM to be trusted by farmers in a way an agribusiness platform or certifier cannot be, regardless of intentions.

Three Deployment Models for Consent Managers.

Model	Description
Government-Operated CM	Operated by the state Agriculture Department or its designated implementing agency (e.g., AIAIC in Maharashtra). Provides a universal, zero-cost CM for all farmers in the jurisdiction. Appropriate for early-stage deployments where private-sector CM supply is thin. **Must be operated as a ring-fenced unit with its own DPO and audit chain separate from other department functions**, to preserve structural neutrality.
Licensed Private CMs	Registered under a Sahamati-equivalent self-regulatory framework, licensed by the relevant Digital Governance Authority, supervised by the Data Protection Board. Farmers choose among licensed CMs, creating competitive pressure on service quality. Revenue model: **fixed per-artefact fee paid by the Data Fiduciary (never by the Data Principal)**, as in the RBI Account Aggregator framework.
FPO-Federation CM	Operated by a consortium of FPOs for their collective membership. Useful where farmers trust their FPO more than an abstract government or private intermediary. Must satisfy the same conformance requirements as other CMs and **must not condition FPO membership on consent choices** (DPDPA Section 6(4); GDPR Art. 7(4)).

Regardless of deployment model, every OATS-conformant Consent Manager must be **registered in the OATS Consent Manager Registry** — a public registry maintained by the OATS Multi-Stakeholder Governance Council. Registration requires: legal-entity incorporation and a published DPO; published conformance test results from the OATS Reference Laboratory; published SLA committing to the SLAs in FRS-13 / SRS-13; operational grievance channel meeting §13.8 requirements; annual independent audit against the conformance suite. Failure in any triggers suspension from the Registry.

13. Regulatory Compliance Framework and Legal Architecture

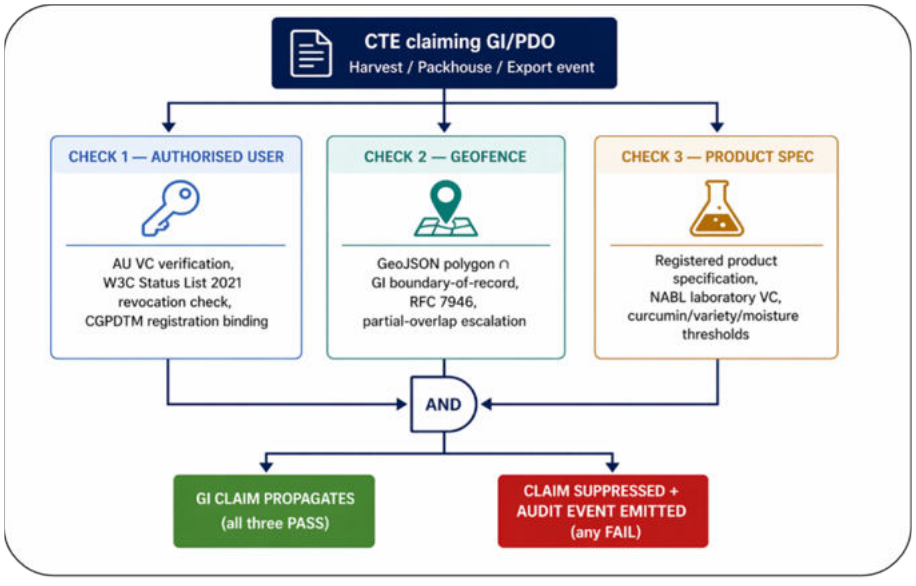
The OATS compliance architecture operationalises compliance-by-architecture within the Chapter 4 hourglass model. Regulatory logic is embedded directly into the data flow rather than layered as documentation on top. Events captured at Layer 2 become the canonical source from which all compliance artefacts (traceability reports, export certificates, due-diligence statements, geographical-indication attestations) are derived; the Layer 4 governance plane enforces validation rules, consent, and auditability. This eliminates retrospective documentation burdens and ensures compliance outputs are generated automatically from real-time operational data. OATS models the global regulatory landscape along three structural axes mapping to its modular compliance engines: horizontal regulations (baseline traceability obligations across all commodities — implemented through the core event schema), vertical regulations (commodity-specific or claim-specific requirements — extensions to the canonical data model), and extraterritorial regulations (handled through verifiable credentials and cross-border compliance artefacts, ensuring obligations imposed by importing jurisdictions are met without transferring underlying sensitive data). Prescriptive regimes are encoded as deterministic validation checks at Layer 3; outcome-based regimes are satisfied through queryable event chains producing regulator-specific outputs on demand.

13.1 GI Tag and Protected Designation of Origin

Geographical Indications are the highest-value claim OATS supports. A GI-tagged basmati rice, an Alphonso mango, a PDO-protected Kalamata olive or Darjeeling tea commands a price premium **two to ten times** the equivalent non-GI product. The premium derives entirely from consumer trust in the authenticity of the geographical origin claim — OATS's role is to make the legal claim operationally verifiable at the point of every supply-chain event so the premium is commercially defensible against fraud attempts.

The OATS GI Verification Module: Three-Check Enforcement:

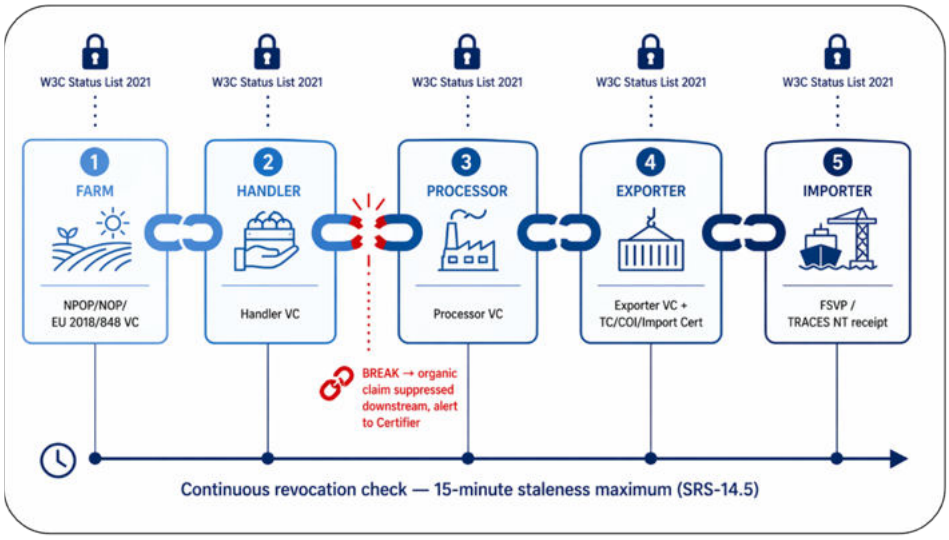
Executes at the Harvest CTE and at every subsequent value-added CTE claiming the GI. **All three checks must pass** for the GI claim to propagate; a failure on any check causes the claim to be suppressed on downstream events, with the suppression itself recorded as an auditable EPCIS event. **Check 1 — Authorised User credential binding** — at each CTE claiming the GI, the actor presents its Authorised User VC issued by the Registered Proprietor, bound to the specific GI registration number at CGPDTM; the L-4 VC infrastructure verifies signature and revocation status against the W3C Status List 2021 endpoint maintained by the Proprietor. **Check 2 — Geofence validation** — the GeoJSON polygon of the harvest or production event is evaluated against the GI's registered geographical boundary-of-record maintained in the OATS Standards Registry (Ch 4 §4.4); a harvest polygon wholly outside the GI boundary fails; a polygon partially inside triggers reviewer escalation. **Check 3 — Product-specification compliance** — the GI's registered product specification (curcumin content minimum for Sangli turmeric; variety restriction for Alphonso mango; milling specification for basmati rice) is evaluated against the event KDE set with a NABL-laboratory VC or equivalent as evidence.



CGPDTM GI Registry API Integration Roadmap: Operationalising the three-check module requires the CGPDTM GI Registry to expose a machine-readable API. Three-stage roadmap: **Stage 1** — read-only JSON API exposing published registration details (canonical geographical boundary-of-record as GeoJSON, current Authorised User list with issue/revocation timestamps, registered product specification achievable within 12 months of a supporting policy decision); **Stage 2** — subscription-based notification stream for AU additions and revocations (Year 2); **Stage 3** — bidirectional integration enabling Authorised Users to transact quotas and transfers natively through OATS (Year 3+).

13.2 Organic Certification Legal Framework: NPOP, NOP, EU Organic

Three organic regimes dominate global trade: **India's NPOP** (statutory foundation: Foreign Trade e (Development and Regulation) Act 1992; administrative authority APEDA; current operational manual 8th Edition; certification by APEDA-accredited Certification Bodies; e-TraceNet for Transaction Certificates); **United States' NOP** (7 CFR Part 205; administered by USDA Agricultural Marketing Service; **Strengthening Organic Enforcement (SOE) Final Rule effective 19 March 2024** materially tightened operator-chain verification; previously exempt handlers/traders/brokers/exporters now in scope, NOP Import Certificate required for organic imports); **European Union's Regulation (EU) 2018/848** (effective 1 January 2022, replacing EC 834/2007; introduced **group-certification mechanism for smallholder producers** via FPO Internal Control System certified by an EU-approved control body — of considerable relevance to Indian FPO-based organic supply chains where individual farm certification is economically infeasible). OATS implements a **single Organic Module** parametrised by destination-market regime and equivalence chain — the operator maintains a correctly-issued certification VC chain, the module generates destination-specific export documentation from that chain.

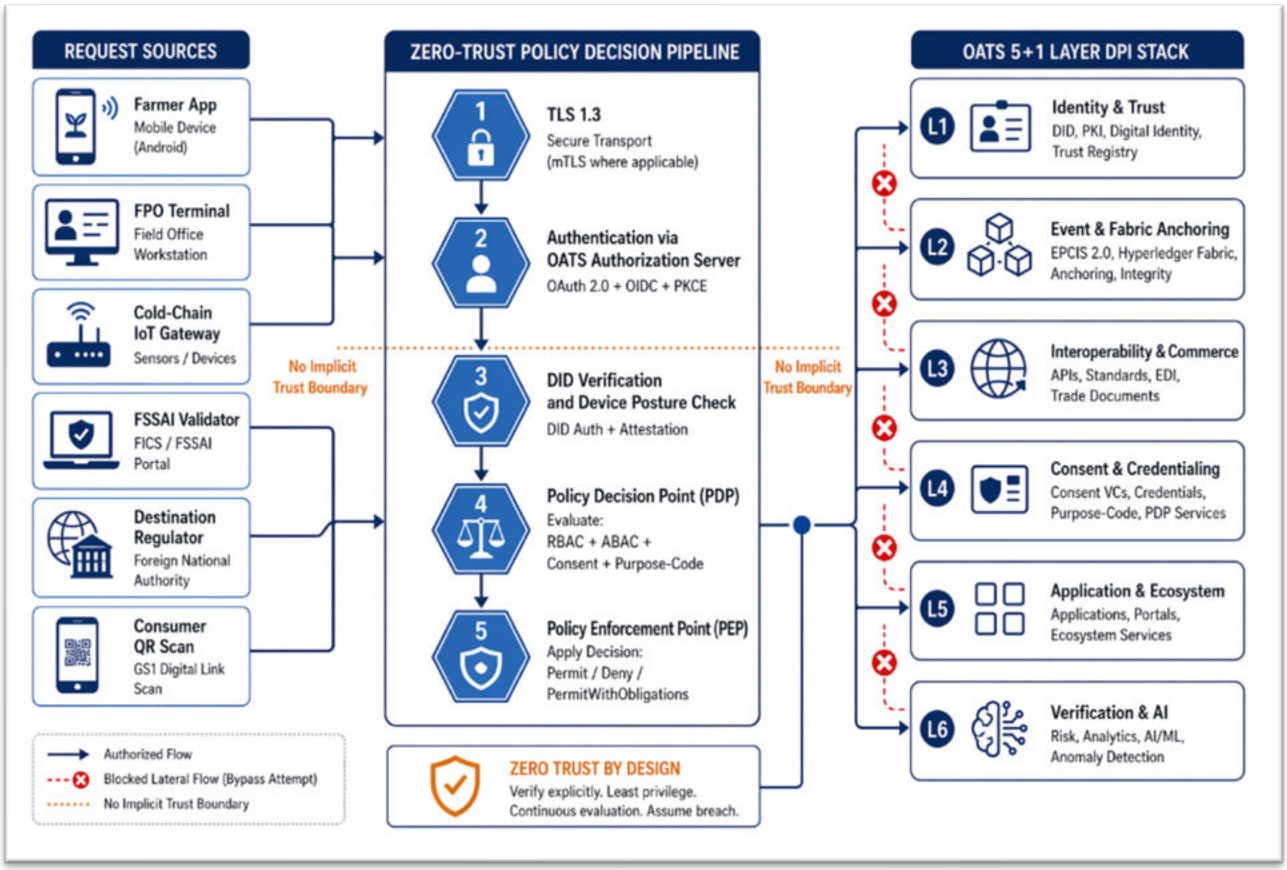


14. Cybersecurity, Privacy and Data Protection Architecture

The OATS security architecture adopts a **zero-trust model in alignment with NIST SP 800-207** and is instantiated within the Chapter 4 hourglass architecture as a cross-cutting control anchored in identity and governance layers but enforced across every interaction. **No actor, device, network, or system component is implicitly trusted regardless of its location** in the ecosystem. Every request to access data, invoke an API, retrieve a credential, or submit an event is authenticated, authorised, and validated in real time against identity proofs, policy constraints, and contextual attributes. Zero-trust is essential in OATS because the operational boundary spans heterogeneous environments (farmer devices, field infrastructure, government systems, cross-border regulatory platforms, cloud services) where traditional perimeter-based security assumptions are invalid.

14.1 OATS Security Architecture: Zero-Trust by Design

Zero-trust in OATS is implemented through continuous verification of actor identity using DID-based credentials, strict enforcement of least-privilege access combining RBAC and ABAC, and cryptographic validation of every data exchange and event submission. Each interaction is an independent trust decision evaluated at the API Gateway and consent-governance layers; trust is derived from verifiable controls rather than network location, making the system resilient to insider threats, lateral movement attacks, and cross-domain vulnerabilities.



The Five Zero-Trust Tenets Applied to OATS (NIST SP 800-207 — five apply directly and non-negotiable to every OATS deployment; the remaining two are operational amplifications of the first five).

Tenet	Principle	OATS Implementation
ZT-1	All data sources and computing services are resources	Every OATS component including Event Ingestion Service DID Resolver VC Verification Service PEVC Compliance Engine IoT Telemetry Ingest Consumer QR Resolver Regulatory Dashboard and each Hyperledger Fabric peer node is treated as an independent protected resource with its own authentication authorization and audit boundary ensuring no implicit trust between components
ZT-2	All communication is secured regardless of network location	TLS 1.3 is enforced across all API endpoints and service mesh-based mutual TLS is applied for all intra-service communication ensuring that no plaintext traffic exists even within internal clusters or Fabric organisations
ZT-3	Access to individual resources is granted on a per-session basis	OAuth 2.0 issued JWT tokens have a maximum one-hour lifetime with each session evaluated independently using DID identity purpose code requested data tier and consent posture ensuring no carryover of trust between sessions
ZT-4	Access is determined by dynamic policy including observable state	Authorization decisions are executed through a Policy Decision Point using policy engines such as Open Policy Agent or XACML evaluating requester attributes resource sensitivity and environmental context including time geolocation device posture and threat intelligence inputs
ZT-5	The enterprise monitors and measures the integrity and security posture of all owned and associated assets	Continuous telemetry from hosts containers Fabric nodes and IoT devices is streamed to the Security Operations Centre with automated quarantine enforcement for any asset deviating from defined security posture baselines ensuring real-time enforcement of trust conditions

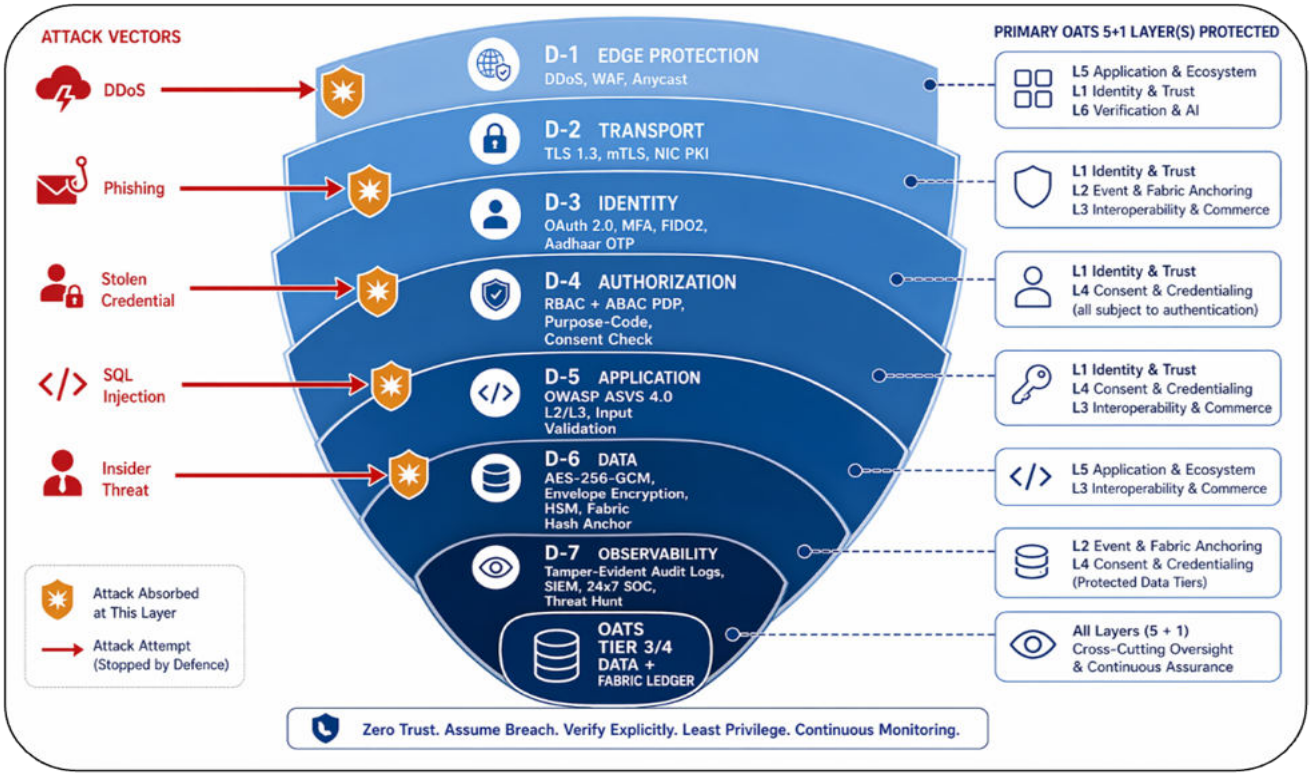
Zero-Trust Continuity Principle: Zero-trust is a *continuous property*, not a deployment state. Every OATS API request is re-evaluated in full — identity, authorisation, purpose, consent, context — regardless of how recently the same requester performed a similar action. **A successful query one second ago confers no right to the next query.** This distinguishes zero-trust from session-based security and is why it withstands credential theft, insider abuse, and compromised-device scenarios that defeat perimeter models.

The OATS Seven-Layer Defence-in-Depth Stack:
Zero-trust does not replace defence-in-depth — it intensifies it.
D-1 Edge Protection — DDoS mitigation, WAF with OWASP Top 10 rule-set, global anycast load balancing at the API Gateway boundary.
D-2 Transport — TLS 1.3 minimum on all external endpoints.
D-3 Identity — OAuth 2.0 + OpenID Connect + PKCE through the OATS Authorisation Server; MFA mandatory for all administrative, government-validator, and high-tier commercial roles; farmer-facing authentication uses Aadhaar OTP (where legally permitted), AgriStack Farmer ID, or offline biometric verification for low-literacy users.
D-4 Authorisation — zero-trust policy evaluation on every API request via the Policy Decision Point, combining RBAC and ABAC with purpose-code binding and consent verification at the point of enforcement.

D-5 Application — OWASP ASVS 4.0 Level 2 minimum for public endpoints (Level 3 for regulatory endpoints), input validation, output encoding, parameterised queries, threat modelling for every new service.
D-6 Data — AES-256-GCM encryption at rest on all persistent stores; SHA-256 hash anchoring on Hyperledger Fabric for integrity-critical records (envelope encryption with keys managed in FIPS 140-3 Level 3 HSMs.
D-7 Observability — tamper-evident audit logging, SIEM correlation, continuous vulnerability scanning, 24×7 SOC monitoring with active threat hunting.

Anti-Pattern: Perimeter Security with Flat Internal Trust. Several national agricultural platforms have been deployed with a firewall-demarcated perimeter inside which all services trust each other. **Flat internal trust means any single compromised internal service grants lateral movement to every other service and every connected database.** The equivalent in the Chapter 4 architecture would be a Fabric deployment where peer nodes exchange traffic without mTLS because they share a private VPC — a pattern that defeats the tamper-evidence guarantees of the Fabric channel architecture itself. OATS conformance explicitly prohibits flat internal trust patterns; deployments exhibiting them are not eligible for the OATS Conformance Mark at Standard or Advanced levels.

OATS Seven Layer Defence-in-Depth Stack

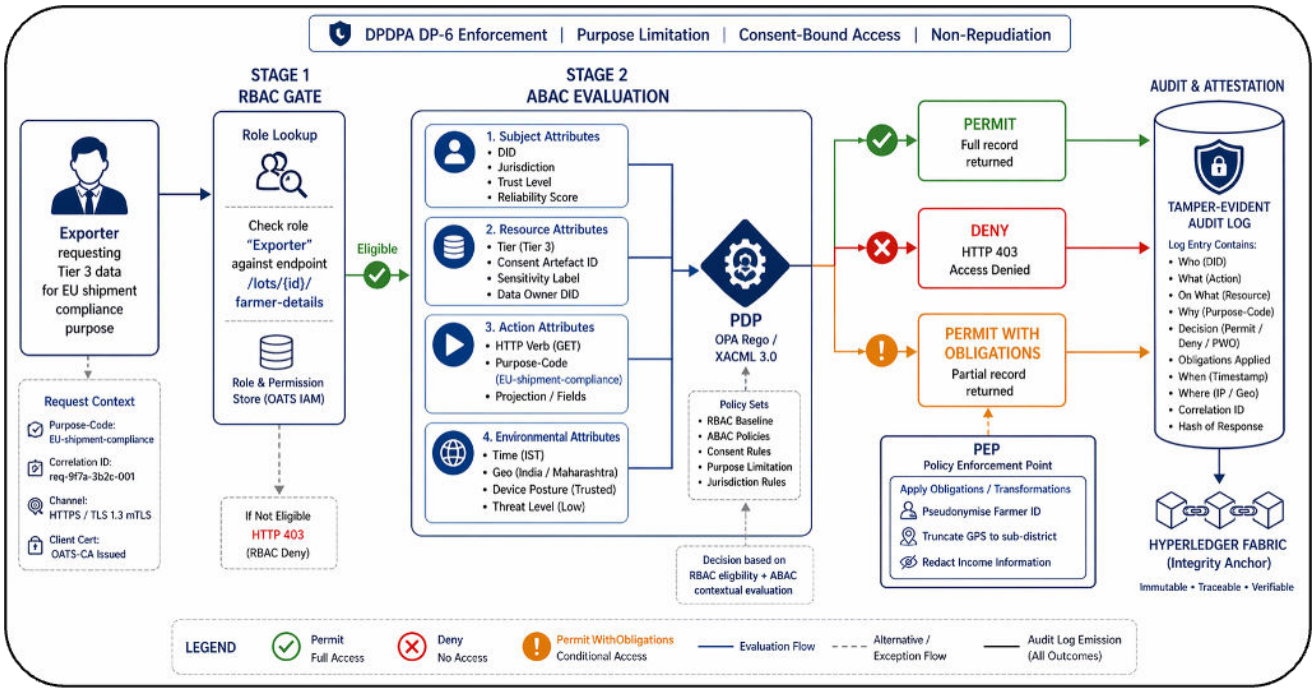


14.2 Identity and Access Management: Role-Based and Attribute Based

Identity and Access Management (IAM) in OATS is the enforcement layer through which consent, data governance, and regulatory compliance are made operational rather than declarative. It binds the legal constructs to the technical execution layer, ensuring that every access to data, every invocation of an API, and every interaction across the OATS ecosystem is authenticated, authorised, and auditable. Without a robust IAM layer, the guarantees of purpose limitation, consent enforcement, and non-repudiation collapse, rendering the system non-compliant with DPDPA 2023 and incapable of withstanding regulatory or judicial scrutiny. IAM is therefore a foundational trust control anchored in Layer 1 (Identity, Trust & Registry) and enforced across all higher layers of the OATS 5+1 architecture.

The OATS IAM model is explicitly hybrid, combining Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) in a sequential evaluation model. RBAC provides the structural baseline by assigning stable, coarse-grained permissions based on organisational roles such as farmer, FPO operator, exporter, certifier, or regulator. This enables predictable and manageable access boundaries aligned with institutional responsibilities. ABAC then refines these permissions through dynamic, context-aware evaluation using attributes such as purpose code, consent status, data tier classification, jurisdiction, time, device posture, and risk signals. The enforcement sequence is deterministic: RBAC first determines whether an entity is eligible to access a class of resources, and ABAC then evaluates whether the specific request instance is permissible under current conditions. Access is granted only if both layers approve, ensuring that role eligibility is always constrained by real-time governance conditions.

RBAC + ABAC Policy Decision Flow at the OATS Policy Decision Point



14.3 Key management and PKI Architecture

OATS operates three coordinated but distinct cryptographic infrastructures:
a classical PKI for X.509 certificates used in TLS, mTLS, and document signing;
a Decentralised Identifier (DID) infrastructure for W3C DID-based identity and Verifiable Credential signing;
a Hyperledger Fabric CA infrastructure for Fabric peer and orderer identity within OATS Layer 2 blockchain channels. All three are anchored in the same sovereign trust roots.

14.4 Audit Logging and Non-Repudiation

Non-repudiation is the property that an entity cannot plausibly deny having performed an action it did perform. For a food traceability DPI, non-repudiation is not a security nicety — it is the legal foundation on which every regulatory mechanism rests. When FSSAI issues a recall notice based on an OATS chain-of-custody query, the recalled lots' participants cannot credibly claim they did not handle those lots. When APEDA issues an export rejection based on a PEVC gap report, the exporter cannot credibly claim that gap did not exist. Non-repudiation converts traceability data from commercial information into legally admissible evidence.

Non-repudiation in OATS is constructed through three coordinated mechanisms: cryptographic signing of every domain-significant event by the acting entity's DID; tamper-evident audit logging of every authentication, authorisation, and data-access operation; and cryptographic anchoring of critical audit logs on the Hyperledger Fabric governance channel.

14.5 Data Protection Impact Assessment (DPIA) Framework

A DPIA is a structured evaluation of the privacy risks of a data-processing activity and the measures taken to mitigate those risks. For OATS, DPIAs are not discretionary best practice — they are legal obligations under both DPDPA 2023 and GDPR.

DPDPA 2023 obligations require any Data Fiduciary designated as a Significant Data Fiduciary (SDF) to: appoint a Data Protection Officer resident in India; appoint an independent data auditor for periodic data audits; conduct periodic DPIAs. DPDP Rules 2025 specify that state governments deploying OATS at scale, processors handling farmer personal data for more than one lakh farmers, and platform operators maintaining national-scale farmer registries are likely to be SDF-designated. OATS implementors in India must plan for SDF designation from the outset. The DPIA must be completed and approved before the commencement of any OATS processing activity involving personal data at scale, and repeated: every 24 months under normal operations; upon any material change in processing activity, data categories, recipients, or retention periods; upon any change in the applicable regulatory framework; following any confirmed breach affecting Tier 3 personal data.

PART IV

MARKET OUTCOMES & VALUE CREATION

CHAPTER 15-16

- *The market-facing layer of OATS - operationalising the consumer "right to know" as an architectural property of the DPI*
- *A four-pillar disclosure model via GS1 Digital Link QR codes with a sub-three-second consumer journey*
- *Publishes to SmartLabel, Open Food Facts, and ONDC Agriculture from a single event source*
- *Closes the accountability loop through consumer grievance and feedback workflows feeding Layer 6 anomaly detection*
- *Converts traceability events into financial infrastructure — Agri-Credit Score, supply-chain finance, warehouse-receipt finance via eNAM / WDRA, smart-contract payment triggers*
- *Crop insurance and DBT integration tied to verified events; gender-responsive finance design*



15. Consumer Transparency and Market Access

The right to know is the **normative foundation of this chapter**, the assertion rooted the Codex Alimentarius traceability principles, and India's Consumer Protection Act 2019 that every consumer of an agricultural or food product is entitled to a **machine-verifiable, understandable, and timely disclosure** of the product's origin, certification status, handling history, and food-safety assurances. **OATS does not introduce the right to know; it operationalises it at population scale through a shared open protocol that any brand, retailer, or regulator can query without intermediation.** The chapter is framed around three normative commitments inherited from the OATS Unified Principles Framework of Chapter 2: **inclusivity, verifiability** and **minimal data collection .** Consumers must be able to verify a product without creating an account, logging in, or surrendering any personal data.. This chapter specifies the operational consumer transparency layer: the Four-Pillar Disclosure Model, GS1 Digital Link consumer journey design, Smart Label and Open Food Facts integration, Bhashini-powered multilingual access, premium-market access mechanics, ONDC D2C commerce integration, EU Digital Product Passport conformance, and the grievance-feedback loop into AI/ML risk intelligence.

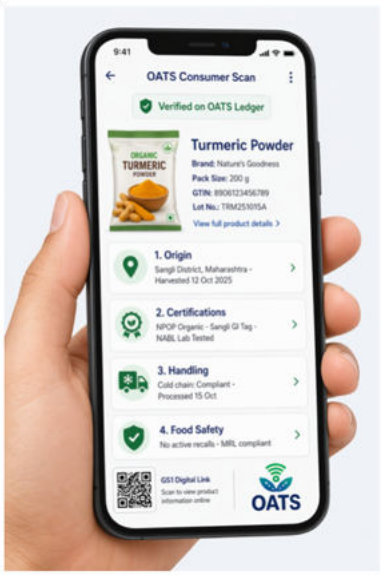
Design Principle. The brand owns the product; **OATS owns the verification**. A consumer scanning a turmeric pack does not trust the brand — they trust the Fabric ledger, the NPOP certifier's VC, and the FSSAI Recall API. This separation of trust from brand is the architectural reason the OATS consumer interface is specified as a Layer 5 DPI module, not as a brand-configurable feature.

15.1 Consumer Transparency: The Right to Know

Table below provides **The Four-Pillar Consumer Transparency Disclosure Model.** Jurisdiction-neutral at the protocol layer with jurisdiction-specific disclosure requirements applied as configuration at the Standards Registry level.

Pillar	What Consumer Sees	Underlying OATS Event/VC
P1 · Origin & Provenance	District/estate-level farm location; harvest date range; variety; FPO name (if applicable); GI zone attestation where relevant.	CTE-04 Farm Harvest ObjectEvent; AgriStack Farmer ID (pseudonymised); GI Zone VC.
P2 · Certifications & Quality	Organic, GI, Fairtrade, GlobalGAP, BCI, NABL lab-tested indicators; expiry date of each certificate; issuing authority.	W3C VCs issued by NPOP certifier, GI Registry, Fairtrade, NABL labs; Status List 2021 revocation check.
P3 · Handling & Journey	Processing facility; cold chain compliance verdict (compliant/conditional/non-compliant); shipping date; retail arrival date.	CTE-07 Packhouse TransformationEvent; IoT cold-chain AssociationEvent; CTE-09 Shipping ObjectEvent.
P4 · Food Safety & Alerts	Active recall flag (if any); allergen declarations; residue test summary (pass/fail); country of destination eligibility.	FSSAI Recall Alert Event; NABL MRL VC; OATS AI/ML Anomaly Flag Event.

Why Consumer Transparency is a DPI Responsibility:



In conventional food systems, consumer-facing transparency is delivered by brands through proprietary apps, bespoke QR experiences, and marketing websites — producing three structural failures: (i) each brand reinvents its own verification stack driving compliance cost up and interoperability down; (ii) **consumers cannot trust a brand-controlled disclosure because the disclosing party is also the party with an economic interest in what is disclosed**; (iii) smaller producers — precisely those most in need of verified provenance to access premium markets — cannot afford the custom-app route. OATS resolves all three failures by moving the consumer-verification interface **out of the brand layer and into the DPI layer**: the GS1 Digital Link Resolver is a public infrastructure endpoint operated under OATS governance (not by any individual brand); SmartLabel and Open Food Facts integrations publish the same Fabric-verified data irrespective of brand size; the Bhashini-powered interface is available to every OATS-registered lot at zero marginal cost.

15.2 GS1 Digital Link QR Code Consumer Journey Design

Grounded in the GS1 Digital Link Standard (ISO/IEC 18975) and aligned with **GS1's global Sunrise 2027 migration to 2D data carriers at retail point-of-sale**. The journey is designed to complete in **under three seconds globally and under one second within India**, with zero registration, zero personal-data collection, and full offline fallback for low-connectivity scenarios.

The GS1 Digital Link URI — Anatomy of a Scannable Traceable Lot. Every OATS-traced consumer unit carries a QR code encoding. The process may be defined through a **the following six steps:**

- **S1** — Consumer opens native phone camera (no app install); camera OS recognises GS1 QR as a URL; browser invoked.
- **S2** — Browser loads OATS Resolver page; language auto-detected from device locale; Resolver looks up LGTIN in OATS Lot Registry and returns redirect to rendered provenance page
- **S3** — Consumer sees Four-Pillar summary (Origin, Certifications, Handling, Food Safety) in local language; Resolver calls queryLotHistory() on Fabric, assembles event chain, verifies each VC against Status List 2021.
- **S4** — Consumer taps "See Full Journey" for event-by-event timeline view with farm photo (where consented); Resolver streams full EPCIS event chain as JSON-LD; renders timeline
- **S5** — Consumer optionally taps "Report Issue"; feedback captured anonymously and routed to FSSAI and producer via OATS Grievance Module
- **S6** — **Offline fallback**: if no connectivity, QR shows cached provenance summary signed 24 h ago via PWA service worker

Context-Aware Resolver — One QR, Many Audiences. The GS1 Digital Link Resolver specifies a **link type negotiation mechanism** by which the same physical QR code returns different representations to different requesters. OATS implements four contexts: **Consumer device (default)** — human-readable provenance page in device locale language, anonymous, no personal data captured. **Regulatory device (FSSAI inspector app presenting DID)** — full EPCIS event chain with

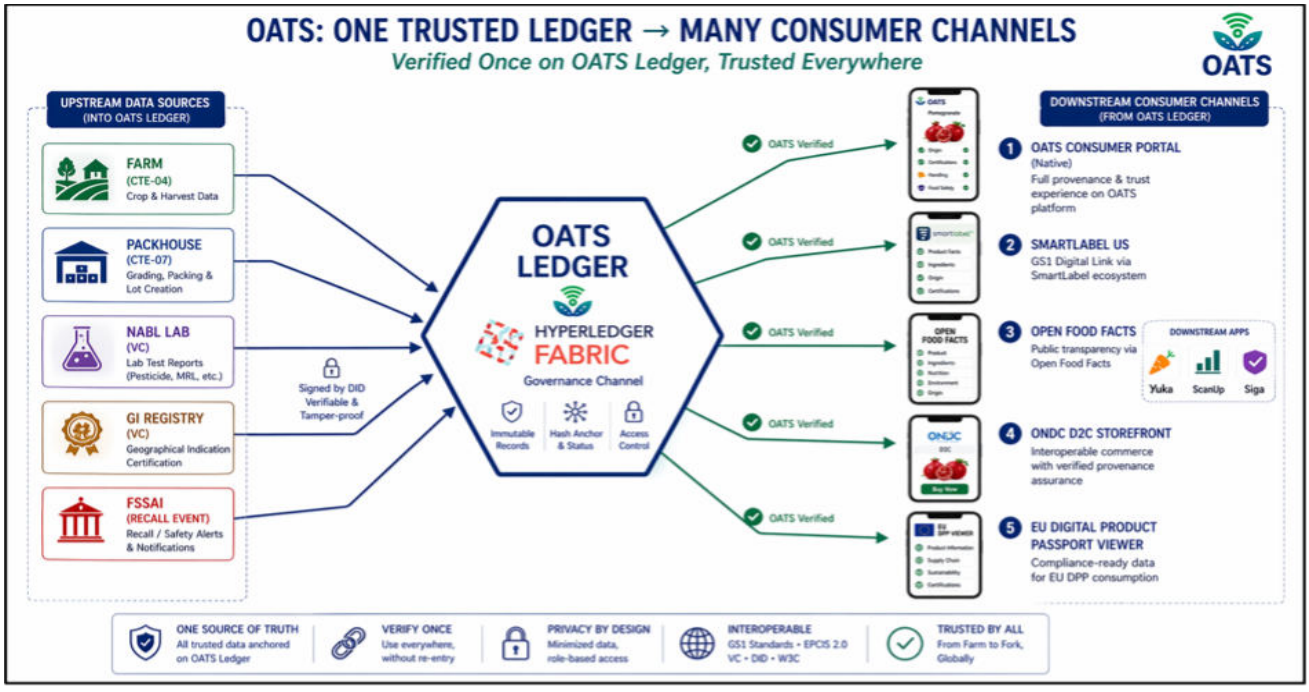
all KDEs, all VCs un-redacted, and AI/ML anomaly flags. **Retailer ERP (presenting OATS API credential)** — structured JSON-LD for integration with ERP, POS, and self-checkout verification flows. **Export authority (EU TRACES NT, US FDA PREDICT)** — the OATS Pre-Export Verification Certificate (PEVC) package per Ch 3 §3.11. **A single printed QR code serves every stakeholder — consumer, regulator, retailer, and destination authority — without privacy leakage across audiences.** Context-sensitivity is enforced by the Resolver at the protocol layer, not by the brand.

15.3 SmartLabel and Open Food Facts Integration

OATS does not replace industry-standard consumer information channels; it feeds them with verified data. Two most consequential external publication channels: the **Consumer Brands Association SmartLabel initiative** (dominant in the US market for packaged food extended disclosure) and **Open Food Facts** (the world's largest open food-product database, used by dozens of downstream health, nutrition, and sustainability apps including Yuka, ScanUp, Siga, and academic research pipelines).

SmartLabel Integration Architecture. When a brand owner registers an OATS-traced lot and opts in to SmartLabel publication, the OATS Layer 5 SmartLabel Adapter generates a SmartLabel-conformant Product Information JSON at the time of CTE-07 Packhouse Transformation. The SmartLabel JSON is populated with Four-Pillar data drawn from the Fabric event chain — **not from brand marketing copy**. The same GS1 Digital Link QR can resolve to either the OATS Resolver (default) or the SmartLabel page where the brand has registered, with the underlying data **byte-identical across both channels** since both pull from the same OATS Event Query API. *This eliminates the current industry problem of divergent claims where the SmartLabel page and the brand website disagree on product origin or certification status.*

Open Food Facts Integration. ODbL licence is compatible with OATS Principle P-1 (Open by Default) and P-4 (Interoperable by Specification). OATS publishes to Open Food Facts through the Open Food Facts API v2 as a registered data-quality contributor.



15.4 Premium Market Access: GI, Organic and Fair-Trade Value Premiums

Consumer transparency and smallholder income are two sides of one coin. The OATS Strategic Objective of Unlocking premium market access for smallholder producers (is operationalised at the consumer interface layer.

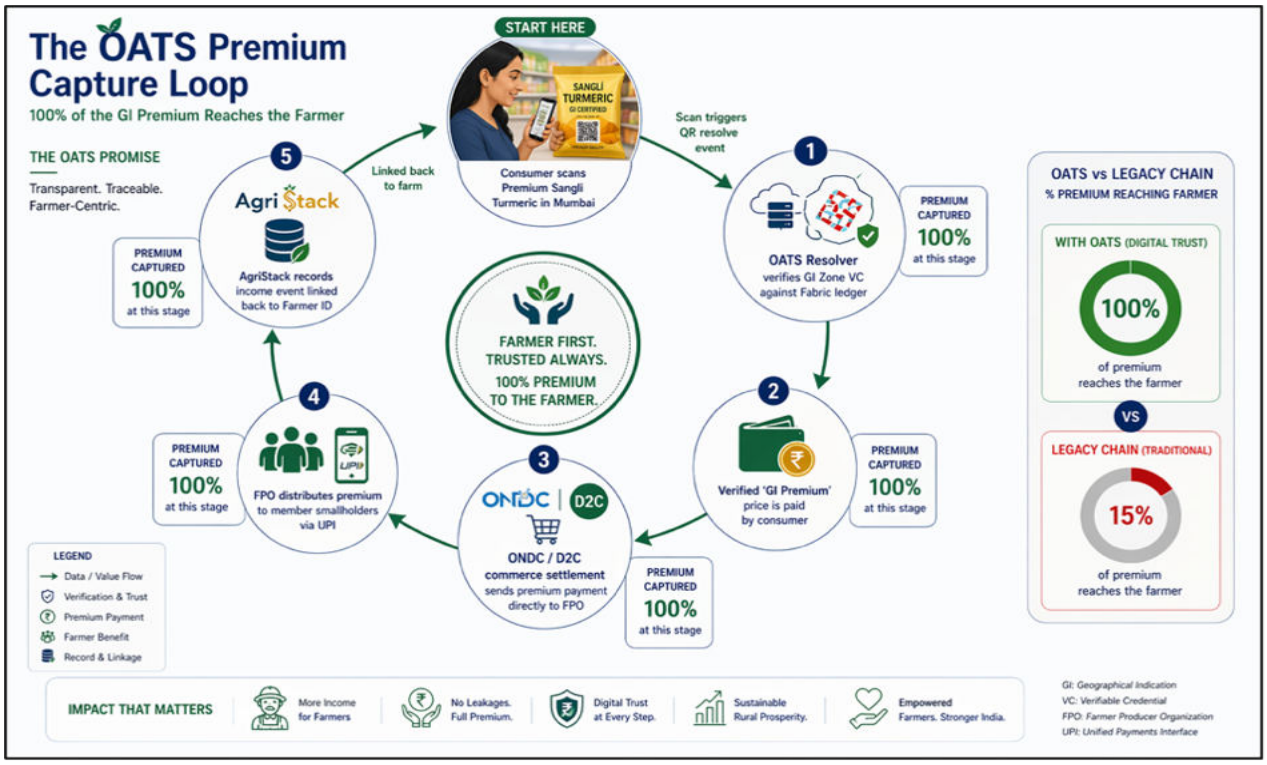
The Premium-Capture Problem. *The current GI and organic premium markets suffer from a classic* ***information-asymmetry failure****.* A consumer in Bengaluru paying a 40% premium for "Sangli Turmeric" has no independent way to verify that the turmeric in the pack actually originated in the Sangli GI zone — historically, random sampling studies have found ***30–60% of GI-labelled products in retail are non-compliant with their stated GI zone***. The premium is captured, but not by the farmer who actually grew the GI-zone produce; it is captured by counterfeiters and opportunistic brands, with none of the price signal reaching the originating smallholder community. *OATS closes the asymmetry with a cryptographic chain-of-proof from the GI-registered farm, through the packhouse, to the consumer QR scan.* ***The GI Zone Verifiable Credential*** *(issued by the INGRES GI Registry and satellite-verified against ISRO Bhuvan field geo-polygons) is embedded in the Fabric event chain and surfaced in the consumer provenance page.* ***A consumer can distinguish a genuine Sangli turmeric lot from a counterfeit with a single scan at zero cognitive cost.*** *The price premium is then re-routed to the originating farmer through OATS-linked D2C commerce rather than intercepted mid-chain.*

Five Premium Categories and the OATS Credential Stack.

Premium Category	Core Credential (W3C VC)	Additional Proofs	Typical estimated Premium
Geographical Indication (GI)	GI Zone VC issued by INGRES / APEDA GI Registry	Satellite field-polygon attestation (Sentinel-2); Harvest ObjectEvent GPS; producer group DID	15–45% over non-GI baseline (Basmati, Darjeeling, Alphonso)
Organic (NPOP / EU Organic / USDA NOP)	Organic Producer Certification VC issued by accredited CB	Group Certification VC (FPO-level); input-use records; NABL residue test VC	20–60% over conventional (turmeric, coffee)
Fair Trade / Fairtrade	Fairtrade SPO Certification VC; Fair Trade USA Mark VC	Fair price premium payment event; FPO dividend disbursement record	10–30% over conventional (coffee, cocoa, tea)
Sustainability (Rainforest Alliance, BCI, EUDR)	RA / BCI / UEBT VC; EUDR DDS VC	Field geo-polygon + deforestation-free satellite attestation; chain-of-custody records	5–20% (plus EU market access)
One-District-One-Product (ODOP) origin attestation	ODOP Origin VC issued by MoFPI district authority	AgriStack Farmer ID + district boundary check	10–25% (emerging; pilot data)

All five categories share the same architecture: a W3C VC issued by the authoritative credentialing body , a Fabric hash anchor, a satellite/GPS geo-verification where applicable, and a consumer-facing surface via the GS1 Digital Link QR. Each premium category plugs into the same protocol; no new integration is needed per credential type.

The OATS Value Proposition to Smallholders. *OATS does not force price premiums; it creates the verification infrastructure that allows premiums consumers are already willing to pay to reach the originating producer.*



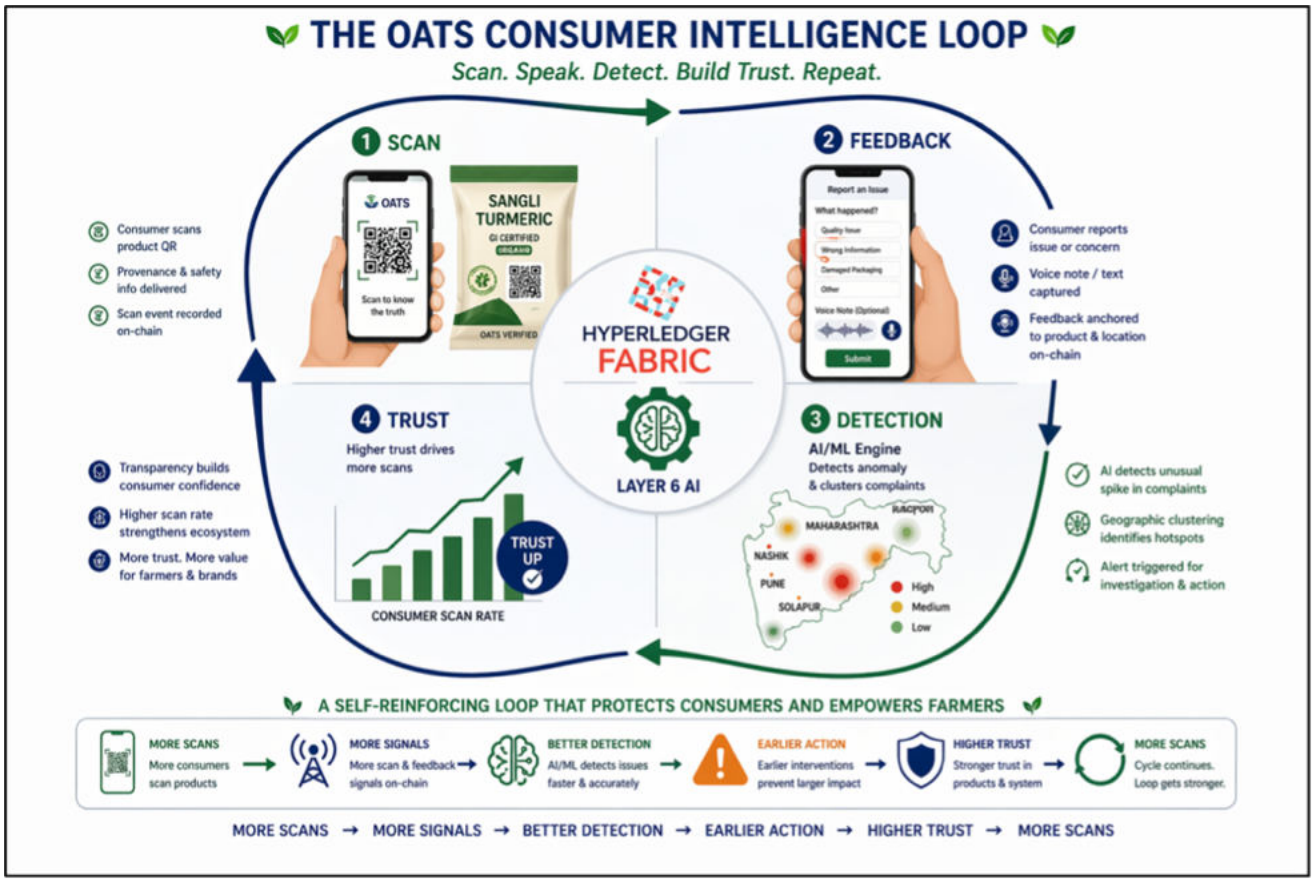
15.5 ONDC and D2C Commerce Integration for GI Products

OATS operates as a registered BPP (Beckn Provider Platform) on the ONDC Agriculture domain. Every OATS-traced consumer unit, not just export lots, is automatically catalog-published to ONDC via the OATS-Beckn Gateway. The ONDC buyer app (BAP) side is consumer-facing: any ONDC-compliant BAP (Magicpin, Paytm, Mystore, etc.) can surface OATS-traced products with the full Four-Pillar provenance summary inline.

Beckn catalogue enrichment populates seven OATS-specific attributes on every catalogue item: item.descriptor.name carrying product name + GI qualifier (e.g., "Turmeric Powder Sangli GI"); item.descriptor.images carrying producer FPO / farm image with DPDPA consent; item.tags[oats:lot_id] carrying OATS LGTIN lot identifier (hidden, used by BAP verification call); item.tags[oats:provenance_url] carrying GS1 Digital Link URI surfaced as "See full journey" link; item.tags[oats:certifications] carrying list of active VC types (organic, GI, fair-trade) surfaced as certification badges; item.tags[oats:origin] carrying district-level origin per DPDPA minimisation surfaced as map pin; item.price.oats_premium_verified Boolean surfaced as "Verified premium" badge for fraud prevention.

15.6 Consumer Grievance and Product Feedback Mechanisms

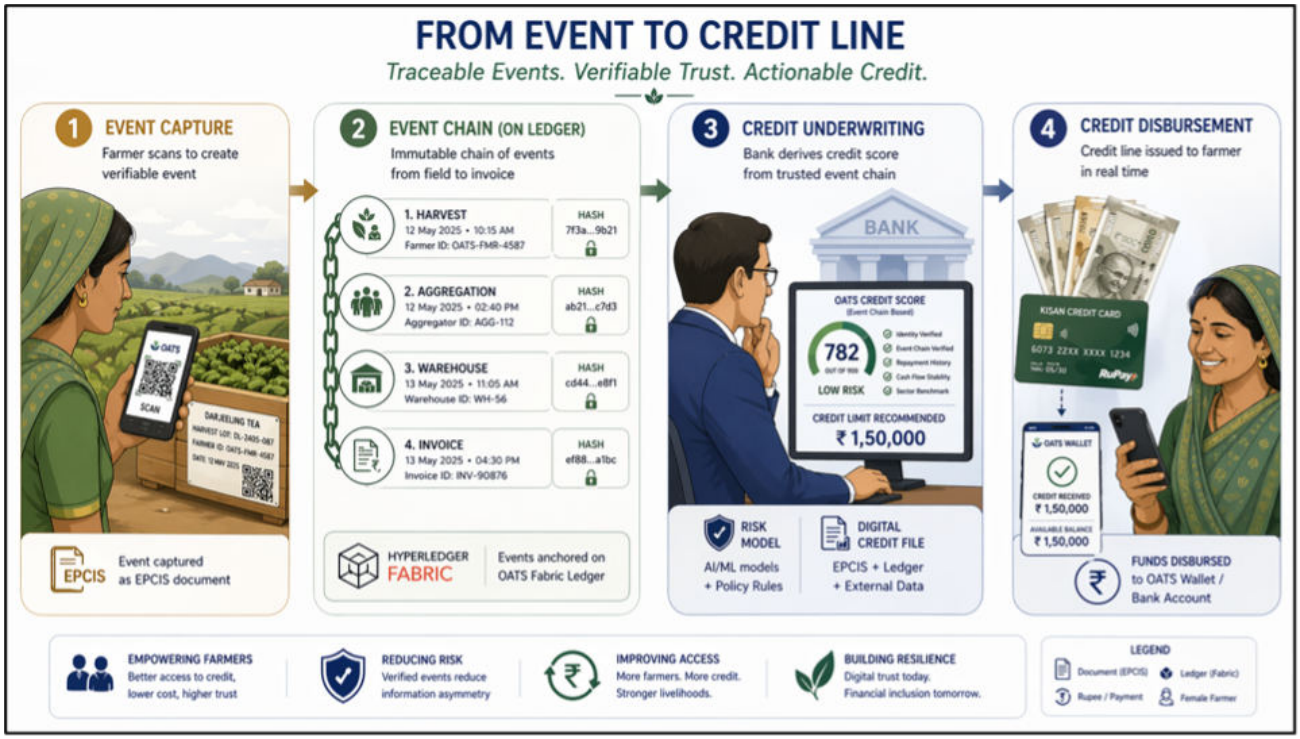
Every OATS-traced lot is not just consumer-readable; it is consumer-writable in a controlled, moderated way. This is the accountability feature that distinguishes OATS from read-only provenance apps — the mechanism by which consumer signals inform the OATS AI/ML anomaly detection engine and the FSSAI risk-profiling system.



16. Financial Inclusion and Value Chain Finance Module

The central premise of this chapter is that **an OATS event chain, a continuous sequence of cryptographically anchored, credential-attested, actor-signed EPCIS 2.0 events from farm declaration through export shipment — constitutes collateral-grade evidence in its own right**. For the first time, a smallholder's farming activity — seeding dates, area declared, input usage, yield harvested, lot sold, price received, warehouse tonnage deposited, invoice raised against a registered buyer is available to a lender or insurer as a **verifiable, tamper-evident, machine-readable history** rather than as a self-declared paper trail. *The 2021 Findex Database recorded that 76% of adults globally now have an account with a financial institution, yet **only 29% of smallholders in low-income economies have ever received a formal agricultural loan**. The binding constraint is no longer account access but underwriting information.* OATS directly closes that gap: every lot-level event carries an actor DID signature, a SHA-256 hash anchored on Hyperledger Fabric, and a chain-of-custody link to preceding and subsequent events. A lender querying the OATS Provenance API with the farmer's consent receives a complete, structured, cryptographically verifiable farming history covering three or more seasons — **the foundation of a credit score**.

This chapter specifies the operational financial-inclusion layer: four financial primitives derived from OATS data, the Agri-Credit Score, supply-chain finance via co-signed Invoice VCs on TReDS, smart-contract milestone escrow, DBT-CBDC integration patterns, PMFBY parametric insurance, eNWR pledge finance, gender-responsive design, and the four-phase financial sustainability glide-path under the Traceability-as-a-Service commercial model.



Table— The Four Financial Primitives Derived from OATS.

Financial Primitive	OATS Data Source	Instrument Enabled

Verified Farming History (3+ seasons)	ObjectEvent (declare), TransformationEvent (harvest), TransactionEvent (sale) on farmer-channel	KCC renewal at preferential rate; term loan for farm capex
Verified Commodity in Storage	AssociationEvent linking OATS lot ID ↔ WDRA eNWR; IoT temperature/humidity sensor stream	Pledge finance against eNWR; warehouse receipt discounting
Verified Receivable / Invoice	TransactionEvent with buyer GLN, purchase order, invoice reference, and signed delivery confirmation	Invoice discounting on TReDS; factoring; bill of exchange
Verified Delivery Milestone	EPCIS ShippingEvent + ArrivalEvent + sensor telemetry attestation at destination GLN	Smart-contract escrow release; trade finance drawdown; LC settlement

Interaction Model with India Stack Financial Rails: OATS does not attempt to replicate existing financial infrastructure, it federates with **Aadhaar eKYC for identity, UPI for payment execution, eSign for document signature, DigiLocker for certificate storage, and the Account Aggregator (AA) framework for consented financial-data sharing**. In the OATS topology, the **farmer's OATS Wallet becomes an AA-recognised Financial Information Provider (FIP) publishing a new data type, Agricultural Activity Data** — that lenders (FIUs) consume under a farmer-granted consent artefact. This positions verified traceability data alongside bank statements and GST returns as a first-class underwriting input.

16.1 Digital Credit Scoring from Supply chain Event data

The OATS Credit Scoring Service (CSS) is a Layer 5 analytics component that ingests a farmer's consented OATS event history and produces a numeric **Agri-Credit Score (ACS) on a 300–900 scale** compatible with the CIBIL/CRIF score format used by Indian lenders. **The ACS is not a substitute for the bureau score — it is a complementary score derived from activity data that bureaus do not see, specifically addressing the thin-file problem** that excludes the majority of smallholders from formal credit.

Table— ACS Feature Space and Weighting

Feature Family	OATS Source Events / Credentials	Indicative Weight
Farming Consistency seasons declared, continuity of crop plan, adherence to declared calendar	ObjectEvent (declare), TransformationEvent (harvest); AgriStack parcel record	20%
Yield Reliability - declared vs. measured yield; satellite-verified crop area; mass-balance at aggregation	TransformationEvent, Sentinel-2 phenology match, AggregationEvent mass-balance	20%
Compliance Quality - PHI adherence, MRL pass rate, VC validity (organic / GI / BCI), calibration status	W3C VC chain, NABL lab VC, CBI inspection VC	15%
Market Depth - number of buyer GLNs, repeat-buyer ratio, mandi diversity, export participation	TransactionEvent buyer pattern; Beckn BAP match history	15%
Price Realisation - average price vs. district benchmark; premium capture for	TransactionEvent commercial value; eNAM / ONDC price reference	10%

GI/organic lots		
Storage Discipline - eNWR deposits, cold-chain SLA adherence, warehouse audit VC status	AssociationEvent (IoT sensor), WDRA eNWR cross-reference	10%
Repayment Track Record — prior KCC, past OATS-linked loan history (if any), PMFBY premium adherence	Account Aggregator feed; OATS loan-repayment VC	10%

Weights are calibrated per commodity sector via supervised learning on historical lender outcome data. **The calibration model is owned by the OATS Governance Council and published as an open technical specification so that every lender computes the same score from the same inputs** — avoiding the fragmentation that has plagued alternative-data scoring in other jurisdictions. Lenders are free to layer proprietary scorecards on top of the ACS but **may not substitute it with a closed replacement** if they consume OATS data under the standard data-sharing agreement.

16.2 Supply Chain Finance: Invoice Discounting and Factoring

The binding constraint on FPO and mid-tier agri-processor working capital is not the absence of buyers — it is the **30-to-90 day payment cycle** between delivery of a lot and realisation of cash. The OATS Supply Chain Finance Gateway (SCFG) converts an OATS-traced invoice into a discountable instrument on the **Reserve Bank of India's Trade Receivables Discounting System (TReDS)** and on ONDC's Financial Services domain, unlocking same-day liquidity for verified supplier-buyer pairs.

From TransactionEvent to Discountable Receivable: A Beckn-confirmed commercial transaction between a supplier BPP and a buyer BAP automatically generates a GS1 EPCIS 2.0 TransactionEvent on the OATS trade-channel, issued as a Verifiable Credential signed by the OATS-Beckn Gateway's DID and cryptographically referencing the parent Lot Declaration VC. In parallel, the supplier issues the commercial invoice itself as a **Commercial Invoice VC signed by the supplier's DID** with the same parent-VC reference. The Invoice VC carries: supplier GLN, buyer GLN, OATS lot ID(s), invoice number, purchase order number, agreed value, currency, agreed payment date, and cryptographic references to the parent Lot Declaration VC and upstream certification VCs (FSSAI, APEDA, phytosanitary, NABL lab). **Upon delivery confirmation (an ArrivalEvent signed at the buyer's GLN), the buyer co-signs the Commercial Invoice VC**, attesting that (i) the goods were delivered, (ii) the buyer has irrevocably accepted, and (iii) the invoice is non-disputed. **The result is a co-signed receivable credential that is intrinsically discountable** — provenance, regulatory compliance, commercial commitment, and buyer acceptance are all verifiable through a single VC presentation back to the sovereign root. **This eliminates the requirement for a separately assembled "Verified Receivable VC" and removes any dependency on the SCFG as a trust intermediary** — the SCFG's role becomes presentation routing to TReDS and ONDC Financial Services, not attestation.

The five-step receivable workflow:

- **T+0** — Beckn confirm generates EPCIS TransactionEvent VC at the OATS-Beckn Gateway. Supplier issues Commercial Invoice VC (signed) at supplier BPP, Goods dispatch generates ShippingEvent VC at Logistics BPP).
- **T+Δ** — Goods arrival generates ArrivalEvent VC + buyer co-sign of Invoice VC at Buyer BPP (on physical receipt).
- **T+Δ+1h** — Co-signed Invoice VC presented on TReDS; auction opens (same-business-day auction SLA).
- **The mechanism is deliberately financier-neutral**. Any RBI-registered TReDS financier (banks, NBFC-Factors) may bid; OATS's role is strictly to enable presentation, with pricing and financing competition happening on the external rail. This structural separation between infrastructure and commercial activity is a direct application of **OATS Principle P-12 (DPI is infrastructure, not platform)**.
- The VC-native chain also directly enables trade credit, supplier financing, and dynamic discounting applications previously gated by the need for separate trust assertions over each piece of evidence.

16.3 Smart Contract Payment Triggers at Delivery Milestones

Where an OATS deployment includes Hyperledger Fabric v2.5 as the immutability layer, the **Traceability Chaincode can be extended with a Milestone Settlement module** that binds the release of escrow funds to the successful commit of defined EPCIS events. **This is functionally equivalent to a letter of credit with delivery-event verification replacing the document-examination step of a conventional LC but executes in minutes rather than days and at a fraction of the cost.**

Table— Milestone Schema.

Milestone	Triggering Event	Verifiable Evidence
M1 - Dispatch	ShippingEvent at source GLN, lot sealed, seal ID recorded	Photographic seal VC + transporter DID signature
M2 - In-Transit Integrity	Continuous IoT sensor stream within SLA thresholds	Cold-chain SLA attestation VC signed by sensor operator
M3 - Arrival	ArrivalEvent at destination GLN, seal intact, weight within tolerance	Destination weighbridge VC + port / buyer signature
M4 - Quality Acceptance	NABL lab VC confirming MRL / moisture / brix within contract spec	Laboratory Result VC with digital signature
M5 - Final Reconciliation	Settlement reconciliation completed; no buyer dispute raised within window	Dispute-free timestamp + buyer final signature

The chain code, written in **Go or Node following the Fabric Smart Contract programming model**, holds the escrowed amount in a pseudo-account reference (funds themselves remain in a scheduled-commercial-bank escrow account governed by an OATS-bank MoU) and releases proportionate amounts upon each milestone event being committed to the trade-channel with valid DID signatures. **Disputes route to a designated arbitration authority whose finding is itself recorded as an AssociationEvent on the chain — preserving the full decision history.**

16.4 CBC and DBT Integration for Direct Benefit Transfer

India's Direct Benefit Transfer architecture currently pushes subsidy and scheme payments (PM-KISAN, input subsidies, PMFBY claim settlements) through Aadhaar-seeded bank accounts via PFMS and APBS rails. **The architecture is mature but blind: the sovereign disbursing agency confirms that a rupee reached a bank account; it cannot confirm that the rupee reached the correct farming activity.** OATS closes this assurance loop in two modes.

- **Pattern A — Traceability-Conditional DBT on APBS.** The Ministry or disbursing scheme publishes an OATS-integrated beneficiary eligibility rule — e.g., for a Direct Income Support scheme: *"₹2,000 per eligible farmer per tri-season, contingent on (i) parcel declared in AgriStack, (ii) OATS ObjectEvent (declare) recorded within the declaration window, (iii) no double-counting with another farmer-ID on the same parcel."* OATS provides a real-time eligibility attestation API consumed by the scheme's PFMS workflow; **APBS release occurs only on a positive attestation**. This pattern requires no change to the CBDC architecture and can be deployed immediately on existing DBT Mission infrastructure.
- **Pattern B — Programmable CBDC with Outcome Binding.** In the **retail CBDC (e₹-R) pilot**, tokens can be issued with programmable spending conditions encoded by the issuing bank. OATS extends this by providing the **outcome-verification oracle**: a PMFBY claim settlement may be issued as a programmable e₹-R token that can be spent at any merchant with no restriction, but with a **post-hoc verification hook** — if the underlying yield-loss claim is later found to be fraudulent against OATS event data, the compensating clawback is triggered automatically. **This preserves the farmer's consumption freedom while closing the fraud-window** that has historically undermined scheme credibility. The legal foundation is being actively explored under the RBI Concept Note on CBDC.

16.5 Crop Insurance Integration with Traceability Events

Pradhan Mantri Fasal Bima Yojana (PMFBY) in its Revised 2023 Guidelines explicitly moves the scheme towards yield-based and weather-indexed settlement with technology-driven loss assessment**.** OATS delivers the technology layer that makes this operationally feasible at population scale — combining satellite yield verification, IoT-attested weather event capture, and farmer-declared loss events into a single verifiable chain the insurer can underwrite against.

Three Insurance Integration Patterns.

Pattern	Risk Priced Against	Trigger Evidence	Settlement Window
Yield-Index (traditional PMFBY)	District-level threshold yield shortfall	District CCE result + OATS crop-area VC + satellite phenology VC	60 days post-season close
Parametric Weather-Index	Rainfall deficit, heat stress, excess rain	IMD / ECMWF weather VC keyed to GLN of declared parcel	T+7 days of weather event recording
Peril-Specific Lot-Level	Cold-chain breach, transit damage, adulteration	OATS sensor-telemetry VC + NABL laboratory VC on affected lot	T+48 hours of lot-level event

The insurer, on enrolling a farmer, receives a **consented OATS event subscription for the insured parcel** — every declared sowing, spray, harvest, and sale event flows to the insurer as a structured stream. **This transforms agricultural insurance from a post-loss inspection model to a continuous-monitoring model**, in which fraud detection is instantaneous (yield claims not matching

declared area, or claims on parcels with no declared crop) and legitimate claims settle automatically against a rule published in the scheme's OATS Regulatory Parameter Registry entry. **Premium calculation itself benefits**: a farmer with three seasons of OATS-verified good agricultural practice (PHI, MRL pass history, consistent yield) qualifies for a lower premium under the scheme's technology-driven risk-adjustment provision.

16.6 Warehouse Receipt Finance: Integration with eNAM and WDRA

OATS supports the existing eNAM and WDRA infrastructure as the operational rails for warehouse-receipt-based finance with one architectural extension: **the electronic Negotiable Warehouse Receipt (eNWR) issued by WDRA-registered warehouses is issued as a Warehouse Receipt Verifiable Credential** signed by the warehouse operator's DID, with a cryptographic reference to the parent Lot Declaration VC of the deposited commodity. The eNWR VC carries: warehouse GLN, WDRA registration number, depositor entity ID, deposited lot ID(s), commodity, quantity, deposit date, quality grade, and the chained reference to the parent Lot VC and upstream certification VCs.

A lender financing against the eNWR can verify in a single chained VC presentation: (i) the warehouse's authority to issue, (ii) the depositor's title to the goods, (iii) the underlying provenance and lot quality, and (iv) the regulatory and quality certifications applicable to the goods — replacing a multi-document verification flow that previously required cross-referencing eNWR records with separate quality test reports, certification status checks, and provenance queries. The **eNWR-as-VC pattern is a Phase-0 deliverable on the Certificates-as-VCs +1 track** — WDRA can begin issuing eNWRs as VCs ahead of full OATS deployment, with the lot-to-eNWR binding established progressively as the OATS lot registry is populated.

OATS ↔ WDRA / eNAM Linkage.

Linkage Point	OATS Artefact	External System	Governance
Deposit moment	AssociationEvent linking OATS lot ID ↔ WDRA eNWR number; warehouse GLN recorded	WDRA eNWR issuance system	eNWR not valid for OATS pledge finance until AssociationEvent is committed
Quality attestation	NABL Lab Result VC attached to the deposited lot; warehouse grading VC	NABL LIMS + warehouse QMS	Lender queries VC chain before sanctioning pledge limit
Storage integrity	Continuous IoT sensor event stream on lot (temperature, humidity, pest control)	Warehouse IoT gateway	Cold-chain SLA attestation refreshed daily; lender notified of any breach
Pledge creation	TransactionEvent recording pledge on eNAM pledge module	eNAM pledge portal (SFAC)	Simultaneous Fabric commit on finance-channel; NABARD refinancing eligibility attested
Release / auction	TransformationEvent or TransactionEvent recording stock release / auction settlement	WDRA eNWR + eNAM	Funds routed to lender first; net to depositor via APBS/UPI

16.7 Gender-Responsive Finance Design for Women Farmer

Women account for an estimated **33% of agricultural land-holders and up to 60% of agricultural labour in South Asia, yet receive less than 10% of formal agricultural credit** — a structural exclusion driven by land-title, mobility, and consent-architecture barriers rather than productivity or repayment performance. OATS is designed from the ground up to surface, recognise, and credit the economic activity of women farmers — **a core conformance requirement under OATS Principle P-18 (Inclusive by Design)**, not an optional add-on.

16.8 Financial Sustainability and Private sector Participation

A traceability infrastructure of this scale cannot be built without a dedicated budget. The credibility of the OATS Blueprint as an implementable DPI rests on a transparent financial sustainability model, one that distinguishes a non-rivalrous public core funded by public means from value-added commercial services priced at recovery, and that defines a phased glide-path from initial concessional finance to a self-supporting operating posture. The model is built on a single organising idea: verifiable provenance is itself a valuable economic good for the downstream value chain, and the infrastructure that produces it can be financed by the parties who capture that value **—** without ever charging the smallholder for the right to be traced**.** Operates under OATS Principles P-1 (Public Goods), P-4 (Open Standards), P-12 (Cost Effectiveness), and P-19 (Sustainable Finance), aligned with World Bank Group PIM Guidance, IFAD's Rural Finance Policy, OECD Principles on PPPs, and G20 Principles for Quality Infrastructure Investment.

Traceability-as-a-Service (TaaS) — Four Commercial Verticals:

Delivered to non-producer counterparties on a fee-paying basis while **smallholders, FPOs, and cooperatives remain zero-rated**.

(i) **Regulatory Compliance Attestation** — on-demand per-lot provenance VCs issued to importers, customs authorities, and brand owners to satisfy due-diligence obligations under EUDR, EU CSDDD, US FSMA, UK Environment Act forest-risk schedules, FSSAI Recall Regulations, and equivalent regimes in Japan, Korea, and the Gulf (per-attestation fee plus annual enterprise licence — the largest near-term revenue opportunity).

(ii) **Premium Quality and Specialty Provenance** — verifiable origin and cultivar credentials for high-margin commodity classes (single-estate specialty coffee, single-origin cocoa, Darjeeling/Assam first-flush teas, single-varietal Basmati, mango and banana cultivar-of-origin, single-estate vanilla, single-source spices and cardamom) where retail premiums of 10–40% reward auditable provenance (per-lot issuance fee, volume-tiered, with margin ceiling on smallholder-borne pass-through).

(iii) **Organic and Regenerative Certification Anchoring** — NPOP / USDA-NOP / EU 2018/848 / Naturland / Bioland / JAS / KOFA certificate chains cryptographically anchored, extending to Regenerative Organic Certified, EOA Africa, Fair for Life, Rainforest Alliance (certifier annual subscription plus per-lot anchor fee, lowering certification-paperwork overhead borne by smallholder cooperatives).

(iv) **Geographical Indication Proof of Provenance** — tamper-evident proof for the **600+ GIs registered under the Indian GI Act 1999** (Darjeeling Tea, Basmati Rice, Naga Mircha, Coorg Cardamom, Alphonso Mango, Banglar Rasogolla, Malabar Pepper, Kashmir Saffron, Mysore Silk) alongside global counterparts (Parmigiano Reggiano, Champagne, Tequila, Roquefort, Colombian Coffee), addresses the **multi-billion-dollar annual counterfeit-GI problem** and WIPO Lisbon Agreement / TRIPS Articles 22–24 obligations.

Private Sector Participation

- **Tier A: Conformant Service Providers** (capture devices, mobile apps, FPO digitisation, last-mile connectivity, certified-laboratory testing — open licensing regime; conformance established through OATS Conformance Test Suite; pricing remains competitive market function.
- **Tier B : Authorised Value-Added Service Operators** (TaaS-derived financial decision-support — execute an Authorised Operator Agreement requiring DPDPA-compliant data handling, fee transparency, audited margin ceiling on services consumed by smallholders, and **Open API parity — any function offered to a paying customer must be exposed to the Open Reference Implementation at protocol cost**).
- **Tier C: Strategic Infrastructure Partners** (cloud, network, managed-service — multi-year framework agreements with vendor-neutrality, exit-portability, and source-code-escrow clauses; **no Tier C partner may hold a position that compromises multi-jurisdiction governance**). **Three non-negotiable guardrails across all tiers**: data sovereignty remains with the data principal under DPDPA 2023; raw event data may not be sold or used to train commercial models without DEPA-grade consent; any commercial IP developed against the OATS Reference Implementation must contribute back schema and conformance refinements under the **Apache-2.0 / Open Government Licence hybrid**.

Four-Phase Blended Financing Glide-Path:

Each phase gated by Key Sustainability Indicators (KSIs) rather than elapsed time alone**.**

- **Phase 1 — Ignition (Years 0–2)** — 100% concessional and grant capital from sovereign budget plus diversified pool: **MDBs** (World Bank, IFAD, ADB, AfDB, IDB, IsDB, AIIB); **bilateral** (KfW/GIZ Germany, JICA Japan, AFD/Proparco France, FCDO UK, USAID, Norad, SIDA, SDC, DANIDA, DFAT, KOICA); **philanthropic** (Gates Foundation, Rockefeller, Ford, IKEA, Mastercard, AGRA, Skoll). KSI gates: minimum active producer DIDs, two conformant Layer 4 query services, operational Governance Council with audited grievance redress.
- **Phase 2 — Co-Investment (Years 2–4)** — Concessional declines to 60–70%; balance from commercial co-investment in Layer 5 financial-service connectors (TReDS, KCC, PMFBY) as revenue-share concessions, pooled impact-investor windows (FCDO MOBILIST, Mastercard Africa Growth Fund, BMGF Catalytic Finance), and producer-organisation own-contribution; Sustainability Fund begins receiving TaaS revenue principally from Compliance Attestation and GI verticals.
- **Phase 3 — Blended Operations (Years 4–7)** — approximately 30% concessional / 40% Sustainability Fund revenue / 30% structured commercial finance (Sustainability-Linked Loans, Agriculture-Green Bonds aligned to **ICMA Green Bond Principles**, outcome-linked partial credit guarantees from MIGA, GuarantCo, or USDFC); KSI gates: TaaS revenue covers at least half of Public Core operating cost, no deploying jurisdiction falls below inclusion floor, gender-disaggregated dashboard shows continued convergence. **Phase 4 — Self-Sustaining (Year 7 onward)** — routine operations met from Sustainability Fund revenue and fiscal allocation; concessional capital retained only for capability expansion and inclusion subsidies. Critically, the glide-path is non-extractive: at no point does the model contemplate user-fees for smallholders accessing core traceability functions, and at no point does the model allow private appropriation of the Public Core.

16.9 Integration with Bharat Trade Net (BTN): India's Trade Documentation and Financing DPI

Bharat Trade Net (BTN) is being established as India's unified Digital Public Infrastructure for international trade — a single platform for trade documentation and trade financing connecting exporters, importers, banks, customs and regulatory agencies, complementing the Unified Logistics Interface Platform (ULIP), and aligned with international electronic-trade-document practice including the MLETR-aligned electronic Bill of Lading. **BTN is a peer DPI to OATS, not a component of it.** OATS is the system of record for verified agri-food provenance and the issuer of verifiable trade documents and receivables; BTN is the rail that distributes those documents to counterparties and routes the associated financing.

Status note: At the time of writing, BTN's detailed technical interfaces are being operationalised. The integration is therefore specified in terms of the artefacts and flows OATS controls — verifiable trade documents, receivable credentials, and settlement callbacks carried over the standard Information Mediator adapter pattern — so the specification remains valid as BTN's API surface stabilises. Field mappings in 16.9.4 are reconciled to BTN's published object model as it becomes available.

The design rests on the **multi-party-verifiability principle** the blueprint adopts from TradeTrust (Chapter 9): a trade document is most useful when any counterparty can verify it independently, without contacting the issuer. OATS issues its trade artefacts as W3C Verifiable Credentials whose validity any BTN participant can confirm through the OATS VC Verification API and Status List 2021, with no bilateral integration required.

16.9.1 The OATS–BTN Relationship

OATS connects to BTN through a single bidirectional adapter carrying two logical rails — a **documentation rail** (16.9.2) and a **financing rail** (16.9.3). The flow is predominantly outbound (OATS issues, BTN consumes); only settlement and status callbacks are inbound. Five OATS artefacts feed BTN:

- **PEVC** — composite export-clearance document; documentation rail; linkable to the eBL.
- **Commercial Invoice VC** — co-signed; underpins both rails.
- **Receivable VC** — discountable instrument; financing rail.
- **Phytosanitary / certification VCs** — supporting documents bundled with the consignment record.
- **eNWR Verifiable Credential** — warehouse-receipt instrument financeable through BTN.

16.9.2 Documentation Rail

OATS submits verifiable trade documents to BTN as verifiable trade-document objects; the PEVC is the anchor artefact, already composing certification, phytosanitary, food-safety, and provenance evidence into a single cryptographically signed credential. Where BTN carries an MLETR-aligned eBL, OATS documents are cryptographically referenced to that eBL **by reference, not by copy** — OATS does not hold the eBL, BTN does not hold OATS event records. BTN counterparties (importers, destination customs, banks) verify each OATS document independently through the OATS VC Verification API and Status List 2021, removing the issuer-verification bottleneck.

16.9.3 Financing Rail

The co-signed Commercial Invoice VC and derived Receivable VC produced by the OATS Supply Chain Finance Gateway (Section 16.2) are routed to BTN-connected financiers as an **additional channel** alongside RBI's TReDS and ONDC's Financial Services domain — the exporter or FPO chooses the rail.

- *Single-financing guarantee:* each Receivable VC is anchored to the OATS ledger; a receivable financed through any rail is marked across all rails, preventing the double-financing failure mode.
- *Settlement callbacks to milestone release:* BTN settlement events are admitted as an external triggering source for escrow release in the Milestone Settlement module (Section 16.3), binding trade finance to verified delivery.
- *Warehouse-receipt finance:* the eNWR VC (Section 16.6) is presentable for financing through BTN as an additional channel to eNAM / WDRA-linked lenders.

16.9.4 The OATS–BTN Adapter

A single bidirectional adapter on the Chapter 10 Information Mediator (X-Road v7). Outbound, it transforms OATS Verifiable Credentials into BTN trade-document objects and financier submissions; inbound, it receives BTN status and settlement callbacks as CloudEvents. The adapter is idempotent, with exponential-backoff retries and a dead-letter queue (SRS-10.8). Illustrative field mapping (reconciled to BTN's published object model): Lot ID / parent Lot Declaration VC → consignment reference; supplier / buyer GLN → trading-party identifiers; invoice number / value / currency / terms → invoice object fields; VC proof + Status List entry → verification endpoint reference (no key material transferred); eBL reference (if present) → title-document linkage by reference only.

Failure handling. BTN is an external dependency treated under the federated-resilience pattern of Section 5.9. BTN unavailability never blocks OATS issuance — documents and receivables are issued and queued; financing submissions retry under circuit-breaker policy; settlement callbacks reconcile on recovery. Trust-critical checks (lawful basis, consent, revocation) fail closed.

16.9.5 Governance, Data Minimisation, Consent

- Cross-border payload minimisation: BTN submissions carry KDE-profile-minimised payloads; farmer identifiers, FPO member lists, and personal data are excluded from cross-border payloads unless specifically mandated (SRS-2.9, SRS-12.7).

- Lawful basis and consent: cross-border flows operate under DPDPA 2023 cross-border-transfer provisions and the cross-jurisdiction governance regime of Section 11.5; personal data flows only under DEPA-aligned consent (Chapter 12); the lawful-basis check is trust-critical and fails closed.

- Audit: every BTN submission and settlement callback is recorded in the append-only, cryptographically chained audit trail (Section 11.6), Merkle roots anchored to the permissioned ledger, 7-year retention.

APPENDICES & REFERENCES

APPENDIX A - CONSOLIDATED FRS / SRS COMPACT MATRIX

A.1 Conformance Tier Framework

Tier	Scope (canonical: Ch 2 §2.10, Ch 3 §3.6, Ch 6 §6.7)
OATS-Core	L1 DID/VC; L2 EPCIS 2.0 capture of CTE-01/02/04/05/07/09 with mandatory KDEs; L3 OpenAPI 3.1; L4 DEPA consent; basic Provenance Query
OATS-Standard	Core + full Ch 7 (GS1 Digital Link Resolver); CTE-03/06/08/10; Ch 8 OATS-Beckn Gateway; Ch 9 Hyperledger Fabric anchoring; Ch 14 EUDR/FSMA/Organic/GI engines
OATS-Advanced	Standard + full IoT cold-chain (FIWARE/OGC); Ch 11 AI/ML with explainability; Ch 18 sustainability VCs; Ch 20 EU DPP; Ch 21 financial-inclusion connectors

Only Ch 14 §14.9 source-tags individual FRS/SRS with tier flags; these are preserved verbatim. Tier assignment for other modules is a senior-reviewer action item (§A.4).

A.2 Functional Requirement Specifications (FRS)

Module 1 — Identity and Trust Infrastructure *(Ch 5)*

ID	Name	Description
FRS-1.1	API Authentication	DID or JWT on every request; anonymous read only for public QR (L5)
FRS-1.2	VC Issuance	W3C VCs for licences/compliance within 24h of certifying event
FRS-1.3	DPDPA Consent	DPDPA 2023-compliant consent; immutable artefact storage
FRS-1.4	Consent Withdrawal	Withdraw via mobile/USSD/IVR within 24h; data minimisation in 7 days
FRS-1.5	DID Resolution	OATS Resolver returns DID Document within 500ms
FRS-1.6	VC Verification	PEVC API verifies VC validity/revocation within 2s
FRS-1.7	Identity Federation	Federate with AgriStack, FPO, FSSAI, APEDA to prevent duplicate entry
FRS-1.8	RBAC Enforcement	Role-based access control with least-privilege principles
FRS-1.9	Audit Logging	Tamper-evident logs retained 7 years (FSS Act 2006)
FRS-1.10	DID Issuance	did:oats or did:agristack within 24h of enrolment; keys + GLN
FRS-1.11	Enrolment Pathways	FPO-batch, Aadhaar-self, assisted (CSC/KVK); no smartphone required *(†)*
FRS-1.12	Key History	Full DID Document key rotation history 7y after deactivation
FRS-1.13	Progressive Validation	Crop declaration on ID confirmation; lot-creation deferred to parcel link
FRS-1.14	VC Schema Registry	Immutable VC schemas at resolvable URIs in Developer Portal
FRS-1.15	Data Principal Rights	Portal for access/correction/grievance rights under DPDPA 2023

Module 2 — Registry and Credentialing Layer *(Ch 5)*

ID	Name	Description
FRS-2.1	Canonical Index	Index records for all entities; update from source registries within 24h
FRS-2.2	Registry Performance	Return registration status and VC hashes within 300ms
FRS-2.3	GIS Mapping	Facility GIS coordinates (WGS 84); geolocation/route analysis
FRS-2.4	IoT Calibration	Flag expired-cert devices; mark events 'sensor_unverified'
FRS-2.5	Product Unique ID	Link every product to GS1 GTIN for global uniqueness
FRS-2.6	Privacy-First Storage	Store only VC hashes/metadata; full content with issuing authority
FRS-2.7	Status Sync	Reflect cert suspension/revocation within 15 min of issuer update
FRS-2.8	Trust Chain Enforcement	Register VCs only if Issuing Body accreditation is Active
FRS-2.9	IoT Provenance	Link devices to operator DIDs + hardware certs; include in EPCIS data

FRS-2.10	Export Compliance	Destination-Country KDE Profiles updated within 90d of regulatory change
FRS-2.11	Farmer Lifecycle	Progressive status (crop record / lot-creation deferred until parcel link)
FRS-2.12	Cached-Response Annotation	Every response served from cache during source-registry failure SHALL carry registry_status, source_registry, as_of, and staleness_seconds; no cached value is presented as live.
FRS-2.13	Trust-Critical Fail-Closed	PEVC issuance, VC revocation verification, and consent verification SHALL refuse to proceed on data exceeding the trust-critical staleness bound; return an RFC 9457 typed error with retry guidance.
FRS-2.14	Reconciliation Audit Event	Every federated-registry reconciliation pass SHALL emit a signed, append-only audit event; divergences beyond the configured threshold SHALL raise a Data Quality Alert.

Module 6 — Traceability Event Data Model *(Ch 6)*

ID	Name	Description
FRS-6.1	EPCIS Event Support	All five EPCIS 2.0 types: Object/Aggregation/Transformation/Transaction/Association
FRS-6.2	CTE Implementation	All ten OATS CTEs (CTE-01 to CTE-10) with mandatory KDE capture
FRS-6.3	Event Validation	Validate against EPCIS 2.0, CBV 2.0, OATS Vocabulary, KDE Mandatoriness Matrix
FRS-6.4	Lot ID Generation	Issue new LGTIN only at CTE-04 (Harvest) and CTE-07 (Transformation)
FRS-6.5	Mass Balance	Real-time validation at Transformation; alert FSSAI FICS on threshold breach
FRS-6.6	IoT Ingestion	FIWARE NGSI-LD / OGC → EPCIS sensorElementList via AssociationEvent
FRS-6.7	Chain-of-Custody	Full upstream/downstream event chain for any Lot ID with input-output bindings
FRS-6.8	Cold Chain Monitoring	Commodity-specific thresholds; alerts within 30s
FRS-6.9	FSMA 204 Export	FDA Sortable Spreadsheet (DID-signed) within 24h regulatory window
FRS-6.10	EU Article 18 Query	One-step-back / one-step-forward queries with contact resolution
FRS-6.11	Data Retention	5y (standard) / 10y (export-related) immutable records
FRS-6.12	Event Correction	EPCIS 2.0 §6 error semantics; use CorrectionEvents, never modify originals

Module 7 — Physical-Digital Linkage *(Ch 7)*

ID	Name	Description
FRS-7.1	Carrier Neutrality	QR, GS1 DataMatrix, RFID (EPC Gen2v2), NFC equally; no privileging
FRS-7.2	GS1 Digital Link	All identifiers encode/resolve to GS1 Digital Link URI (ISO/IEC 18975)
FRS-7.3	Resolver Latency	<3s globally, <1s within operating jurisdiction
FRS-7.4	IoT Telemetry	Accept FIWARE NGSI-LD / OGC SensorThings → canonical OATS schema
FRS-7.5	Breach Alerting	Cold-chain breach to FSSAI FICS and stakeholder wallets within 30s
FRS-7.6	Offline Capture	Farm-gate offline events; sync preserves original cryptographic timestamps
FRS-7.7	Contextual Resolution	Different content per role (Consumer/Inspector/Retailer) via same URI
FRS-7.8	Device Compliance	Device registry (firmware/calibration); flag expired sensors
FRS-7.9	Consumer Privacy	Anonymous access; no registration; no PII collection
FRS-7.10	Sunrise 2027 Ready	Labels readable by POS scanners and consumer smartphones (2D barcodes)

Module 9 — DLT Anchoring *(Ch 9)*

ID	Name	Description
FRS-9.1	Scoped Anchoring	Hashes of EPCIS batches, VCs, Status Lists to append-only consortium ledger
FRS-9.2	Privacy Preservation	No personal/sensitive data on-chain; hashes and non-personal metadata only

FRS-9.3	PEVC Anchoring	Every PEVC anchored within 10s; independent proof verification
FRS-9.4	Smart Contracts	Deterministic execution for compliance rules; consistent across nodes
FRS-9.5	Recall Propagation	Across derived lots within 2s of declaration via on-ledger execution
FRS-9.6	Query Performance	Anchor verification within 2s of valid query
FRS-9.7	Observer Access	Read-only for authorised regulators; no consensus or submission rights
FRS-9.8	Governance Transparency	Publish governance records and execution statistics
FRS-9.9	Ledger Substitutability	Substitute underlying ledger without impacting interface consumers
FRS-9.10	Governance Safeguards	Veto on anchoring prohibited/sensitive data categories

Module 10 — API Architecture and Microservices *(Ch 10 §10.12)*

ID	Name	Description
FRS-10.1	API-First Design	Every capability via versioned API; no UI-exclusive functions
FRS-10.2	Documentation Standards	OpenAPI 3.1, AsyncAPI 2.6, GraphQL SDL at Developer Portal
FRS-10.3	Developer Sandbox	Zero-registration sandbox with synthetic data; daily auto-reset
FRS-10.4	Event Notifications	Webhook delivery within 30s for 99% of events in 24h window
FRS-10.5	Information Mediator	External registries via national Information Mediator
FRS-10.6	Rate Limiting	Per-principal limits with published tiers; 18-month deprecation notices
FRS-10.7	Idempotency	Idempotency-Key header with 24h window
FRS-10.8	Request Correlation	Single X-Correlation-ID across REST/Kafka/webhooks/logs
FRS-10.9	Version Coexistence	Concurrent major versions ≥18 months at distinct URIs
FRS-10.10	Legacy Adapter	Adapters for systems unable to emit native EPCIS 2.0/Beckn/CloudEvents
FRS-10.11	Public Provenance	Anonymous read-only GraphQL endpoint via GS1 Digital Link
FRS-10.12	Conformance Harness	Test harness at Developer Portal for third-party API validation
FRS-10.13	Automated SecOps	Security playbooks for detected API-surface threat classes
FRS-10.14	Deployment Topology	On-Prem, Public Cloud, Federated topologies
FRS-10.15	Compliance Logging	Tamper-evident logs for auth/consent/VC actions retained 7y

Module 11 — Data Governance *(Ch 11)*

ID	Name	Description
FRS-12.1	Data Classification	Four-tier (Open/Institutional/Consented Personal/Regulatory) at API Gateway
FRS-12.2	Fiduciary Registry	Fiduciary / Significant Fiduciary / Processor registry and DPO contacts
FRS-12.3	Federated Queries	Sensitive data stays at origin; transfer only via consent/statute
FRS-12.4	Request Validation	Reject failed Tier/Scope/Purpose/Identity checks; log within 1s
FRS-12.5	Principal Interface	Vernacular mobile/USSD/voice/assisted channels for consent and rights
FRS-12.6	Rights Resolution	Ack 48h; resolve 15 working days; escalate to Farmer Data Rights Ombudsman
FRS-12.7	Purpose Binding	Usage strictly to specific purpose code; new consent for different purposes
FRS-12.8	Retention Lifecycle	Tier-specific retention; daily state transition; action within 7d of expiry
FRS-12.9	Breach Notification	Verifiable notice to DPB and Principals within 72h of confirmed breach
FRS-12.10	Cross-Border Gateway	Full payloads within jurisdictional bounds; minimum verification transmitted
FRS-12.11	Transparency Report	Annual de-identified reports on access, consent, breaches, Ombudsman cases

Module 12 — Consent Management System *(Ch 12)*

ID	Name	Description
FRS-13.1	Compliance Foundation	DPDPA/GDPR artefacts; no personal data into event chain without consent
FRS-13.2	Multilingual Rendering	English + all 22 scheduled Indian languages via text and voice/TTS

FRS-13.3	Channel Parity	Grant/revoke/withdraw via App, USSD, IVR, FPO-assisted terminals
FRS-13.4	Consent Granularity	Single-purpose artefacts; data categories by KDE catalogue identifiers
FRS-13.5	Easy Withdrawal	As simple as grant; effective 24h; propagated to consumers in 7d
FRS-13.6	Audit Integrity	Tamper-evident append-only logs accessible to Principals and DPA
FRS-13.7	Principal Dashboard	Active consent list, access history, grievance, JSON-LD export
FRS-13.8	Selective Disclosure	BBS+ to verify specific attributes without full credential exposure
FRS-13.9	Grievance Ladder	Three tiers (72h / 15d / Statutory); never block DPB escalation
FRS-13.10	System Integration	OATS Entity Registry, AgriStack/MOSIP, API Gateway Tokens
FRS-13.11	Proactive Notification	15d before consent expiry; 60s on data access event
FRS-13.12	Cooling-off Period	24h reversal for high-stakes consents (multi-year / cross-border)
FRS-13.13	Assisted Consent	Co-signing witness + biometric affirmative action
FRS-13.14	Structural Neutrality	CMS stores only signed artefacts + minimal auth profiles
FRS-13.15	Data Retention	5y beyond last processing; align FSS Act / FSMA 204

Module 13 — Regulatory Compliance Framework *(Ch 13)*

ID	Name	Description	Tier
FRS-14.1	Regulatory Rule Engine	Versioned rule-sets on EPCIS 2.0; simultaneous EUDR/FSMA/Organic/GI eval	**Core**
FRS-14.2	EUDR Module	EUDR Due Diligence Statements (JSON/GeoJSON) for 7 commodities in 60s	Standard
FRS-14.3	FSMA 204 Module	FDA-sortable spreadsheets (21 CFR Part 1 Subpart S) for Lot Codes in 60s	Standard
FRS-14.4	GI/PDO Verification	Three-check: credential binding + geofence + product-spec; suppress non-compliant	Standard
FRS-14.5	Organic Module	Verify NPOP/NOP/EU organic VC across handler chains; suppress on breaks	Standard
FRS-14.6	Bilateral Adapters	OATS-EU TRACES, OATS-USA FDA via MC-6	Advanced
FRS-14.7	Rule-set Versioning	SemVer; retain MAJOR versions for 10y rolling window	Standard
FRS-14.8	Compliance Gap Report	JSON-LD/PDF of failed rules, missing evidence, remediation paths	**Core**
FRS-14.9	Data-Protection Overlay	L-4 consent, cross-border controls, DPDPA SDF (DPO/DPIA/Audit)	Standard
FRS-14.10	Regulator API	Authenticated read-only APIs; log access as `oats:regulator_access` events	Standard

Module 14 — Cybersecurity, Privacy and Data Protection *(Ch 14)*

ID	Name	Description
FRS-15.1	Zero-Trust Access	PDP evaluates identity/purpose/consent/context every request
FRS-15.2	Data Encryption	AES-256-GCM with envelope encryption + per-record DEKs for Tier 3
FRS-15.3	Transport Security	Mandatory TLS 1.3 public APIs; mTLS + pinning for gov-to-OATS
FRS-15.4	Multi-Factor Auth	MFA for admins/regulators; FIDO2 or PKI smartcards
FRS-15.5	Composite Policies	RBAC + ABAC; PermitWithObligations for runtime data minimisation
FRS-15.6	Tamper-Evident Logs	Service DID-signed; Merkle roots anchored to Fabric every 5 min
FRS-15.7	Log Retention	7y audit logs (FSS Act); 5y consent logs post-processing
FRS-15.8	Rapid Revocation	Certificates/VCs within 15 min of compromise via OCSP + Status List 2021
FRS-15.9	Automated Response	SEV-1 containment within 15 min without manual approval
FRS-15.10	Breach Notification	Principals notified in registered language within 72h of Tier 3 breach
FRS-15.11	Statutory Reporting	CERT-In within 6h; Data Protection Board within 72h
FRS-15.12	DPIA Register	Updated every 24 months; redacted forms published

FRS-15.13	Pentesting	Quarterly OWASP ASVS 4.0 L2/L3; Critical findings remediated in 7d
FRS-15.14	Bug Bounty	Responsible-disclosure programme with safe-harbor and rewards
FRS-15.15	Algorithm Agility	Central Crypto Register; PQC migration plan within 3y

Module 15 — Consumer Transparency and Market Access *(Ch 15)*

ID	Name	Description
FRS-20.1	Resolver Latency	Four-Pillar provenance page within 1s in India, 3s globally
FRS-20.2	Anonymous Access	Read-only without registration, login, or personal-data collection
FRS-20.3	Multilingual Delivery	22 scheduled Indian languages via Bhashini NMT; equivalent packs elsewhere
FRS-20.4	Text-to-Speech Playback	Bhashini TTS of Four-Pillar within 2s of "Listen" action
FRS-20.5	Context-Aware Resolution	Audience-appropriate output per ISO/IEC 18975
FRS-20.6	SmartLabel Publishing	Four-Pillar verified data within 60s of CTE-07 acceptance (consented brands)
FRS-20.7	Open Food Facts Publishing	OATS-verified fields with "OATS Verified" badge within 5 min
FRS-20.8	ONDC Catalog Enrichment	Lot ID, provenance URL, certs, origin, premium-verified flag in every response
FRS-20.9	Digital Product Passport	CIRPASS DPP JSON-LD within 60s of CTE-09 (EU-bound lots)
FRS-20.10	Grievance Routing	Within 10 min; food-safety <2h, privacy 7d, certification 15d, general 30d
FRS-20.11	Offline Mode	Fabric-signed cached bundles within 24h; "as-of" timestamp
FRS-20.12	Consumer Signal Aggregation	Anonymised grievance clusters to L6 AI/ML within 5 min

Module 16 — Financial Inclusion and Value Chain Finance *(Ch 16)*

ID	Name	Description
FRS-21.1	Agri-Credit Score Computation	ACS (300–900) within 10s of consented request; top 5 features returned
FRS-21.2	DEPA Consent Enforcement	DEPA v1.1 artefacts signed by Principal DID for every financial disclosure
FRS-21.3	Verified Receivable VC	TReDS-compatible Receivable VC within 10 min of buyer ArrivalEvent
FRS-21.4	Milestone Escrow Release	Escrow against EPCIS milestones (Dispatch/Transit/Arrival/Quality/Reconciliation)
FRS-21.5	DBT Eligibility Attestation	Signed VC eligibility <3s per query; bulk-attestation for scheme cycles
FRS-21.6	PMFBY Event Streaming	Insurer endpoint streams <60s; yield-index + parametric weather support
FRS-21.7	eNWR Linkage	AssociationEvent (lot ID ↔ eNWR) within 5 min of issuance
FRS-21.8	Multi-Actor DID Issuance	Distinct DIDs to all adult farming participants regardless of title-holder
FRS-21.9	Gender-Disaggregated Dashboard	Quarterly: DIDs/loans/claim times/grievance outcomes by gender

FRS-21.10	Open Scoring Specification	Feature weights as open spec; reviewed ≤12 months; commodity-calibrated
FRS-21.11	Financial Grievance Redressal	Binding resolution SLA ≤30 calendar days for any financial dispute
FRS-21.12	Optional Participation	Participation-optional; no consent required for core traceability
FRS-21.9	Verifiable Document Submission to BTN	OATS SHALL submit a verifiable trade document (PEVC, Commercial Invoice VC, phytosanitary VC, or eNWR-VC) to BTN as a verifiable trade-document object, with eBL linkage where applicable; BTN parties verify independently via the OATS VC Verification API.
FRS-21.10	BTN Receivable Routing	OATS SHALL route a co-signed Receivable VC to a BTN financier channel as an additional rail to TReDS / ONDC; BTN settlement status reflected back to the originating milestone.
FRS-21.11	Cross-Rail Single-Financing Guarantee	A receivable financed through any rail SHALL be marked across all rails (TReDS, ONDC, BTN) to prevent double financing.

A.3 System Requirement Specifications (SRS)

Module 1 SRS *(Ch 5 §5.9)*

ID	Name	Standard / Metric
SRS-1.1	DID Standards	W3C DID Core v1.0; did:oats open spec co-published with MeitY/MOSIP
SRS-1.2	VC Standards	W3C VC Data Model v2.0; JSON-LD proof (Ed25519 or ECDSA-SD)
SRS-1.3	Revocation Method	W3C Status List 2021; cached bitstring 15-min; no per-VC online lookups
SRS-1.4	Auth Protocols	OAuth 2.0, OIDC 1.0, PKCE for public clients; JWT lifetime ≤1h
SRS-1.5	Transport Security	TLS 1.3 min; TLS 1.2 legacy IoT (18-mo migration); 1.0/1.1 prohibited
SRS-1.6	Gov Integration	mTLS + cert pinning; OATS CA subordinate to NIC CA
SRS-1.7	Consent Format	DEPA Consent Artefact v1.1 with OATS purpose codes; DID-signed
SRS-1.8	Rate Limiting	1k/min Actors, 10k Gov, 100 IoT; burst 3× for 60s; HTTP 429
SRS-1.9	Availability	99.9% L1; 99.95% DID Resolver and VC Verification
SRS-1.10	Deployment	OCI containers; Kubernetes; HPA enabled
SRS-1.11	Long-term Retention	All audit logs + DID/VC operations in append-only store 10 years

Module 2 SRS *(Ch 5 §5.9)*

ID	Name	Standard / Metric
SRS-2.1	Identifiers	GS1 GLN (Facilities), GS1 GTIN (Products), W3C DIDs (Identity)
SRS-2.2	Architecture	Federated registry; InDEA 2.0 RaaS; OATS holds lightweight index only
SRS-2.3	API Specs	OpenAPI 3.1; JSON-LD; 24-month backward compatibility
SRS-2.4	Revocation Reliability	Status List 2021 (15-min sync); 99.99%; alert if >30 min stale
SRS-2.5	Geodata Format	GeoJSON (RFC 7946); 5-decimal precision; AgriStack parcel linkage
SRS-2.6	Data Versioning	Version every change with timestamp/actor DID; 7y history; no deletions
SRS-2.7	Event Notifications	Pub/sub CloudEvents v1.0; <60s latency (<15 min for revocation)
SRS-	Scalability	Microservices (Entity/Product/Facility/Cert/Device); standby replication

2.8		
SRS-2.9	Cross-Border Payload	KDE Profile data minimisation; exclude farmer IDs unless mandated
SRS-2.10	Degraded-Mode Read	Last-known-good served with registry_status=cached annotation; revocation-sensitive operations blocked, not served stale.
SRS-2.11	Registry Reconciliation	Source-of-truth wins on conflict; signed audit event on every pass (7-year retention).
SRS-2.12	Upstream Circuit Breaker	Per-registry circuit breaker with severity-tier alerting via the Notification Service.

Module 6 SRS *(Ch 6 §6.10)*

ID	Name	Standard / Metric
SRS-6.1	API Bindings	GS1 EPCIS 2.0 REST; SOAP legacy-only with deprecation timeline
SRS-6.2	Event Backbone	Apache Kafka; 10k events/sec per node; end-to-end <100ms
SRS-6.3	Immutable Storage	Content-addressed, hash-chained (IPFS-compatible)
SRS-6.4	Serialisation	JSON-LD per EPCIS 2.0 context; GS1 Digital Link URIs for primary EPCs
SRS-6.5	Notification Pattern	Pub/sub CloudEvents v1.0; matching events <30s
SRS-6.6	Query Performance	200 events <3s; 1k events <10s; 10k events <60s
SRS-6.7	Tolerance Engine	OATS Mass Balance Tolerance Registry; default ±2%; registry updates only
SRS-6.8	Reference Implementation	OpenEPCIS (Apache 2.0); alternatives must pass Conformance Test Suite
SRS-6.9	Reliability & Recovery	99.95%; RTO ≤4h; RPO ≤15 min; dual-AZ replication
SRS-6.10	Inter-module Comms	REST (OpenAPI 3.1) + JSON-LD; OAuth 2.0 + PKI cert management
SRS-6.11	IoT Gateway	Bidirectional FIWARE NGSI-LD / OGC SensorThings ↔ EPCIS sensor payloads
SRS-6.12	Vocabulary Governance	vocab.oats.int version-controlled; 18-month breaking-change notice

Module 7 SRS *(Ch 7 §7.9)*

ID	Name	Standard / Metric
SRS-7.1	Carrier Standards	QR (Level M), DataMatrix (ISO/IEC 16022), RFID UHF 865–867 MHz (WPC/DoT)
SRS-7.2	URI Syntax	GS1 Digital Link v1.3 with AIs (01,10,21,17,00); resolver.oats.gov.in
SRS-7.3	Scalability & Uptime	CDN with 3+ India edge nodes; 50k concurrent anonymous; 99.95%
SRS-7.4	Gateway Protocols	FIWARE NGSI-LD v1.6, OGC SensorThings v1.1 via HTTPS/MQTT v5.0
SRS-7.5	Sensor Management	Reading per FSSAI Registry (default 5-min temp-sensitive); NTP 24h sync
SRS-7.6	FPO Agent App	W3C PWA (APK); 30-day offline; CRDT sync; 6+ vernacular languages
SRS-7.7	Printer Specs	203 DPI; 58mm width; Bluetooth LE; min 20×20mm QR smartphone-readable
SRS-7.8	Access Control	§7.8.2 Matrix; DID-based mTLS or OAuth 2.0 bearer tokens
SRS-7.9	Data Tiering	Edge raw telemetry 24 months; OATS Core summary + hashes 10 years
SRS-7.10	Event Formatting	CloudEvents v1.0 HTTP/MQTT; mandatory actor/device DID signing

Module 9 SRS *(Ch 9 §9.12)*

ID	Name	Standard / Metric
SRS-9.1	Platform Type	Permissioned DLT (ref: Hyperledger Fabric or Besu); OATS conformance
SRS-9.2	Consensus Model	Explicitly defined, fault-tolerant; permissionless (PoW) prohibited
SRS-	Interface Security	Standardised IFC-DLT APIs with mTLS; fully documented

9.3		
SRS-9.4	Latency Thresholds	Rapid commitment for event batches and credential issuance
SRS-9.5	Status Checkpoints	Status List anchoring at regular intervals; synchronised timestamps
SRS-9.6	Deployment Safety	Smart contracts require validated test vectors; deterministic execution
SRS-9.7	Identity Integration	All transactions linked to verifiable identities via DID
SRS-9.8	Validator Set	Minimum validator set; multi-party representation
SRS-9.9	IoT Scalability	Two-tier model for high-frequency IoT telemetry
SRS-9.10	High Availability	Multi-zone distributed deployment; DR standards
SRS-9.11	Auditability	All ledger operations audit-logged; long-term retention
SRS-9.12	Data Protection	No personal data processing or exposure at ledger layer
SRS-9.13	Interoperability	Cross-chain via open protocols (e.g., IBC) with defined security

Module 10 SRS *(Ch 10 §10.12)*

ID	Name	Standard / Metric
SRS-10.1	REST API Standards	OpenAPI 3.1; TLS 1.3+; JSON-LD bodies; RFC 9457 errors (problem+json)
SRS-10.2	Event Standards	AsyncAPI 2.6; CloudEvents 1.0 (UUIDv7); backward-compatible schema
SRS-10.3	Kafka Throughput	≥10k events/sec per node; p95 ≤100ms; horizontally scalable
SRS-10.4	Policy Pipeline	10-step Gateway (TLS, WAF, DDoS, JWT, RBAC, Consent, Schema, Rate, ID, Route)
SRS-10.5	Security Handshake	mTLS Gov/IoT; JWT via OATS JWKS; Ed25519 or ES256 only
SRS-10.6	Mediator Protocol	X-Road v7 (or equivalent); RFC 3161 timestamps; non-repudiable logs
SRS-10.7	GraphQL Security	Query cost analysis, depth limit, persisted queries; Apollo Fed v2; no mutations
SRS-10.8	Webhook Protocol	CloudEvents 1.0 HTTP; Ed25519 sigs; 5× exponential backoff; DLQ
SRS-10.9	Orchestration	OCI containers; CNCF Kubernetes; OpenTelemetry; GitOps (Flux/Argo CD)
SRS-10.10	Service Mesh	Intra-cluster mTLS (Istio/Linkerd); declarative auth; trace propagation
SRS-10.11	Portal Assets	Postman collections; auto-generated SDKs; machine-readable changelogs
SRS-10.12	Sandbox Scale	10k Farmers, 200 FPOs, 100k events; daily reset; DPDPA-exempt (synthetic)
SRS-10.13	Crypto Baseline	AES-256; Ed25519; FIPS 140-3 L3 HSM; 90-day cert rotation; PQC ready
SRS-10.14	Availability/DR	3-AZ replication; RTO 4h / RPO 15m; quarterly DR drills
SRS-10.15	Service SLOs	99.95% critical path (Identity, VC, EPCIS, PEVC); 99.9% others
SRS-10.16	Idempotency Cache	24h TTL; return recorded response for duplicates
SRS-10.17	Correlation Flow	Mandatory X-Correlation-ID across every downstream call and log

Module 11 SRS *(Ch 11)*

ID	Name	Standard / Metric
SRS-12.1	Consent Specification	DEPA v1.1 + OATS extensions; Ed25519Signature2020 via Principal DID
SRS-12.2	Revocation Tracking	W3C Status List 2021; 5-min updates; 99.99% availability
SRS-12.3	Secure Audit Trail	Append-only chained log; Merkle roots anchored hourly; 7y retention
SRS-12.4	Gateway Latency	p99 Tier/Scope/Purpose/Identity checks <50ms
SRS-12.5	Processing Inventory	GDPR Art. 30 inventory; exportable within 24h of regulatory request
SRS-12.6	Data Lifecycle Engine	Daily evaluation; anonymisation k-anonymity ≥5, l-diversity ≥3
SRS-12.7	Federated Latency	Cross-Border Gateway federated queries <5s with lawful-basis validation
SRS-12.8	Encryption Standards	AES-256-GCM at rest (FIPS 140-2 L3 HSM); TLS 1.3 in transit
SRS-12.9	Multilingual Access	Vernacular + voice per OATS Voice Interaction Specification
SRS-12.10	High Availability	99.9%; active-active failover ≥2 regions within jurisdiction
SRS-12.11	Deployment Model	OCI containers on Kubernetes with horizontal pod autoscaling
SRS-12.12	Machine-Readable Ops	Transparency Report in CSV + JSON-LD within 90 days of FY close

Module 12 SRS *(Ch 12)*

ID	Name	Standard / Metric
SRS-13.1	Artefact Standards	W3C VC v2.0; JSON-LD with Ed25519Signature2020 or BBS+/ECDSA-SD
SRS-13.2	Semantic Schema	Derived from DEPA v1.1 with OATS extensions as open spec
SRS-13.3	Revocation Logic	W3C Status List 2021; 15-min cached bitstring; no per-artefact online lookup
SRS-13.4	Secure Connectivity	TLS 1.3 min; mTLS + cert pinning for Gov/AgriStack integrations
SRS-13.5	Authorisation	OAuth 2.0 / OIDC; mandatory PKCE; purpose-bound JWTs embed consent ID
SRS-13.6	API Design	OpenAPI 3.1; mandatory sandbox with synthetic data
SRS-13.7	Protocol Standards	USSD (ETSI TS 100 625); IVR (W3C VoiceXML 2.1)
SRS-13.8	Service Availability	99.9% overall; 99.95% Consent Collector/Revocation; 72h maintenance notice
SRS-13.9	Latency Benchmarks	Grant <2s p95; Gateway verification <300ms p95
SRS-13.10	Template Governance	Version-controlled repository; updates trigger version increments + re-consent
SRS-13.11	Cloud-Native Ops	OCI containers; CNCF Kubernetes; HPA (CPU/Mem/Request triggers)
SRS-13.12	Storage Longevity	≥5y consent; 7y audit logs; align FSS Act 2006 and FSMA 204
SRS-13.13	Audit Chaining	Cryptographically chained entries; anchored to Hyperledger every 10 min
SRS-13.14	Breach Engineering	72h notification; multi-channel alerts (SMS/App/FSC) for Tier-3/4
SRS-13.15	Version Control	All interfaces versioned; 18-month migration period for breaking changes
SRS-13.16	Transparency Dash	Monthly public reporting: volumes, withdrawal latency, grievance, SLA

Module 13 SRS *(Ch 13)*

ID	Name	Standard / Metric	Tier
SRS-14.1	Modular Engine Design	Overlays (EUDR, FSMA) as separately deployable engines; upgradeable	**Core**
SRS-14.2	Rule-set Format	Versioned JSON-LD bound to OATS Core Vocabulary; signed by competent authority	Standard
SRS-14.3	Throughput & Latency	≥1,000 lots/sec per node; p95 multi-overlay eval ≤2s nominal	Standard

SRS-14.4	GeoData Standards	GeoJSON (RFC 7946) on WGS 84; polygon topology validation; 4-ha EUDR decomp	Standard
SRS-14.5	Revocation Staleness	W3C Status List 2021; max cache 15 min; uncertain = not-verifiable	**Core**
SRS-14.6	Immutable Audit Logs	10y export / 2–7y domestic; append-only storage	Standard
SRS-14.7	Integration Security	mTLS + cert pinning + app-level message signing via DID-bound keys	Standard
SRS-14.8	API Standards	OpenAPI 3.1 + JSON-LD context; 12-month parallel ops on MAJOR breaking	**Core**
SRS-14.9	Federated Propagation	Cross-jurisdiction federation; rule-set updates ≤60 min with signature verification	Advanced
SRS-14.10	Independent Audit	Annual third-party audit against OATS Conformance Profile; redacted published	Standard

Module 14 SRS *(Ch 14)*

ID	Name	Standard / Metric
SRS-15.1	Architecture Standard	NIST SP 800-207 (Tenets 1,2,3,4,6); annual verification
SRS-15.2	Crypto Validation	FIPS 140-3 L2 min; sovereign root ops require FIPS 140-3 L4 HSMs
SRS-15.3	TLS Cipher Suites	TLS_AES_256_GCM_SHA384, CHACHA20_POLY1305, AES_128_GCM only; legacy/CBC disabled
SRS-15.4	Sovereign PKI	Subordinate under NIC Root CA or equivalent
SRS-15.5	Revocation Services	OCSP Responders 99.95%; CRL Distribution Points every 4h
SRS-15.6	Policy Engine	OPA/Rego; evaluation <50ms p99
SRS-15.7	Log Storage	Append-only immutable with MFA-delete; roots to DLT within 10 min
SRS-15.8	SIEM Ingest	100k events/sec; 365-day hot retention; 7-year archive
SRS-15.9	SOC Operations	24×7; MTTD ≤15 min; MTTR ≤30 min
SRS-15.10	Image Scanning	Dual-scanner (Trivy/Grype); block High/Critical CVEs
SRS-15.11	K8s Hardening	CIS Kubernetes Benchmark L1 + L2; weekly auto scans
SRS-15.12	DPO Governance	Resident Indian DPO; direct report to highest body
SRS-15.13	Audit Integrity	Pentest reports within 10 days; no operator pre-filtering
SRS-15.14	Red Teaming	Annual TIBER-EU aligned; redacted summary within 90 days
SRS-15.15	Crypto Governance	Signed versioned register; 90-day notice except crypto emergencies

Module 15 SRS *(Ch 15)*

ID	Name	Standard / Metric
SRS-20.1	Progressive Web App	W3C PWA on Android 8+ or iOS 13+ without native installation
SRS-20.2	Digital Link Resolver	ISO/IEC 18975 link-type resolver; Accept headers + DID/API credentials
SRS-20.3	CDN Geographic Coverage	Min 3 Indian + 3 international regions; <1s India / <3s global
SRS-20.4	API-Gateway Mediation	L3 + L4 API access only (Event Query, VC Verification); auth, rate-limited
SRS-20.5	Bhashini Integration	ULCA-compliant NMT/TTS/ASR; edge translation cache 24h TTL
SRS-20.6	Open Food Facts API	OFF API v2 data-contribution spec; OATS schema extension
SRS-20.7	DPP Output Format	JSON-LD 1.1 conforming to CIRPASS DPP CDM and UN/CEFACT UNTP
SRS-20.8	VC Revocation Checking	W3C Status List 2021; 99.99%; 15-min non-revocation confirmation
SRS-20.9	Accessibility Conformance	W3C WCAG 2.2 Level AA audited annually; progressive disclosure (GDS P1)
SRS-20.10	Grievance Framework	OpenG2P notification framework; DPDPA pseudonymised consumer IDs
SRS-20.11	Service Availability	99.95% on rolling 30-day window; automatic CDN fail-over <60s
SRS-20.12	Open-Source Licensing	Apache 2.0 or EUPL as Digital Public Goods per OATS P-1

Module 16 SRS *(Ch 16)*

ID	Name	Standard / Metric
SRS-21.1	Credit Scoring Microservice	Stateless Kubernetes microservice with HPA; JSON-LD OpenAPI 3.1; p95 <2s
SRS-21.2	Financial VC Conformance	W3C VC v2.0; JSON-LD proof (Ed25519Signature2020 or ECDSA-SD)
SRS-21.3	DEPA & Account Aggregator	DEPA v1.1; Sahamati AA-1.1.2 with two production AAs; Fabric anchor <10s
SRS-21.4	TReDS Integration	RBI TReDS via mutual-TLS REST; single abstract factoring adapter for all 3 TReDS
SRS-21.5	Milestone Chaincode	Go-based Hy scikit-learnperledger Fabric v2.5 chaincode; formally verified against schema
SRS-21.6	PFMS / APBS / CBDC	mTLS with NIC-CA client certs; RBI e₹-R spec for programmable-token integration
SRS-21.7	PMFBY Delivery Patterns	Webhook push (HMAC-SHA256) + signed-query pull; idempotent exactly-once
SRS-21.8	Warehouse Receipt API	WDRA eNWR + eNAM pledge-finance REST APIs; atomic AssociationEvent commit
SRS-21.9	DID Issuance & Schema	One DID per adult; biometric-seeded key derivation; OATS Schema v2.0
SRS-21.10	Open Data Dashboard	Machine-readable CSV + JSON-LD endpoint + Transparency Portal dashboard
SRS-21.11	Service Availability	99.9% L5 financial services; 99.95% Credit Scoring and Verified Receivable VC
SRS-21.12	Audit Trail Retention	10-year tamper-evident aligning FSS Act 2006 and RBI loan-record requirements
SRS-21.13	Regulatory Parameter Registry	JSON-Rules-Engine machine-readable rule sets; signed regulator updates
SRS-21.14	API-Gateway Mediation	L5 components access events only via L3 Provenance Query Service
SRS-21.15	OATS–BTN Adapter	Bidirectional, idempotent adapter on the Information Mediator (X-Road v7); CloudEvents callbacks with exponential-backoff retries and a dead-letter queue; degraded-mode behaviour per Section 5.9.
SRS-21.16	Cross-Border Payload Minimisation	BTN payloads SHALL be KDE-profile-minimised; personal data excluded unless mandated (SRS-2.9 / SRS-12.7); lawful-basis validation SHALL fail closed.
SRS-21.17	Verification Without Key Transfer	BTN submissions SHALL reference the OATS verification endpoint and Status List; no OATS key material or full event records SHALL be transferred to BTN.

APPENDIX B — STANDARDS INDEX AND REFERENCES

Category	Standard / Document	Issuer	Year	URL
W3C Identity & Web	DID Core v1.0	W3C	2022	w3.org/TR/did-core/
	VC Data Model v2.0	W3C Credentials CG	2025	w3.org/TR/vc-data-model-2.0/
	VC Status List 2021	W3C CCG	2022	w3.org/community/reports/credentials/CG-FINAL-vc-status-list-2021
	Progressive Web Apps Manifest	W3C	2024	w3.org/TR/appmanifest/
	WCAG 2.2 Level AA	W3C WAI	2023	w3.org/TR/WCAG22/
	ARIA 1.2	W3C	2023	w3.org/TR/wai-aria-1.2/
	Web Speech API	W3C	2020	w3.org/TR/webspeech-api/
	VoiceXML 2.1	W3C Voice Browser WG	2007	w3.org/TR/voicexml21/
	JSON-LD 1.1	W3C	2020	w3.org/TR/json-ld11/
DIF	Presentation Exchange 2.0; BBS+ Signatures	Decentralized Identity Foundation / IRTF CFRG	2023	identity.foundation/presentation-exchange/
GS1	EPCIS 2.0 (ISO/IEC 19987:2024); CBV 2.0	GS1 Global / ISO	2024	gs1.org/standards/epcis
	EPCIS 2.0 REST Bindings Implementation Guideline	GS1 Global	2022	gs1.org/docs/epcis/EPCIS-REST-Bindings
	General Specifications v24	GS1 Global	2024	gs1.org/standards/barcodes-epcrfid-id-keys/gs1-general-specifications
	Digital Link Standard v1.3 (ISO/IEC 18975)	GS1 Global / ISO	2022	gs1.org/standards/gs1-digital-link
	EPC Tag Data Standard 2.0	GS1 Global	2024	gs1.org/standards/epcrfid/tds
	Sunrise 2027 Programme (Retail 2D Barcode Transition)	GS1 Global	2021–2027	gs1.org/2Dbarcodes
	US FSMA 204 Recommendations	GS1 US	2023	gs1us.org
	GTIN Allocation and National Resolver Roadmap	GS1 India	2024	gs1india.org
ISO TC 34 (Food)	ISO 22000:2018 Food Safety Mgmt	ISO TC 34/SC 17	2018	iso.org/standard/65464.html
	ISO 22005:2007 Traceability in the Feed and Food Chain	ISO TC 34/SC 17	2007	iso.org/standard/36297.html
ISO Other	ISO 23412:2020 Temperature-Controlled Refrigerated Delivery	ISO TC 315	2020	iso.org/standard/75468.html
	ISO 8000 Data Quality	ISO TC 184/SC 4	ongoing	iso.org/standard/50798.html
	ISO 14021 Self-Declared Environmental Claims	ISO	ongoing	iso.org/standard/66652.html
	ISO/IEC 17065 Conformity Assessment	ISO/CASCO	2012	iso.org/standard/46568.html
ISO/IEC JTC 1/SC 27 (Security)	27001:2022 ISMS; 27035:2023 Incident Mgmt; 27701:2019 Privacy Info Mgmt	ISO/IEC	2019–2023	iso.org/standard/27001
ISO/IEC JTC 1/SC 31 (Auto-ID)	18004:2015 QR Code; 16022:2006 DataMatrix; 18000-63:2015 RFID UHF (EPC Gen2)	ISO/IEC	2006–2015	iso.org/standard/62021.html
ISO/IEC JTC 1/SC 17 (Identification	14443 NFC Type A/B; 15693 NFC Type 5	ISO/IEC	2016–2020	iso.org/standard/73597.html

Cards)				
Codex Alimentarius	CAC/RCP 1-1969 Rev. 2020 Food Hygiene (HACCP); CAC/GL 60-2006 Traceability; CAC/GL 32 Rev. 1999 Organic	FAO/WHO Codex	1999–2020	fao.org/fao-who-codexalimentarius
WHO / FAO	INFOSAN (190+ countries)	WHO / FAO	ongoing	who.int/groups/international-food-safety-authorities-network-(infosan)
	WHO PQS Cold Chain Equipment Specifications	WHO	2024	extranet.who.int/prequal/vaccines/pqs-documents
IPPC	ePhyto Hub XML; ISPM 7/12 Phytosanitary Certificates	IPPC FAO	2021	ippc.int/en/ephyto/
EU Food & Trade	Reg. (EC) 178/2002 General Food Law	European Commission	2002	eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002R0178
	Reg. (EC) 396/2005 MRLs Pesticides	European Commission	2005	eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005R0396
	Reg. (EU) 1151/2012 GI Quality Schemes	European Commission	2012	eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R1151
	Reg. (EU) 1169/2011 Consumer Food Information	European Commission	2011	eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011R1169
	Reg. (EU) 2017/625 Official Controls	European Commission	2017	eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0625
	Reg. (EU) 2018/848 Organic	European Commission	2018	eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0848
	Reg. (EU) 2021/1935 Accreditation	European Commission	2021	eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R1935
	Reg. (EU) 2023/1115 EUDR (Deforestation-Free Products)	European Commission	2023	eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1115
	Reg. (EU) 2024/1143 GI (unified)	European Commission	2024	eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1143
	Reg. (EU) 2024/1781 ESPR / Digital Product Passport	European Commission	2024	eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1781
	Directive (EU) 2024/1760 CSDDD	European Commission	2024	eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L1760
EU Data Protection	Reg. (EU) 2016/679 GDPR	European Parliament/Council	2016	eur-lex.europa.eu/eli/reg/2016/679/oj
	EDPB Guidelines 05/2020 on Consent	European Data Protection Board	2020	edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679
EU Platforms	TRACES NT	EC DG SANTE	ongoing	webgate.ec.europa.eu/tracesnt/login
	iRASFF (Rapid Alert System for Food and Feed)	EC DG SANTE	since 2021	food.ec.europa.eu/safety/rasff_en
	CIRPASS DPP Common	EC / CIRPASS	2024	cirpassproject.eu

	Data Model	Consortium		
	eTranslation	EC DG CNECT	ongoing	commission.europa.eu/resources-partners/etranslation_en
US FDA	FSMA §204 Final Rule (21 CFR Part 1 Subpart S, 87 FR 70910); FSVP (Subpart L); PREDICT; OASIS; Reportable Food Registry	US FDA	2015–2022	fda.gov/food/food-safety-modernization-act-fsma
US Other	USDA NOP (7 CFR Part 205, SOE Final Rule 88 FR 17748)	USDA AMS	2024	ams.usda.gov/rules-regulations/organic
	Uyghur Forced Labor Prevention Act (PL 117-78)	DHS	2021	dhs.gov/uflpa
India Food & GI	FSS Act 2006; FSS (Recall) Regs 2017 + draft 2024; FSS Import Regs 2017; FSSAI Schedule 4	FSSAI	2006–2024	fssai.gov.in
	GI Act 1999 (Geographical Indications of Goods)	GoI / CGPDTM	1999	ipindia.gov.in
	NPOP 8th Ed.; APEDA Act 1985 (e-TraceNet/HortiNet)	APEDA	1985–2014	apeda.gov.in/apedawebsite/organic
	FT(D&R) Act 1992	DGFT	1992	dgft.gov.in
India Data Protection	DPDPA 2023 (Act 22 of 2023); DPDP Rules 2025	MeitY	2023–2025	meity.gov.in/data-protection-framework
	IT Act 2000 (§§43A/72A/79)	MeitY	2000	meity.gov.in/content/information-technology-act-2000
	CERT-In Directions §70B(6)	CERT-In	2022	cert-in.org.in
India Consumer/Disability	Consumer Protection Act 2019	GoI	2019	consumeraffairs.nic.in
	Rights of Persons with Disabilities Act 2016	GoI	2016	disabilityaffairs.gov.in
India DPI	AgriStack Farmer Registry API	MeitY / NeGD	2024	agristack.gov.in
	Bhashini National Language Technology Mission	MeitY	2022	bhashini.gov.in
	InDEA 2.0 Framework Document	NeGD / MeitY	2022	negd.gov.in/india-enterprise-architecture
	DEPA Consent Artefact v1.1	Sahamati / NITI Aayog	2022	sahamati.org.in
	Sahamati Account Aggregator AA-1.1.2 Framework	Sahamati	2022–2025	sahamati.org.in
	MOSIP (Modular Open Source Identity Platform)	MOSIP Foundation / IIIT-B	ongoing	mosip.io
India Finance	Account Aggregator Master Directions (2016 Rev. 2023); TReDS; V-CIP Master Directions; e₹-R CBDC Concept Note	Reserve Bank of India	2016–2024	rbi.org.in
India Agri Finance	PMFBY Revised 2023 Guidelines	Ministry of Agriculture	2023	pmfby.gov.in
	WDRA eNWR Regulations	WDRA	ongoing	wdra.gov.in

	eNAM (National Agriculture Market)	SFAC	ongoing	enam.gov.in
	PM-KISAN; DBT-F (Fertiliser); MSP Procurement (NAFED/FCI)	GoI Ministries / NABARD	2014–2023	pmkisan.gov.in
India Telecom/Spectrum	WPC/DoT UHF RFID 865–867 MHz Spectrum Allocation	DoT	2021	dot.gov.in/spectrummanagement
	TRAI Commercial Communication Regs + DLT Registration	TRAI	ongoing	trai.gov.in
UK	UK Retained EU Law; BRCGS; Environment Act forest-risk schedules; IPAFFS; UKCA	UK FSA / UK Government	ongoing	food.gov.uk
Japan	Plant Protection Act; Positive List System; JAS Organic	Japan PPC / MAFF	ongoing	maff.go.jp/e/
UAE / GCC	SFDA; GSO Standards; Halal Certification	SFDA / GSO	ongoing	sfda.gov.sa/en
Other Jurisdictions	Brazil LGPD (Law 13,709/2018)	Government of Brazil	2018	planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm
	Kenya Data Protection Act 2019	Government of Kenya	2019	odpc.go.ke
	South Africa POPIA (Act 4/2013)	Republic of South Africa	2013	justice.gov.za/inforeg/
	Singapore-Australia Digital Economy Agreement	Governments of SG / AU	2020	dfat.gov.au/trade/agreements/in-force/sadea
	EU-Japan Mutual Adequacy Decision	EC / Japan PPC	2019	commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
	APEC Cross-Border Privacy Rules System	APEC	2011 Rev.	cbprs.org
Certifications & Schemes	GLOBALG.A.P. IFA v6 Smart / CoC v6	GLOBALG.A.P.	2023	globalgap.org
	Better Cotton Initiative Production P&C	BCI	ongoing	bettercotton.org
	Rainforest Alliance / UTZ-merged	Rainforest Alliance	ongoing	rainforest-alliance.org
	Fairtrade International / Fairtrade India	Fairtrade International	ongoing	fairtrade.net
	SMETA / Sedex (2-pillar/4-pillar audit)	Sedex	ongoing	sedex.com
	GRI 13 (Agriculture, Aquaculture, Fishing Sector)	Global Reporting Initiative	2022	globalreporting.org/standards/standards-development/sector-standard-for-agriculture-aquaculture-and-fishing/
	Regenerative Organic Certified; Naturland; Bioland; Fair for Life; EOA Africa	Various certifying bodies	2018–2024	regenorganic.org
WTO / WIPO	TRIPS Agreement Art. 22–24 (Geographical Indications)	WTO	1995	wto.org/english/docs_e/legal_e/27-trips.pdf
	Lisbon Agreement Geneva Act 2015	WIPO	2015	wipo.int/lisbon/en/

	WTO SPS Agreement	WTO	1995	wto.org/english/tratop_e/sps_e/spsagr_e.htm
IETF RFCs	RFC 8446 TLS 1.3; RFC 6749 OAuth 2.0; RFC 7636 PKCE; RFC 9457 Problem Details; RFC 7946 GeoJSON; RFC 3161 Time-Stamp Protocol; RFC 5280 X.509 PKI; RFC 2119 Requirement Keywords	IETF	1997–2023	datatracker.ietf.org
OpenAPI / AsyncAPI / GraphQL	OpenAPI 3.1	OpenAPI Initiative	2021	spec.openapis.org/oas/v3.1.0
	AsyncAPI 2.6	AsyncAPI Initiative	2022	asyncapi.com/docs/reference
	GraphQL Specification (October 2021)	GraphQL Foundation	2021	spec.graphql.org/October2021/
	JSON Schema 2020-12	IETF / JSON Schema Org	2020	json-schema.org/specification
CNCF	CloudEvents v1.0	CNCF Serverless WG	2022	cloudevents.io
	Apache Kafka	Apache Software Foundation	2024	kafka.apache.org/documentation
	Kubernetes	CNCF	2024	kubernetes.io/docs
	Istio Service Mesh	CNCF	2024	istio.io/latest/docs
	OpenTelemetry	CNCF	2024	opentelemetry.io/docs/specs
Hyperledger	Fabric v2.5	Linux Foundation / Hyperledger	2024	hyperledger-fabric.readthedocs.io
	Besu (QBFT/IBFT 2.0)	Linux Foundation / Hyperledger	2024	besu.hyperledger.org
IoT / Sensor	FIWARE NGSI-LD v1.6 (ETSI GS CIM 009)	ETSI ISG CIM / FIWARE	2024	fiware.org/developers/ngsi-ld/
	OGC SensorThings API Part 1 (OGC 15-078r6)	Open Geospatial Consortium	2016	ogc.org/standards/sensorthings
	MQTT v5.0	OASIS MQTT TC	2019	docs.oasis-open.org/mqtt/mqtt/v5.0/
Security & Crypto	NIST SP 800-207 Zero Trust Architecture	NIST	2020	csrc.nist.gov/publications/detail/sp/800-207/final
	NIST SP 800-162 ABAC; SP 800-61 Incident; SP 800-204A/B Microservices	NIST	2012–2023	csrc.nist.gov/publications
	FIPS 140-3 Crypto Modules	NIST	2019	csrc.nist.gov/publications/detail/fips/140/3/final
	FIPS 203/204/205 Post-Quantum Cryptography	NIST	2024	csrc.nist.gov/projects/post-quantum-cryptography
	TIBER-EU Framework (Threat Intel-Based Ethical Red-Teaming)	European Central Bank	2018	ecb.europa.eu/paym/cyber-resilience/tiber-eu/
	OWASP API Security Top 10 (2023); ASVS 4.0	OWASP Foundation	2019–2023	owasp.org/API-Security/
Identity / KYC	UIDAI AUA/KUA APIs	UIDAI	ongoing	uidai.gov.in
	STQC L1 Biometric Devices Certification	STQC	ongoing	stqc.gov.in
	DigiLocker Issuer APIs	NeGD / MeitY	ongoing	digilocker.gov.in
	TPM 2.0 Attestation	Trusted Computing Group	2019	trustedcomputinggroup.org/resource/tpm-library-specification/
Open-Source Licences	Apache 2.0	Apache Software Foundation	2004	apache.org/licenses/LICENSE-2.0
	EUPL	European	2017	eupl.eu

		Commission		
	MIT License	OSI	ongoing	opensource.org/licenses/MIT
	ODbL (Open Database Licence)	Open Data Commons	2009	opendatacommons.org/licenses/odbl/
	Open Government Licence	UK National Archives	2014	nationalarchives.gov.uk/doc/open-government-licence/version/3/
DPI Frameworks	GovStack Building Block Specification v2.0	GovStack Initiative (ITU/DIAL)	2025	specs.govstack.global
	Universal DPI Safeguards Framework v2.0	UNDP / UN Tech Envoy	2025	dpi-safeguards.org
	CDPI Architecture Principles	Centre for Digital Public Infrastructure	2023	cdpi.dev/architecture
	G20 DPI Principles (DEWG Aug 2023)	G20 India Presidency	2023	g20.org
	Digital Public Goods Standard v1.0	DPG Alliance	2020	digitalpublicgoods.net
	X-Road v7 Technical Documentation	Nordic Institute for Interoperability Solutions	2024	x-road.global/documentation
International Bodies	OECD Principles on Public-Private Partnerships; Guidelines on Privacy and Transborder Data Flows	OECD	1980–2013 Rev.	oecd.org/governance/policy-framework-for-investment/
	G20 Principles for Quality Infrastructure Investment	G20	2019	g20.org
	World Bank PIM Guidance; DPI 2025 White Paper	World Bank Group	2025	worldbank.org/dpi
	IFAD Rural Finance Policy; Gender Transformative Approaches Compendium	IFAD	ongoing	ifad.org
	IFC Banking on Women Measurement Framework	International Finance Corporation	ongoing	ifc.org
	ICMA Green Bond Principles	International Capital Market Association	2021	icmagroup.org/sustainable-finance/the-principles-guidelines-and-handbooks/green-bond-principles-gbp/
Human Rights / Privacy	UDHR Art. 12	UN General Assembly	1948	un.org/en/about-us/universal-declaration-of-human-rights
	UNGA Resolution A/RES/68/167 (Right to Privacy in the Digital Age)	UN General Assembly	2013	undocs.org/A/RES/68/167
	UN Guidelines for Consumer Protection (A/RES/70/186)	UNCTAD	2016	unctad.org/topic/competition-and-consumer-protection/un-guidelines-for-consumer-protection
	Charter of Fundamental Rights of the EU (Art. 7/8)	EU	2000	eur-lex.europa.eu/eli/treaty/char_2012/oj
	Puttaswamy v. Union of India (2017) 10 SCC 1	Supreme Court of India	2017	main.sci.gov.in
OATS Reference Implementations	OpenEPCIS Reference Implementation (Apache 2.0)	Benelog GmbH & Co. KG	2022–2025	openepcis.io

APPENDIX C — SCHEMA AND API REFERENCE INDEX

C.1 OATS Verifiable Credential Schemas

Credential Name	Issuer (DID Domain)	Defining Chapter
FarmFoundationalVC	Farmer / AgriStack	Ch 5 §5.3.3
OrganicCertificationCredential (NPOP/NOP/EU_Organic subtypes)	NPOP CB / USDA AMS / EU MS CB	Ch 18 §18.2.1
GIAuthorizedUserCredential; GIZoneVC	CGPDTM / INGRES GI Registry; OATS Standards Registry	Ch 18 §18.3
GAP_ProductionCredential (IFA v6 Smart); GAP_CoCCredential (CoC v6); GAP_MassBalanceAttestation	GLOBALG.A.P. CB; Operator + CB co-sign	Ch 18 §18.4.1
BCICredential; RainforestAllianceCredential; FairtradeCredential; SMETACredential; GRI13SourcingAttestation	BCI; RA CB; Fairtrade Int'l; Sedex auditor; Corporate + assurance provider	Ch 18 §18.6.1
PhytosanitaryCredential; MRLTestCredential; EUDRDueDiligenceCredential	PPQS/NPPO; NABL laboratory; Operator	Ch 18 §18.5.1; Ch 14
FSMA204_CTECredential; FSVP_SupplierCredential	Operator at CTE; US importer	Ch 17 §17.2; Ch 18 §18.5.1
TreatmentCredential; JASOrganicCredential; HalalCredential; ColdChainAttestation	PQ Officer; Japan CB; GSO-recognised body; Logistics operator	Ch 18 §18.5.1
BRCGSCredential; UKOrganicCredential; FSSAILicenceCredential; APEDARegistrationCredential; AGMARKCredential	UK BRCGS auditor; UK CB (UKCA); FSSAI FoSCoS; APEDA; DMI	Ch 18 §18.5.1
HACCPPlanVC; CAPAPlanVC	FBO + FSSAI counter-sign; Operator + FSSAI Designated Officer	Ch 19 §19.1.1; §19.7
WarehouseReceiptVC (eNWR-as-VC); CommercialInvoiceVC (with buyer co-sign)	WDRA-registered warehouse; Supplier + Buyer	Ch 21 §21.7; §21.3.1
PreExportVerificationCertificate (PEVC)	OATS Compliance Engine	Ch 3 §3.11

C.2 EPCIS Events and Critical Tracking Events (CTEs)

Event / CTE	Subject
CTE-01 Seed Sourcing	Seed origin and varietal
CTE-02 Sowing	Sowing declaration
CTE-03 Input Application	Fertiliser/pesticide; PHI start
CTE-04 Harvest	Harvest; LGTIN minting
CTE-05 First Aggregation	Farm-gate aggregation
CTE-06 Storage / Warehouse	Cold-chain/warehouse with IoT
CTE-07 Processing / Transformation	Processing; new LGTIN; mass-balance
CTE-08 Testing / Certification	Lab tests, certification VCs
CTE-09 Export Shipment	Export consignment, PEVC
CTE-10 Consumer Scan	Retail consumer QR scan (pseudonymous)
CertificationApplicationSubmitted / CertificationAuditEvent / CertificationIssuedEvent / CertificationSurveillanceEvent	Certification lifecycle entry/audit/issuance/surveillance
CertificationSuspendedEvent / CertificationRevokedEvent / CertificationRenewedEvent	Suspension / Revocation (with recall coupling) / Renewal
MassBalanceAnomalyEvent	Mass-balance breach
RecallAlertEvent (oats:RecallAlertEvent)	Recall trigger event
IntelligenceEvent (anomaly flag)	AI/ML detection
CorrectionEvent	Event correction per EPCIS 2.0 §6 error semantics

C.3 API Endpoints and Service Surfaces

Endpoint / Service	Function
queryLotHistory() (Fabric chaincode)	Forward/backward lot trace
OATS DID Resolver; OATS VC Verification API	DID resolution <500ms; VC validity + Status List 2021 <2s
OATS Provenance Query Service; OATS Event Bus / Kafka	Full chain verified <2s; EPCIS event streaming (10k events/sec/node)
OATS-Beckn Gateway (BPP); OATS GS1 Digital Link Resolver	Beckn protocol catalog + commerce;

	id.oats.gov.in/01/{GTIN}/10/{LGTIN}
OATS-TraceNet Adapter; OATS-FoSCoS Adapter (bidirectional); OATS-PQMS Adapter / ePhyto Hub	NPOP TC ↔ OATS VC <60s; FSSAI licence lifecycle sync; Phytosanitary VC integration
OATS GI Registry Adapter	CGPDTM batch sync; AU credential issuance
OATS RASFF Adapter; OATS FDA Adapter; OATS FSSAI FICS Adapter; OATS INFOSAN Adapter	EU iRASFF (bi-directional); FDA PREDICT / Reportable Food Registry; Domestic ↔ international alert routing; WHO/FAO routing
OATS DPP Generator; OATS Open Food Facts Publisher; OATS SmartLabel Adapter	CIRPASS + UNTP JSON-LD DPP <60s; OFF API v2 contribution; CBA SmartLabel JSON publication
Bhashini NMT/TTS/ASR APIs	22-language translation, voice
OATS Credit Scoring Service (CSS); OATS Supply Chain Finance Gateway (SCFG); OATS Milestone Settlement Chaincode	ACS 300–900 <10s; TReDS / ONDC Financial Services routing; 5-milestone escrow (Go/Node)
OATS DBT Eligibility Attestation API; OATS PMFBY Event Stream; OATS-WDRA / eNAM Adapter	<3s per query, bulk-attestation; Insurer consented subscription; eNWR-VC + pledge AssociationEvent
OATS Recall Management System (MOD-04); OATS HACCP Plan Registry (L4); OATS RCA Workbench (L5)	Parallel chain propagation; Digital HACCP plan VC; 5-Whys / Fishbone with crypto signing
OATS Consent Manager (CMS); Account Aggregator FIP Endpoint (Agricultural Activity Data)	DEPA v1.1 artefact lifecycle; New AA data type
OATS Information Mediator (X-Road v7); OATS Conformance Test Harness	Federated registry exchange; Third-party API contract validation

Department of Agriculture
Government of Maharashtra



THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

KWPF
Korea-World Bank Partnership Facility

AIAIC
AI and AgriTech Innovation Center
— AI for Every Acre —

TRST01
TRUST-TRANSPARENCY-TRACEABILITY