कृषी कल्याण कर्तव्यम्
कृषी विभाग, महाराष्ट्र शासन

सत्यमेव जयते

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

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.

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 and Ms. Arshia Gupta. 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 **modular reference architecture** from which any government, multilateral agency, or implementing consortium may select the modules relevant to its regulatory context, digital maturity, and agri-food value chains - from a single subnational pilot to a multi-country regional bloc. Each section has been deliberately designed for a distinct audience: policymakers and government sponsors; DPI architects and CTOs; procurement, legal, and compliance teams; system integrators and technical designers; regulators and standards bodies; implementation managers and delivery units; AgriTech vendors and integrators; and development finance institutions.

The publication strategy reflects this: each section is also released as a standalone digital module, enabling every stakeholder to access the section appropriate to their role. 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**. **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 integrate selected modules with existing infrastructure.

Every chapter is supported by a **Functional Requirement Specification (FRS)** defining what the system must do, and a **System Requirement Specification (SRS)** defining how it must be built - together forming the basis for procurement scope, vendor evaluation, and conformance testing (Appendix A). Every component is mapped 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 European Union, the United States, Brazil, and Australia**.

To navigate the Blueprint efficiently, readers should identify their profile from the eight on the following page and follow the **Audience-to-Chapter Map**, which lists the chapters relevant to each profile. Cross-references between chapters enable lateral navigation as the depth of engagement increases.

Audience-to-Chapter Map

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.

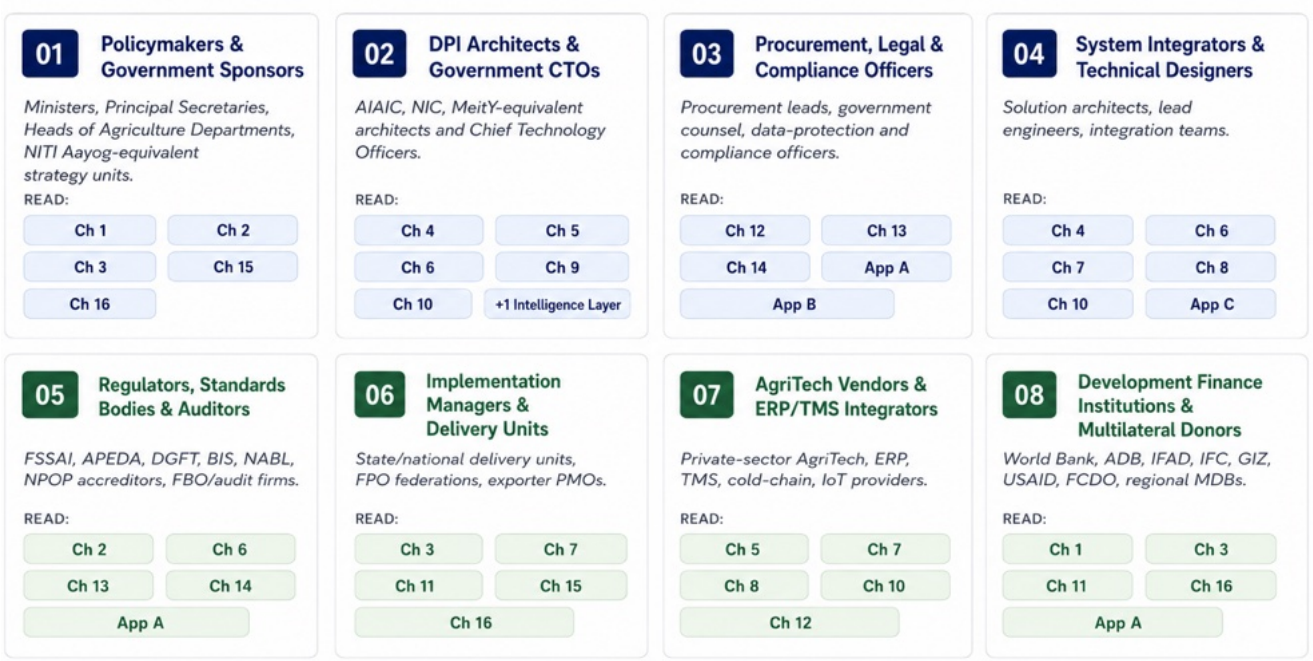


Table of Contents

Executive Summary

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 cost of unsafe food in low- and middle-income countries is estimated at **USD 110 billion annually** in lost productivity and medical expense (WHO–World Bank Technical Review, February 2025). At the same time, three regulatory currents - the European Union's Article 18 / EUDR / Digital Product Passport sequence, the United States' FSMA Section 204 24-hour rule, and the global generation of data-protection regimes are simultaneously making digital traceability mandatory for any jurisdiction that wishes to remain in the high-value export market.

For export-dependent agricultural economies, the cost of inaction is already visible. Two to eight percent of agricultural shipments are rejected or detained at EU ports, three to six percent at US ports, predominantly for traceability gaps and certificate-of-origin failures rather than product-quality defects. Resolving 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, with the same architectural shape as identity, payments, and data-exchange systems - foundational, multi-actor, cross-jurisdictional, and disproportionately valuable when built once, openly, rather than reinvented in every silo.

What OATS Is and What It Is Not

The **Open AgriTrace Stack (OATS)** is the reference architecture for that shared infrastructure. It is **jurisdiction-neutral, vendor-neutral, and technology-neutral**, published as a global public good under Creative Commons Attribution 4.0. It is a modular composition of specifications, frameworks, standards mappings, and implementation guidance from which any government, multilateral agency, or implementing consortium may select the modules relevant to its regulatory context, digital maturity, and value chains.

The architecture is mapped to authoritative global standards - GS1 EPCIS 2.0, ISO 22005:2007, Codex CAC/GL 60-2006, W3C Verifiable Credentials, FSMA 204, EU 178/2002, and DPDPA 2023 with illustrative implementation examples drawn from India, the European Union, the United States, Brazil, and Australia.

OATS is **not a product, not a platform, and not a single vendor's stack**. It can be adopted whole, adapted in part, or extended without seeking permission from any single steward.

Open Beats Proprietary at Scale

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; recall response averages five to six weeks; and switching vendors requires full data migration and re-integration.

DPI repositions foundational components - identifiers, registries, event exchange, consent management - as shared, open, public utilities, analogous to the internet, mobile telephony, and digital payment rails. Integration cost is socialised; interoperability is guaranteed by open protocol specifications; recall propagates across the network in hours rather than weeks; and any compliant application can read from and write to the shared layer.

Open does not preclude commercial participation, it disciplines it. Private-sector AgriTech, ERP, cold-chain, and IoT providers build value-added applications on top of open OATS APIs, competing on quality of service rather than on lock-in. Government builds and operates the core infrastructure layer; the private ecosystem builds the application layer above it.

Trust Is an Architectural Property

In a system where farmers, regulators, processors, retailers, and destination authorities must each verify claims made by counterparties they may never meet, trust cannot be a feature added later. OATS treats trust as a structural property of the architecture.

Every actor, location, lot, and certifier carries a globally unique, cryptographically resolvable identifier - anchored to authoritative national registries rather than maintained as a new identity silo. Every supply-chain event is captured in a single shared standard and digitally signed by the recording actor, so the record cannot be altered without detection. Certifications like organic, geographical indication, GLOBALG.A.P., phytosanitary, fair-trade - are issued as **Verifiable Credentials** rather than PDFs, machine-verifiable across jurisdictions without requiring access to the issuing authority's database.

Selective disclosure allows a farmer to prove EUDR-compliant geo-coordinates to a regulator without exposing them to a buyer, while a consumer scanning a product QR code can verify provenance directly against a sovereign-anchored record - without trusting the brand to be telling the truth. Compliance ceases to be a documentation exercise and becomes a property of correctly recorded operations.

The Smallholder at the Centre

A traceability system that excludes smallholders excludes the majority of the world's agricultural production. OATS treats inclusion as an architectural constraint, not an aspirational outcome. Feature phones, USSD, offline-first capture, and vernacular voice interfaces are first-class participants in the system. Onboarding for smallholder farmers and Farmer Producer Organisations is **free at the point of use**.

The cost of compliance attestation, premium provenance issuance, and certification anchoring is borne by the parties that capture commercial value from the verified record - importers, brand owners, customs authorities, and retailers operating under a Traceability-as-a-Service model.

The financial dimension is equally consequential. A smallholder's verified history of seeding dates, declared area, input usage, yield, lots sold, price received, and warehouse tonnage becomes **collateral-grade evidence** for digital credit scoring, supply-chain finance, parametric crop insurance, and warehouse-receipt finance closing the structural gap in formal agricultural credit that has persisted despite near-universal bank-account access in many low- and middle-income jurisdictions.

Compliance by Architecture

In a fragmented system, the EU's Article 18 / EUDR / Digital Product Passport sequence, the US FSMA Section 204 rule, and global data-protection regimes would each require separate parallel submissions, separate audit trails, and separate documentation streams.

OATS collapses these into a single canonical event chain from which destination-country submissions are **auto-derived**. EU due-diligence statements, FSMA 204 sortable spreadsheets, geographical-indication attestations, phytosanitary credentials, and organic transaction certificates are all generated from the same underlying event record. The architectural principle is that compliance evidence should be a query against the event store, not a parallel data-entry task.

The same architecture delivers sovereign data governance: data remains at source nodes, references rather than copies move across jurisdictional boundaries, and consent is enforced as a system-level control rather than as an application-level feature. Personal data of farmers does not cross borders unless explicitly authorised under a recognised legal instrument; consent can be withdrawn at any time, through any channel the farmer can use.

Three Paths to Adoption

The Blueprint is presented as both a normative reference and an implementation toolkit. The normative side specifies the architecture, design principles, governance values, and conformance levels that define an OATS-conformant traceability DPI. The implementation side provides operational guidance, procurement scaffolding, and standards mappings that enable deployment.

Three deployment frameworks are supported, all converging on the same shared protocol layer:

- **Greenfield National Deployment**: a complete stack deployed by a sovereign or sub-sovereign government with no incumbent traceability infrastructure.
- **Brownfield Augmentation**: selected modules integrate with existing national systems, sector regulators, and enterprise platforms; OATS rides on top of incumbent investments without replacing them.
- **Sectoral Vertical**: a single commodity (cotton, soybean, coffee, shrimp, spice) deployed against a specific regulatory anchor (EUDR, BCI, GDST, NPOP, or equivalent). The same Blueprint serves a single-state pilot and a multi-country regional bloc.

Every chapter is supported by a Functional and System Requirement Specification designed to be procurement-ready and conformance-testable. Three conformance tiers - Core, Standard, and Advanced - allow jurisdictions to enter at the level of digital maturity available to them today and progress as capability grows.

An Invitation to the Field

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.

1. Vision, Mission, and Strategic Framework

1.1 Definitions

The Blueprint adopts the following authoritative definitions, used consistently across all chapters. Where a definition is sourced from an external standard, the citation is provided.

Term	Definition	Authoritative Source
Traceability	The ability to follow the movement of a food through specified stage(s) of production, processing, and distribution. Encompasses tracing of food, feed, food-producing animals, or substances intended to be incorporated into food or feed, through all stages of production, processing, and distribution.	ISO 22005:2007 (Clause 3.8); Codex CAC/GL 60-2006[1]
Digital Public Infrastructure (DPI)	Systems that serve as foundational, digital building blocks for public benefit. DPI may comprise software, platforms, APIs, services, and the related legal, regulatory, and governance frameworks, standards, policies, and processes. *"Public" denotes public benefit, not government ownership.*	World Bank, Digital Transformation White Paper (2025)[2]
Open Stack	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 underlying technology choices.	OATS contextual definition (derived from DPGA, CDPI, GovStack, OSI)
India Enterprise Architecture (InDEA 2.0)	A generic, federated architecture framework based on TOGAF, comprising reference models that may be configured into a Whole-of-Government Architecture. Emphasises a value-driven approach, capability building, and a preference for enabling rather than building.	NeGD / MeitY (2023)[3]
Critical Tracking Event (CTE)	A specific point in the supply chain at which traceability data must be captured — harvesting, packing, shipping, receiving, transformation. CTEs are the operational units of traceability, mandated under FSMA Section 204 (USA) and mapped to GS1 EPCIS 2.0 event types.	GS1 GTS 2.0; FDA Food Traceability Final Rule (87 FR 70910)[4]
Key Data Element (KDE)	A specific piece of information that must be recorded at each Critical Tracking Event — identifiers, dates, quantities, reference documents. The specific KDEs required vary by CTE and regulatory jurisdiction.	GS1 GTS 2.0; FSMA 204; EU Regulation 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 laws and standards, and do no harm by design.	Digital Public Goods Alliance
Verifiable Credential (VC)	A tamper-evident, cryptographically verifiable digital representation of claims made by an issuer about a subject. In OATS, VCs represent certifications, compliance attestations, and chain-of-custody proofs, enabling portable, cross-platform trust without a central verification authority.	W3C VC Data Model 2.0[5]

[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

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

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

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

Data Fiduciary	Under India's DPDPA 2023, any person who, alone or in conjunction with others, 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. Equivalent concept under GDPR: Data Controller.	DPDPA 2023; GDPR Article 4(7) [6]

Three Operational Planes of Traceability

Implementation of any traceability DPI must address three nested planes:

- **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.

1.2 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[7]:

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 low- and middle-income economies an estimated USD 110 billion annually in lost productivity and medical expense (joint WHO–World Bank Technical Review, February 2025). Recall costs alone exceed USD 7 billion per year in the United States; the European Parliament places EU food fraud at EUR 30–40 billion annually.

Trade and market-access dimension:

Three concurrent regulatory movements drive global traceability convergence:

- European Union - Regulation (EC) 178/2002 Article 18 mandates one-up-one-down traceability for all food businesses operating in or exporting to the EU. The Farm-to-Fork Strategy (2020), the EUDR (Regulation (EU) 2023/1115), and the forthcoming Digital Product Passport under ESPR (Regulation (EU) 2024/1781) progressively intensify these obligations.

[6] 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

[7] WHO GERG 2025 Baseline

- United States - FSMA Section 204 (FDA Food Traceability Final Rule, 87 FR 70910) mandates electronic lot-level traceability records for foods on the Food Traceability List, with FDA authorised to demand records within 24 hours.
- Emerging global frameworks - Japan's Food Labelling Act, Australia's National Livestock Identification System, Canada's Safe Food for Canadians Act, and 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 is the most effective systemic deterrent against high-value-category fraud - organic, geographical indication, and premium-origin claims being the most-exploited categories.

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 five to six weeks; smallholders are excluded by cost and complexity.

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 and numbering), and payment rails (shared clearing). The contrast is structural, not incremental.

Proprietary Platforms	DPI (OATS)
Each participant pays individually for integration.	Integration cost is socialised — built once, used by all.
Interoperability requires bilateral negotiation and custom code.	Interoperability is guaranteed by open protocol specifications.
Recall response depends on voluntary data sharing by competitors.	Recall accesses a common event ledger in hours, not weeks.
Smallholders are excluded by cost and technical complexity.	Smallholders participate via low-cost, offline-capable interfaces.
Data sovereignty rests with the platform operator.	Data sovereignty rests with the data principal; consent is sovereign.
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.	Innovation is permissionless; anyone may build on open protocols.
Audit trails are controlled and editable by the platform operator.	Audit trails are immutable, timestamped, and cryptographically verifiable.
Licence fees and per-transaction charges compound over time.	Marginal cost of participation approaches zero as the network scales.

This is the architectural case for traceability as DPI. The remainder of this Blueprint operationalises that case.

1.4 The OATS Design Philosophy: Open, Federated, Sovereign

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, the Centre for Digital Public Infrastructure (CDPI), InDEA 2.0, OECD and Government Digital Service (GDS) principles, DPDPA 2023, the Global Food Traceability Centre (GFTC), and ISO 22005:2007 with Codex CAC/GL 60-2006. These are codified into the **20 OATS P-Principles** organised in four categories (Chapter 2), each translated into an enforceable design rule and an explicit anti-pattern. The five tenets summarise the design intent:

Tenet	Architectural Commitment	What It Rules Out
Open by Default	Every interface specification, data model, API contract, and governance rule is publicly available, royalty-free, and implementable by any party.	No proprietary identifier, schema, or protocol at any registry layer.

Federated by Architecture	Data is generated and retained at source; OATS Core stores routing, identifiers, and access-control lists only. Each jurisdiction operates its own node.	No centralised national database; no single jurisdiction can disrupt another.
Sovereign by Design	Personal, commercial, and strategic data remain under the relevant sovereign's jurisdiction. The Data Principal is always at the centre; consent rests in human hands.	No silent cross-border bulk transfer; no platform-side override of consent.
Inclusive by Architecture	Offline-first operation; vernacular voice, USSD, and multilingual interfaces; zero participation cost for smallholders at the point of use.	No English-only interfaces; no smartphone-only onboarding; no fee to be traced.
Trustworthy by Construction	Trust is layered: identity (cryptographically verified actors), event integrity (timestamped, signed events), claim verifiability (W3C VCs), and audit transparency (immutable audit logs).	No editable audit trails; no PDF-based certifications that cannot be machine-verified.

1.5 Strategic Alignment with Global Frameworks

OATS is structurally consistent with the established normative anchors of the global development and food-safety ecosystem.

- **Sustainable Development Goals.** OATS contributes primarily to six SDGs — SDG 1 (No Poverty), SDG 2 (Zero Hunger), SDG 3 (Good Health and Well-Being), SDG 8 (Decent Work and Economic Growth), SDG 12 (Responsible Consumption and Production), and SDG 17 (Partnerships for the Goals).
- **G20 DPI Consensus Principles (August 2023).** OATS is structurally aligned with the eight DPI 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, and Grievance Redressal.
- **Codex Alimentarius and the 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 Agreement on the Application of Sanitary and Phytosanitary Measures (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.

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 choices that appear reasonable in isolation but systematically violate OATS principles. The OATS governance council and procurement teams must explicitly identify and reject these 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 the 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 (Data Minimisation). **Correct:** Collect only the minimum data required for entity identification.
“Centralised all-data repository” - routing all supply-chain event data through a central government database.	Violates P-2 (Federated), P-11 (Data Sovereignty). **Correct:** Implement a data mesh with federated storage and central metadata only.
“Excel-based KDE collection” - collecting KDEs as spreadsheet submissions without a structured event schema.	Violates P-15 (Event-Based). **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 operational food-safety utility.	Violates P-14 (End-to-End), P-17 (Verifiable). **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). **Correct:** All farmer-facing interfaces must support vernacular languages and voice.

3. Stakeholder Ecosystem and Actor Mapping

3.1 Introduction and Actor Classification Framework

OATS operates as a multi-stakeholder ecosystem in which eight tiers of actors interact under a shared governance framework. Each tier carries a distinct architectural function. The classification below is normative for any OATS-conformant deployment.

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)	Accountability, innovation, and public benefit verification actors: independent monitors of OATS outcomes

Government as Sovereign Architect: Government occupies a uniquely central role across four dimensions that no private actor can perform: **Primary Financier** for the shared infrastructure layer; **Sovereign Architect** providing legal mandate, conformance standards, and 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; and **DPI Steward**, ensuring long-term sustainability and governance beyond any commercial investment cycle.

Supply-chain actors (Tiers 2–4): Farmers and FPOs are the first-mile originators of every traceability record. They register through national digital identity at zero cost and capture harvest events through accessible interfaces — basic mobile apps, USSD on feature phones, and vernacular voice. **Across the farmer tier, 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 occupy the most technically demanding position, responsible for recording every transformation (sorting, grading, drying, milling, packaging, blending) with complete input-output fidelity. Logistics actors — transporters, cold-chain operators, accredited warehouses, ports - safeguard custody continuity and environmental integrity through to the final domestic node.

Regulators (Tier 5) and the application ecosystem (Tier 6): Regulatory and standards bodies define the compliance rules within which OATS operates and issue the certifications that give OATS data legal standing at ports of entry. Their engagement is bidirectional: they consume OATS event data for risk-based decisions and produce certification data as OATS Verifiable Credentials. Technology providers - system integrators, application developers, IoT vendors — build value-added products on top of open OATS APIs. The foundational principle, derived from InDEA 2.0's "enabling rather than building" orientation, is that **government builds the core infrastructure layer while the private AgriTech ecosystem builds the application layer above it** - preventing crowding-out and keeping the infrastructure layer strictly technology-neutral.

Capital mobilisers and accountability actors (Tiers 7–8): Development Finance Institutions and multilateral donors are critical in early-stage deployment, when the public-goods nature of traceability DPI and the long gestation period before commercial returns materialise make purely commercial financing insufficient. Civil society, academic, and consumer organisations perform the accountability, independent research, and public-benefit verification functions that neither government nor industry can perform for itself.

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

The central problem OATS solves is export-consignment rejection at destination ports. A single rejected container represents USD 50,000–500,000 in lost revenue, plus demurrage, return freight, reputational damage, and potential loss of export-body registration. The root cause in most 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 through the **Pre-Export Verification Certificate (PEVC)** — a pre-verified, digitally signed, cryptographically tamper-evident composite traceability record that destination authorities can verify in seconds rather than days. The PEVC is the terminal credential in a chained-issuance trust graph that runs the full length of the supply chain: every credential cryptographically references its parent, producing a single verifiable graph rather than a bundle of parallel documents.

The Six-Stage Pre-Export Verification Workflow

Six actors are involved: 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 Authority (verifies and decides).

Stage	Responsible Actor(s)	OATS Mechanism and Output
1. Continuous chain-of-custody capture (farm to port staging)	All supply-chain actors	Real-time EPCIS 2.0 event capture at every CTE — harvest, processing, grading, cold storage, port staging. Every event cryptographically signed, hash-linked, and immutable.
2. Pre-export KDE completeness check (72 h before loading)	Agriculture Department OATS Delivery Unit (automated API)	Automated check against the destination-country KDE profile. Computes an OATS Completeness Score (0–100); flags deficiencies to the exporter with specific remediation guidance.
3. FSSAI pre-export physical inspection and NOC issuance	Food Safety Authority (Authorised Officer)	Risk-profile-based inspection (high Completeness Score may qualify for documentation-only review). NOC issued as a W3C Verifiable Credential, digitally signed, anchored to the OATS Master Lot ID.
4. Export Promotion Body certifications (parallel streams)	DPPQS (phytosanitary) + APEDA / Commodity Board (Health Certificate, Certificate of Origin, Organic, GI, NABL lab reports)	Each certification issued as a W3C Verifiable Credential cryptographically linked to the OATS Master Lot ID. Both streams must complete before PEVC assembly.
5. OATS PEVC automated assembly and digital signing	OATS Platform (Agriculture Department–operated)	OATS assembles all VCs — FSSAI NOC, APEDA certificates, cold-chain attestation, lab results — into the PEVC, signed by the Agriculture Department as sovereign DPI operator, and rendered as a QR code embedded in the Shipping Bill.
6. Destination-country electronic verification	Destination Regulatory Authority (EU TRACES NT, US FDA PREDICT, equivalent)	Destination authority verifies via the PEVC QR or the OATS Verification API. OATS-verified consignments above the threshold are directed to Green Channel. Outcome: clearance within 4 h vs. the standard 72-h baseline.

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 on the terminal PEVC; and the OATS event ledger's non-repudiable, hash-linked, timestamped record of every event in the chain. The trust chain is **intrinsic to the document structure**, not gateway-mediated - which also enables financial-services composability for invoice financing, trade credit, and warehouse-receipt finance applications.

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

The **OATS Multi-Stakeholder Governance Council (OMGC)** is 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;
- Allocation of the OATS Innovation 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 is a design prerequisite, not a communications activity. Research on digital traceability systems consistently identifies stakeholder resistance - particularly from smallholder farmers facing data-capture burden without visible short-term benefit, and from SME processors perceiving compliance costs exceeding benefits — as the primary cause of system failure after technically successful deployment. OATS engagement is structured around three implementation phases:

Phase	Timeframe and Focus	Key Activities
Phase 1 - Foundation and Co-Design	Months –18 to –6 (18 months pre-launch)	Government convenes the OMGC founding session; establishes the Delivery Unit; secures multi-year OATS budget; issues legal mandate with 24-month implementation grace period. Ethnographic user research with farmer cohorts in three priority commodity corridors; vernacular co-design of farmer registration flows; pilot with 5–10 self-selected FPOs. OATS API specifications published 12 months ahead of compliance deadline; OATS Vendor Registry populated. DFI partners conduct OATS DPI Readiness Assessment.
Phase 2 — Pilot and Validation	Months 0 to +12 (first deployment year)	OATS-Core deployed in 1–2 priority export corridors. FSSAI integrates FICS with the OATS PEVC API; trains Authorised Officers on PEVC verification. 50–100 exporters enrolled and issued first PEVCs; export-rejection-rate change measured. 10,000–50,000 farmers enrolled; satisfaction surveyed at 3 and 6 months; top five friction points remediated. Civil society publishes the OATS Public Performance Dashboard and launches the OATS Fraud Reporting Portal.
Phase 3 — Scale and Institutionalisation	Months +12 to +60 (years 2–5)	OATS-Standard rolled out across additional commodity corridors. Bilateral destination-country systems (EU TRACES, US FDA PREDICT) integrated. PEVC extended to all APEDA-registered commodity categories. Open OATS Innovation Challenge for Fund allocation. OATS Open Research Programme grants published.

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 a cotton-bale custody transfer uses the same Traceability chaincode, 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:

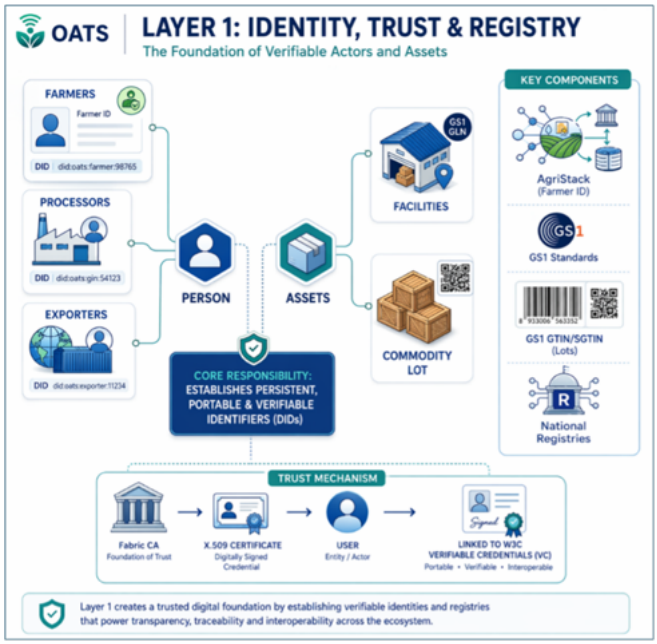
- **Blockchain** provides tamper-evident anchoring for identity credentials, event hashes, consent artefacts, and compliance evidence.
- **Beckn-derived protocols** operate as the open decentralised commerce and traceability discovery network. OATS introduces the **Beckn Network Adapter** as the architectural bridge, translating each Beckn commerce transaction into the corresponding EPCIS 2.0 event so that commerce and traceability are recorded as a single atomic action with no double data entry.
- **GS1 EPCIS 2.0 (ISO/IEC 19987:2024)** is the universal event grammar.

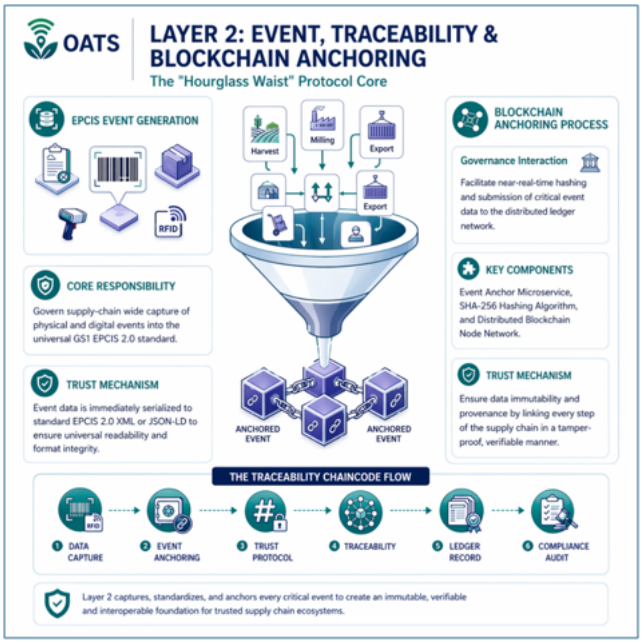
4.2 Master Overview: The OATS 5+1 Layer stack

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 integration role of Hyperledger Fabric and Beckn Protocol.

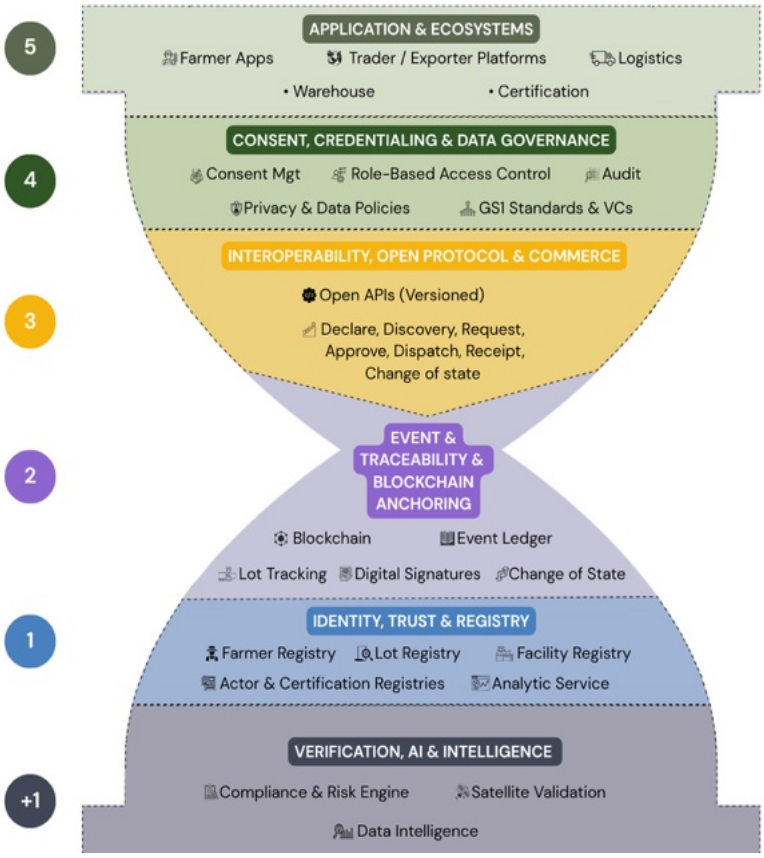
Layer	Name	Core Responsibility	Key Building Blocks	Hyperledger Fabric & Beckn Role
L1	Identity, Trust & Registry	Establishes persistent, portable, verifiable identifiers for every participant and asset across the agri chain; maintains authoritative entity registries; enforces zero-trust access control and DPDPA 2023 consent at the network perimeter.	AgriStack DID; MOSIP (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 the 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).
L3	Interoperability, Open Protocol & Commerce	Defines how systems interact across organisations and jurisdictions for all agri-commodity sectors; implements Beckn Protocol as the open decentralised commerce and traceability discovery network; standardises 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; W3C VC 2.0 Issuance; Selective Disclosure; RBAC Audit Trail; Commodity Certification VC Registry.	VC hashes and revocation events anchored on the 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 that no single application or vendor monopolises the ecosystem across any commodity sector.	Consumer / Trade Transparency Portal; Export Compliance (APEDA); ONDC / APMCs; Commodity Recall Management; Regulatory Dashboards; MahaVISTAAR; State Data Exchanges (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 the governance-channel; deforestation risk models consume satellite data and anchor compliance-attestation hashes on the export-channel.





4.3 The Hourglass Protocol Model



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. Standardised 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 and data policies, GS1 standards, Verifiable Credentials, and audit mechanisms.
- **Layer 5 -** Applications & Ecosystems. Diverse and competitive application layer across commodity sectors — farmer apps, trader / exporter platforms, logistics, warehousing, certification systems, and sector-specific solutions.

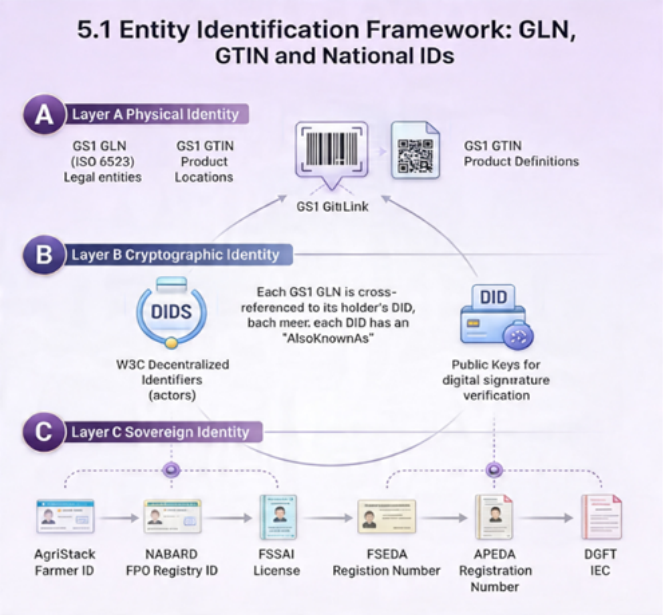
5. Identity, Trust, Registry and Credentialing Standards

A strong agricultural digital ecosystem needs a standardised way to identify supply-chain actors - farmers, organisations, processors, logistics providers, exporters, laboratories, certification bodies, and government authorities. OATS uses GS1's GLN and GTIN for entity and product identification, W3C Decentralized Identifiers for self-managed cryptographic identity, and Verifiable Credentials for portable proof of certification and compliance. Integration with national databases such as AgriStack anchors authenticity and connects OATS to government services, providing a scalable foundation for onboarding, identity validation, and traceability across the value chain.

5.1 Entity Identification Framework: GLN, GTIN and National IDs

Every entity in OATS - farmer, FPO, processor, exporter, warehouse, laboratory, certification body, government authority - must carry a globally unique, persistent, standards-based identifier. The integrity of every traceability event recorded on the immutable event ledger depends on unambiguous resolution of every actor and location referenced. 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 recognised national government identifier that maps to one of these two anchor systems.



The Three-Layer Identifier Taxonomy

Layer	Identifier Type	Purpose
Physical Identity	GS1 GLN (ISO 6523) for legal entities and physical locations; GS1 GTIN for product definitions; SGTIN for serialised lots.	Globally unique, commercially recognised; enables interoperability with any GS1-compliant supply-chain system worldwide; encoded in GS1 barcodes and GS1 Digital Link QR codes at the consumer endpoint.
Cryptographic Identity	W3C Decentralized Identifiers (DIDs) for every OATS-registered actor.	Carry public keys for digital signature verification on events anchored to immutable event ledger and for VC issuance & presentation, independent of central authority.
Sovereign Identity	National government identifiers: AgriStack Farmer ID, FSSAI License Number, APEDA Registration Number, DGFT IEC.	Anchor OATS entities within their regulatory jurisdiction; 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 carries an alsoKnownAs reference to the relevant sovereign identifier; and each sovereign identifier is verified against its authoritative national registry at enrolment and kept current through publish-subscribe synchronisation. All three must be present for an entity to participate fully in OATS event recording and PEVC issuance.

GS1 GLN, GTIN, and SGTIN

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 organisational anchor that makes event records interpretable and verifiable across jurisdictions and systems.

The **GS1 GTIN** is the standard identifier for all OATS-registered agricultural products in the Product Registry, defining product variety, grade, packaging, and certification. Each registered product must have a valid GS1 GTIN from GS1 India. The **SGTIN** adds serialisation 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.

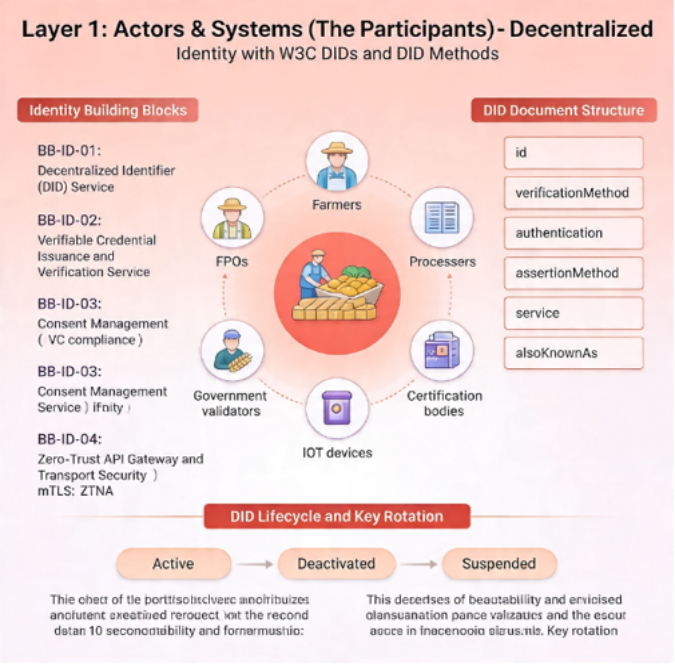
National Identity System Integration

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 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.

5.2 Decentralized identity: W3C DIDs and DID Methods

Layer 1 enables three capabilities: **authenticated identification** of all participants (farmers, FPOs, processors, exporters, government validators, IoT devices, certification bodies) using standards-based decentralised identifiers; **issuance and verification of cryptographically secure credentials** proving compliance or certification status without relying on a centralised authority; and **consent management** aligned with DPDPA 2023, ensuring 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 — 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

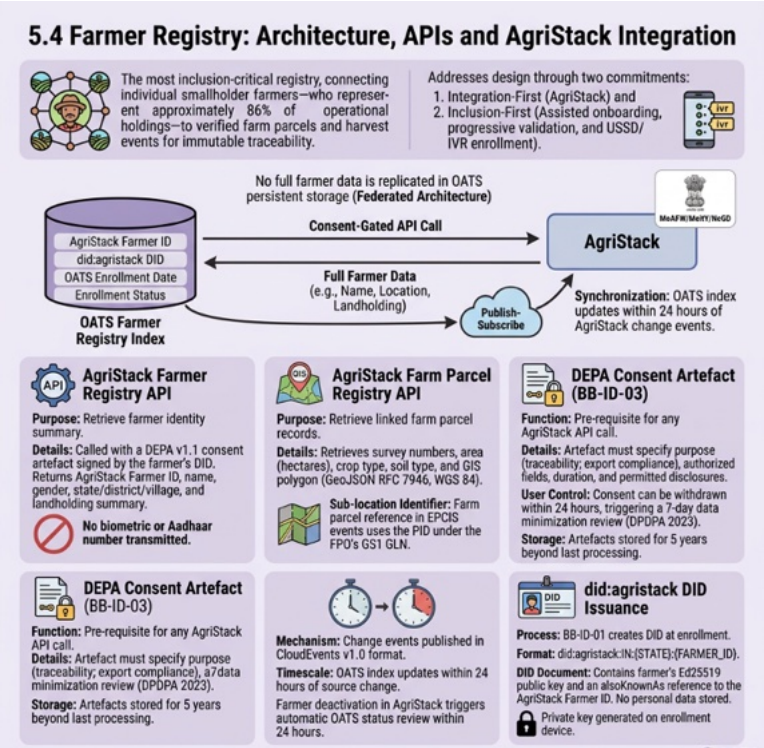
Verifiable Credentials (VCs) form the full trust-chain layer within the OATS ecosystem, covering identity assertions, foundational farm credentials, lot declarations, regulatory certifications, commercial transactions, and the terminal Pre-Export Verification Certificate. Each VC is a digitally signed claim issued by an authorised authority — 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 recognised certification bodies and regulatory authorities — FSSAI, APEDA, NABL-accredited labs, NPOP-accredited organic certifiers, plant quarantine agencies — each operating through their own signing infrastructure linked to a registered DID-OATS issuer identity. The full credential data remains with the issuing authority, while the OATS Certification Registry stores only minimal metadata: credential hash, issuer DID, subject identifier, credential type, issuance date, and current status (valid, suspended, or revoked). This architecture avoids centralising sensitive audit data while 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 — issuance, renewal, 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 W3C Status List 2021 bitstrings rather than querying the ledger, allowing high-frequency validation without impacting system performance.

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 of all operational holdings are below two hectares** (Agriculture Census, MoA&FW). 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.



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 operationalise OATS Principle P-18 (Inclusive by Architecture) and InDEA 2.0 Consent-Based Data Sharing at the first-mile level.

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 - AgriStack Farmer ID, OATS enrolment date, 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-minimisation requirements.

5.5 Business and Facility Registry

Aligned with the InDEA 2.0 Registry as a Service pattern, the Business and Facility Registry is exposed through standardised APIs, allowing any authorised system to validate entity identity and status without duplicating data. A unified registry approach enables real-time verification of registration, licensing, and certification status through a single API call, while higher layers reference entities by their identifiers rather than duplicating information. This addresses the issue of isolated certification silos where multiple agencies maintain disconnected and inconsistent records.

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 authorised Certification Body.

5.6 Product and Commodity Registry

The Product and Commodity Registry is a core Layer 1 component providing canonical definitions for all agricultural products and food commodities traceable within OATS — species and variety, quality grade, applicable certification schemes, destination-country regulatory requirements, and associated GS1 GTIN. The registry functions as the authoritative master-data layer against which all lot-level traceability events are validated at the point of data capture, enabling a **compliance-by-design** approach. It is also a critical input to the **PEVC Compliance Engine**, which uses these definitions to determine the mandatory credential and compliance requirements for each product–destination combination.

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 authorised Certification Body, confirming production within the registered geographic area by an authorised user; the cryptographic hash of this VC issuance event is anchored on the immutable event ledger.

5.7 Certification and Accreditation Registry

The Certification and Accreditation Registry is the compliance-intelligence layer within OATS Layer 1, maintaining real-time status of all certifications associated with registered entities. In line with privacy-by-design principles, the registry stores only essential metadata: VC hash, issuer 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 centralising sensitive audit reports or proprietary certification data.

The OATS immutable event ledger anchors the cryptographic hash of each certification lifecycle event — issuance, renewal, revocation — as a timestamped, 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.

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 characterises 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-recognised Halal Certification Bodies accepted by GCC importing-country authorities. OATS supports multiple recognised Halal bodies whose certifications are accepted by UAE, Saudi Arabia, and other GCC markets.
ISO/IEC 17065	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.

Certification Status Model

Every certification record in the OATS Certification Registry exists in one of four states:

- **Active** - the credential is valid and all revocation checks are passing.
- **Warning** - 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** - a 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** - 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

OATS operates as an identity federation node, not as a sovereign identity issuer. Three federation contexts apply:

- **India-Specific Federation** — AgriStack Farmer Registry is the foundational anchor; OATS federates with the FSSAI FBO Registry, the APEDA Registry, the WDRA accreditation registry, the NABL accreditation registry, and the NIC GI Cloud. Central and state identity systems are both supported through state-level OATS Identity Resolvers maintaining a unified identity framework across central and state levels.

- **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.

- **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: 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 DPDPA 2023.

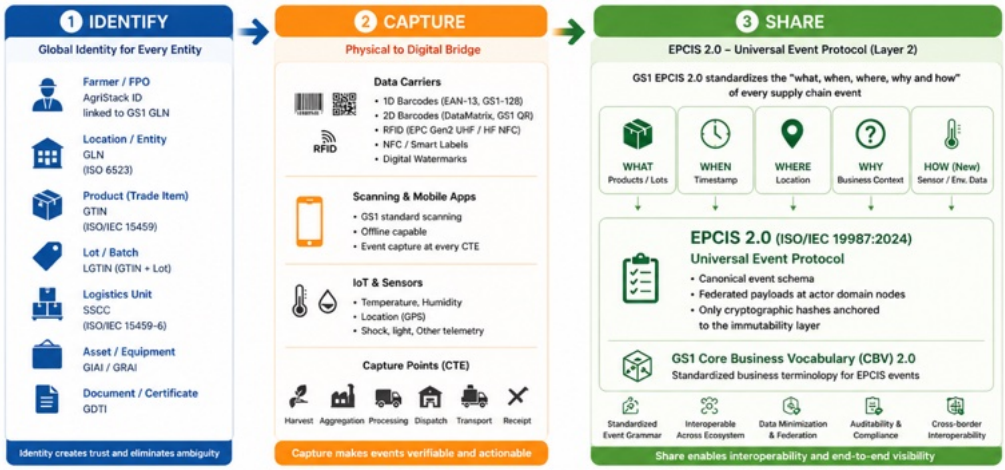
6. Traceability Event Data Model and EPCIS2.0 Implementation

This chapter sets the technical basis for OATS 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 such as FDA FSMA Section 204 CTEs and EU Regulation 178/2002 Article 18 traceability rules, and specifies the essential 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 2. 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, 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** - WHAT, WHEN, WHERE, WHY, HOW. 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 2 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.

CTE#	CTE Name	EPCIS Event Type	Key Identifiers	Triggered by
CTE-01	Seed / Sampling Procurement	ObjectEvent (ADD)	Seed Lot ID, Farmer ID, Dealer ID	Dealer sale; nursery purchase; 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, 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.

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
	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 Name and CIBRC Registration Number	Alphanumeric	CIBRC registered products list (India)

	Active Ingredient and Concentration	Text and numeric	CIBRC label; 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)	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
	Crop Variety Confirmation at Harvest (GI-relevant)	Alphanumeric	Farmer or FPO agent declaration; APEDA for export crops
	Post-Harvest Handling Method	Categorical + 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	OATS TransformationEvent input EPC list
	Output Lot IDs and Quantities (Mass Balance)	Structured list	OATS TransformationEvent output EPC list
	Processing Parameters (Commodity-Specific)	Numeric (various units)	Processor QC system
	Cold Chain Records (Temp / 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	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; 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 mapping 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, 02, 03, 04, 06, 08, 09, 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 the 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. **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** carries arrays of sensor Metadata (device ID, calibration reference) and sensor Report (type, value, uom, time, min/max/mean). OATS ingests IoT sensor data through two open standards: **FIWARE NGSI-LD v1.6** for context-broker-based deployments and **OGC SensorThings API v1.1** for OGC-conformant IoT deployments. Both formats are translated by the OATS IoT Gateway into EPCIS 2.0 sensor Element List payloads. **Association Event for Physical-Digital Sensor Linkage:** every IoT device is registered as an entity with a GIAI device identifier; at deployment to a container, cold store, or vehicle, an Association Event binds the device DID to the relevant lot or SSCC, establishing non-repudiable physical-digital 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.

6.6 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 (a 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.

6.7 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. 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 requirement in practice. OATS satisfies it by combining the EPCIS event store (Apache Kafka 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.

6.8 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 food businesses regardless of size or product category. **EPCIS Event Chain as Article 18 Compliance Mechanism:** Traceability is fully satisfied by the OATS EPCIS event chain — each Transaction Event and Association Event records the upstream supplier (source party DID) and the downstream recipient (destination party DID), with cryptographic linkage to the lot identifiers.

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; and 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 Chapter 5); 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 addresses 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 standardised data carriers — QR codes, DataMatrix, RFID, and NFC — globally unique, web-resolvable identifiers using GS1 Digital Link, and IoT-based environmental monitoring integrated via FIWARE NGSI-LD and OGC SensorThings API. The chapter is positioned within the context of the global transition to next-generation identification systems, particularly the GS1 Sunrise 2027 shift from one-dimensional barcodes to 2D Digital Link–enabled carriers.

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. Four internationally standardised 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 Principles P-1 (Open by Default) and P-2 (Federated by Architecture).

The common technical thread across all four carrier technologies is that each must encode, or resolve to, a GS1 Digital Link URI. 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.

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, DataMatrix, 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.

A GS1 Digital Link URL is a standard HTTPS URL that follows a canonical syntax combining GS1 identifiers expressed as URL path components. The minimum viable Digital Link URI encodes only the Global Trade Item Number (GTIN); extended forms add the Lot Number, Serial Number, Expiry Date, and other GS1 Application Identifiers. The resolver at the domain portion of the URI returns a list of available links — product information, instructions, traceability data, regulatory documents, marketing content — from which the requesting device can select the appropriate response based on context.

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.**

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 standardised lot-number encoding.	GS1 Digital Link QR code on every outbound carton and consumer pack; GTIN + Lot + Expiry + Serial 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 the OATS resolver directly from the SSCC on the Customs Import Declaration.
Consumer	Fragmented brand-specific QR codes; no standardised 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 VC-backed and legally admissible.

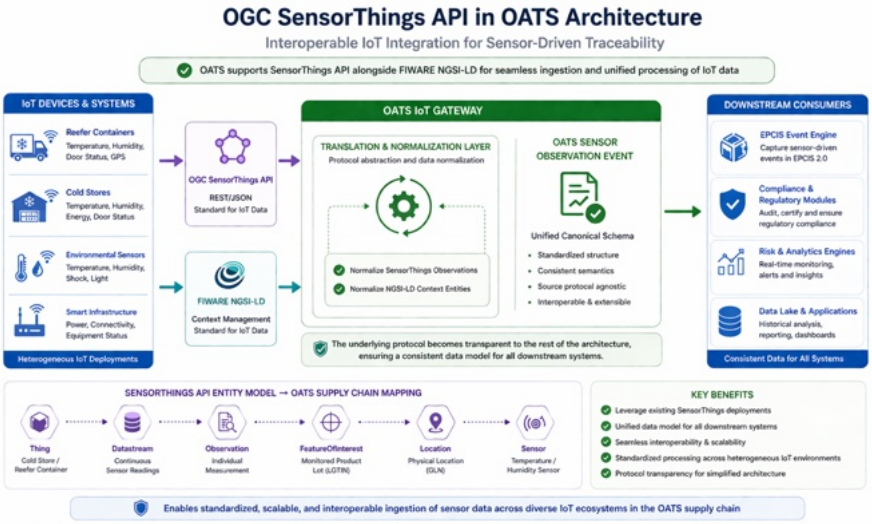
7.4 RFID and EPC Gen2 for Automated Bulk Identification

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 (Chapter 6 §6.5). 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.

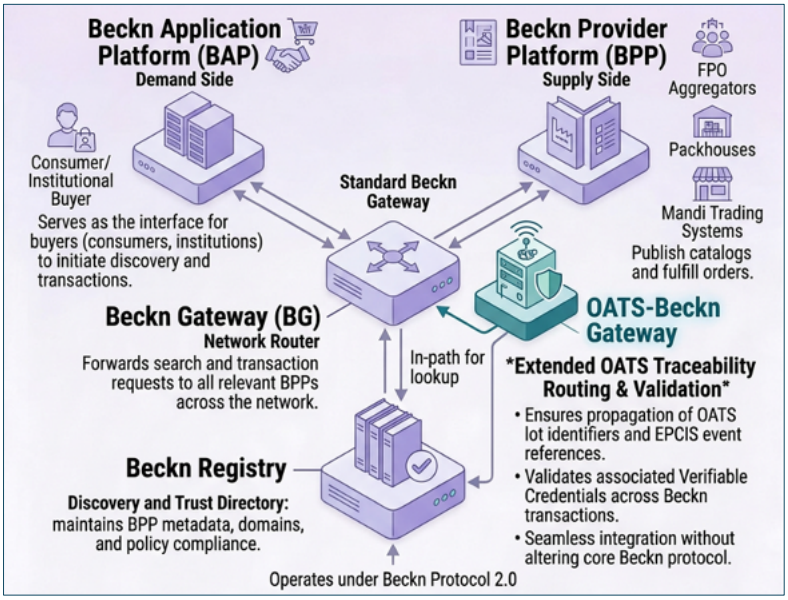
Requesting Actor	Authentication Method	Resolver Response Content
Consumer	None	Product provenance summary, certifications, cold chain status, recall flag
Supply Chain Actor	DID + OAuth / mTLS	Provenance plus role-specific commercial data
Regulatory Authority	Gov DID + mTLS	Full EPCIS event chain, KDEs, 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.

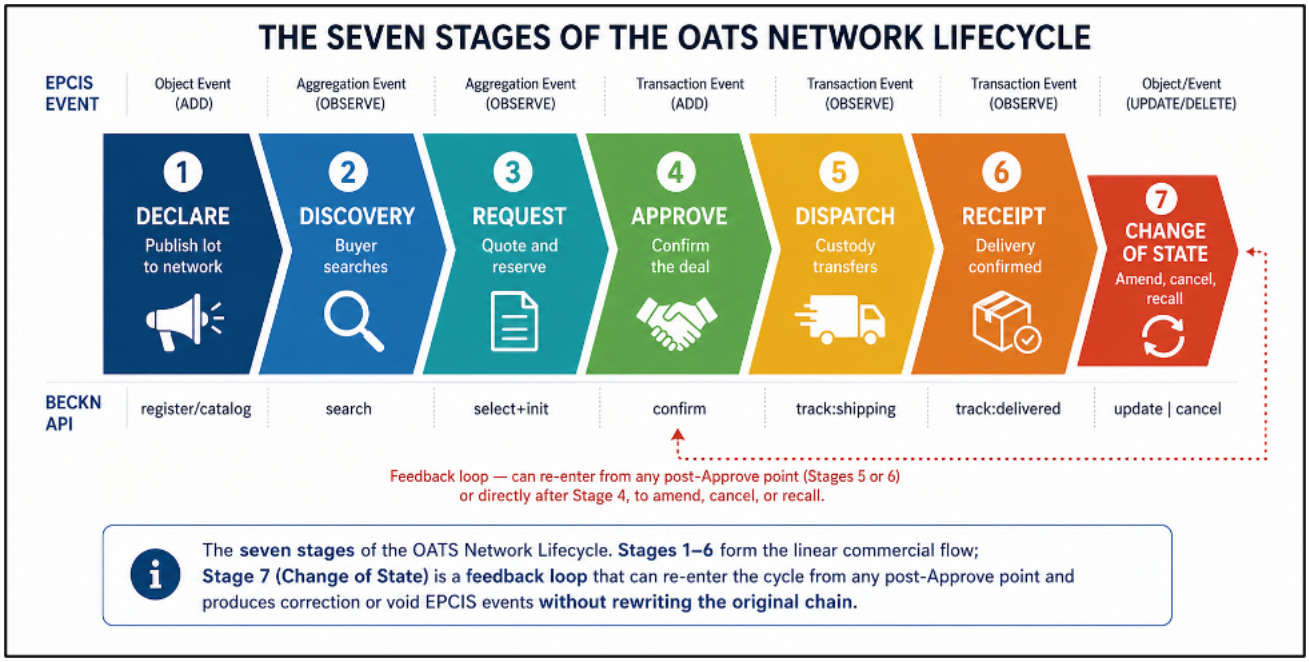
What the OATS Protocol Inherits from Beckn. The four actor model (BAP, BPP, Gateway, Registry); the eight transaction primitives and their callback structure (signed message envelopes with sender DID + payload + signature; the participant Registry with discovery semantics; the tag-group extension mechanism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



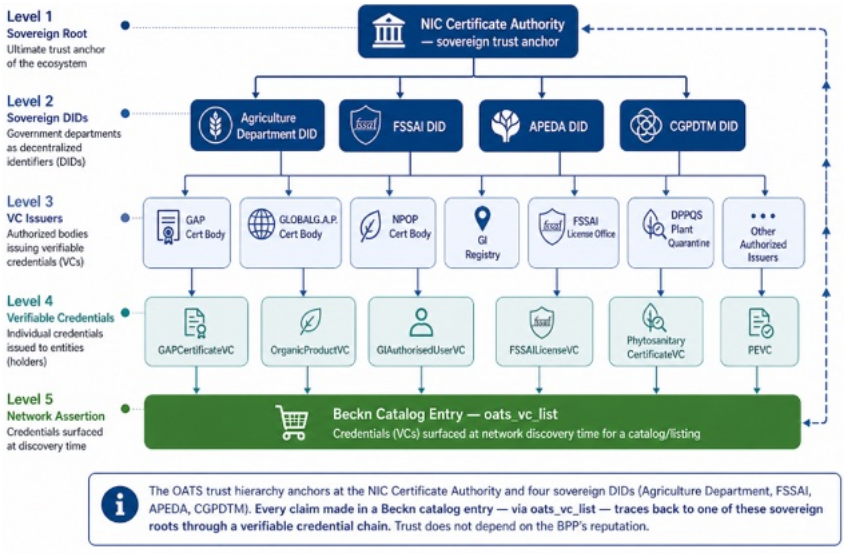
8.4 OATS Network Policies

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 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.

8.6 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 that lot ID, regardless of which Beckn domain produced them.

Worked example. 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 (Hyperledger Fabric, Hyperledger Besu, IOTA, CORD), specifies how W3C VCs are anchored through hash commitments, defines the scope of smart contracts, and draws lessons from implementations including IBM Food Trust, TradeTrust, and Maha-TRACE.

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.

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

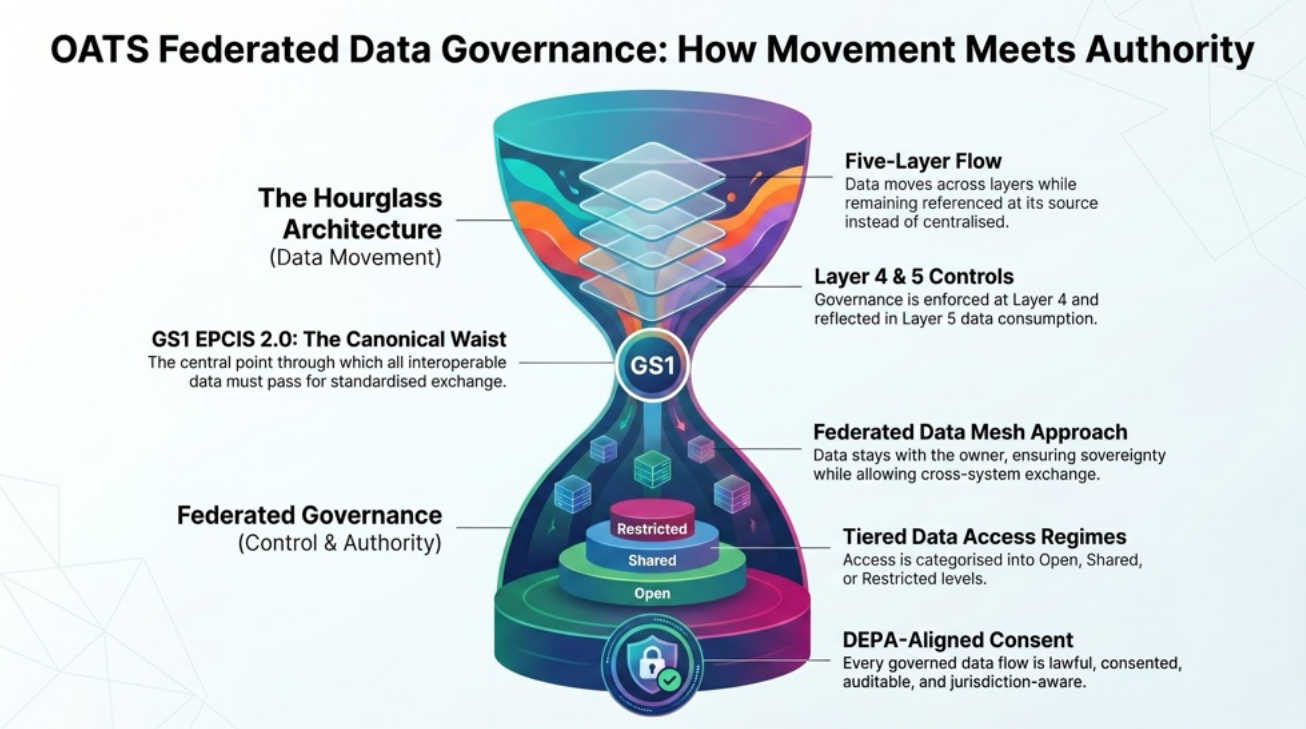
A permissioned ledger derives its trust not from technology alone but from transparent, multi-stakeholder governance. OATS operationalises this through a consortium model under the **Multi-Stakeholder Governance Council** defined in Chapter 3.

10. 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.

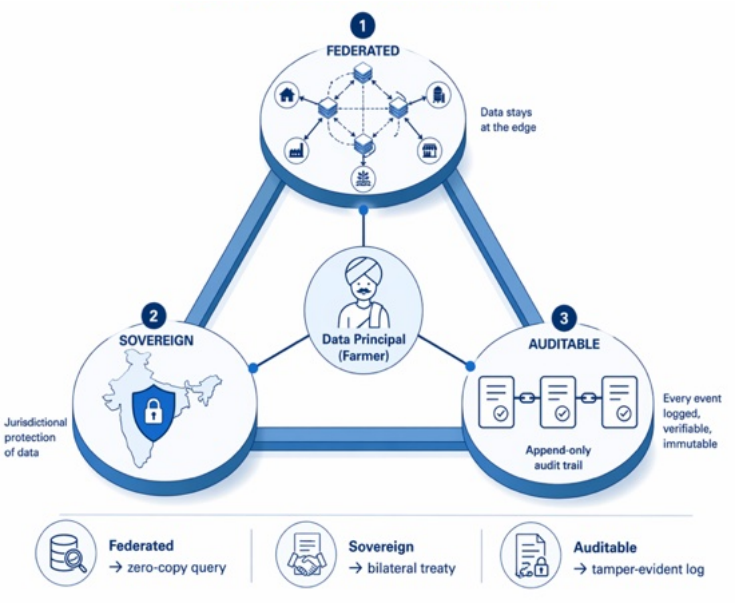
The OATS data governance model is explicitly federated. Data remains at its source in Layer 1 and Layer 2 systems, is referenced rather than centralized, and is exchanged through standardized interfaces without compromising ownership or sovereignty. This chapter formalizes the data mesh approach for 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-aware10.1 OATS Data Governance Philosophy: Federated, Sovereign, Auditable

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 OATS data governance model is explicitly federated: data remains at its source in Layer 1 and Layer 2 systems, is referenced rather than centralised, and is exchanged through standardised interfaces without compromising ownership or sovereignty. This chapter formalises the data mesh approach, defines tiered data access regimes, establishes data-quality and audit requirements, and embeds cross-jurisdiction safeguards. The hourglass remains intact: all cross-system exchange continues to pass through Layer 3, governance controls are enforced through Layer 4, and consumption is reflected in Layer 5.



10.1.1 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.

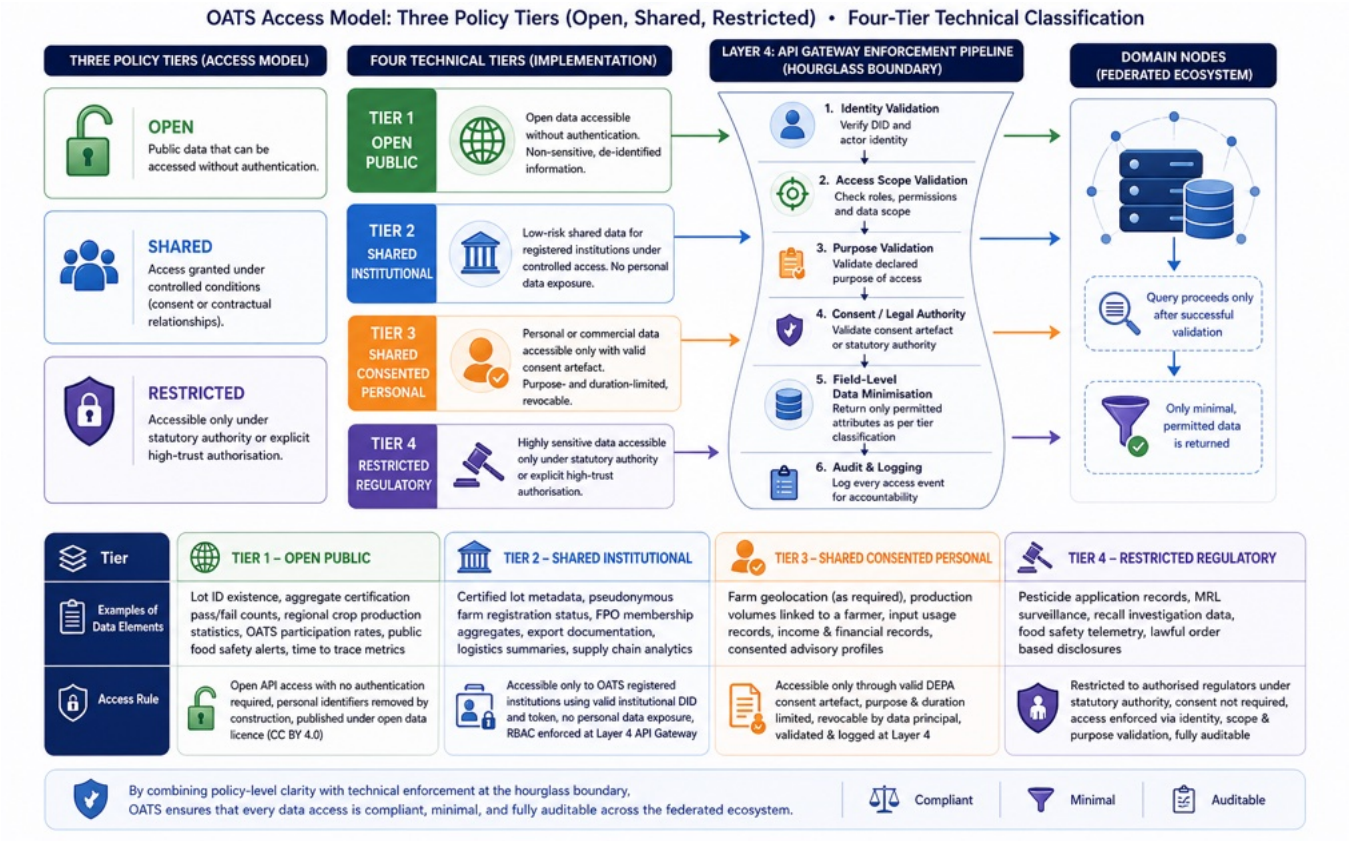
10.2 Data Mesh Architecture for Agri-Food Traceability

Data is treated as a **domain-owned data product**; each participant (farmer system, FPO platform, processor, logistics operator, exporter, regulator) 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, 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.

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. Four governance properties follow that 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.

10.3 Three-Tier Data Access Model



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. 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** on every request:

- **Tier check** - the requested endpoint's classification does not exceed the token's permitted tier.
- **Scope check** - the endpoint is within the token's authorised API set.
- **Purpose check** - the declared purpose aligns with permitted use cases and, for consented data, matches an active consent artefact.

Identity check — the presenting DID matches the token subject and cryptographic proofs are valid.

Any failure produces a structured error response; the denial is recorded in the audit trail. Endpoint-level tier enforcement is complemented by field-level filtering at the API Gateway: each data field in the OATS Data Dictionary carries an associated tier classification, disclosure rules, and purpose bindings, so a single endpoint serves multiple access contexts without duplicating APIs.

Consent architecture. Consent enforcement is embedded into the same API Gateway and domain-node validation flows. The full DEPA-aligned consent specification, including ORGANS principles, consent-artefact schema, and Consent Manager registration, is set out in Chapter 12.

10.4 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. Each jurisdiction has its own data-protection regime, food-safety statute, export documentation framework, and data-localisation rules. **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.

10.5 Data Quality and Audit Trail

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

Enforcement. 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 Data Quality Alerts that trigger remediation workflows for the originating actor and visibility for relevant regulators.

Audit Trail. 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: Merkle roots anchored hourly, with 7-year retention. Audit access is stratified — Data Principals access their own personal-data history through accessible channels (mobile, voice, USSD, assisted centres); Data Fiduciaries review through their Data Protection Officers; regulators access under statutory authority with all access validated and logged; the Farmer Data Rights Ombudsman retains full access for grievance investigation.

10.6 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.

11. OATS Consent management System

Within the Chapter 4 hourglass, consent is a Layer 4 control mechanism governing every movement of personal data. It is **not an application-level feature but a system-level requirement** — a sovereign control exercised by the Data Principal. Where no statutory lawful basis exists, data access is contingent on explicit, informed, revocable consent. The controlling statute for any Indian deployment is the **DPDPA 2023 and DPDP Rules 2025**; most provisions map directly to OATS architectural controls.

11.2 The ORGANS Framework:

The ORGANS Framework — **Open, Revocable, Granular, Auditable, Notice-based, Selective** — distils DPDPA 2023, GDPR, UNDP DPI Safeguards v2.0, and field-tested DEPA Account Aggregator experience into **six design properties every OATS-conformant Consent Manager must satisfy**. Each is independently testable; **five out of six is non-conformant.**

O - Open	Interface specifications, artefact schemas, and audit-log formats published as royalty-free open standards. No proprietary extensions at the consent boundary.
R - Revocable	Revocable at any time through any channel the farmer can use; effect within 24 hours, full propagation in 7 working days.
G - Granular	One artefact per (data category, purpose, recipient, duration). Bundled consent prohibited; schema enforces single-purpose. Operationalises DPDPA DP-2 and GDPR Art. 6(1)(a).
A - Auditable	Every lifecycle event (request, grant, denial, view, update, revocation, expiry, archive) written to an append-only, DID-signed audit log; accessible to the Data Principal and to the DPA on lawful request.
N - Notice-based	DPDPA §5 / GDPR Art. 13–compliant notice required; plain-language grade-5 reading level; vernacular with voice rendering. Notice digest embedded in the artefact — exact text non-repudiable. Machine translation prohibited for legally operative content.
S - Selective	A single consent may authorise sharing of some attributes of a credential while suppressing others.

11.3 Consent Manager Architecture and Registration

A Consent Manager (CM) is a **user-empowering intermediary** whose sole function is to collect, store, notify, revoke, and audit consent artefacts. Following the DEPA design pattern, **a CM is not a data consumer and not a data producer** — it stores no personal data beyond consent artefacts and has no commercial interest in the data flows it mediates. This **structural neutrality** is what makes a CM trustworthy in a way no agribusiness platform or certifier can be. Three deployment models are supported:

Model	Description
Government-Operated	Run by the Agriculture Department or designated agency (e.g., AIAIC in Maharashtra). Universal, zero-cost CM. Must be ring-fenced with its own DPO and audit chain to preserve structural neutrality.
Licensed Private	Registered under a Sahamati-equivalent SRO, licensed by the Digital Governance Authority, supervised by the Data Protection Board. Per-artefact fee paid by the Data Fiduciary, never by the Data Principal.
FPO-Federation	Operated by an FPO consortium for its membership. Same conformance requirements. Must not condition FPO membership on consent choices (DPDPA §6(4); GDPR Art. 7(4)).

Every OATS-conformant CM must be registered in the **OATS Consent Manager Registry** maintained by the OMGC. Registration requires legal-entity incorporation and a published DPO; published conformance-test results from the OATS Reference Laboratory; an SLA committing to FRS-13 / SRS-13; an operational grievance channel; and annual independent audit. Failure in any triggers suspension.

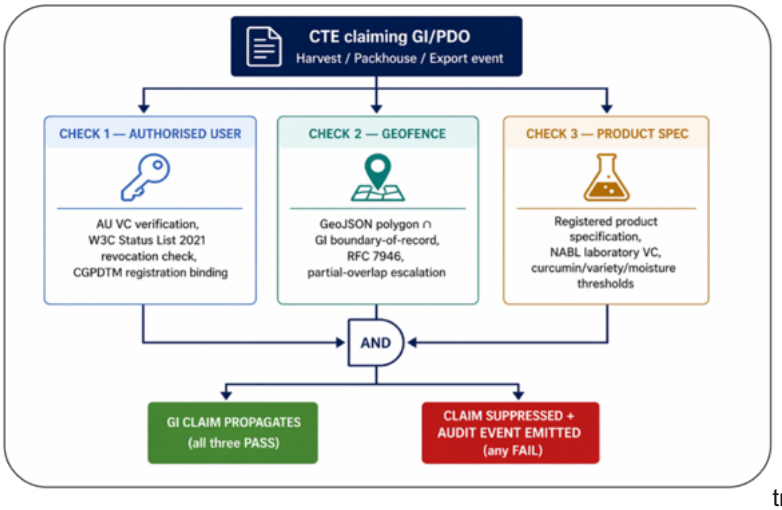
12. Regulatory Compliance Framework and Legal Architecture

The OATS compliance architecture operationalises **compliance-by-architecture** within the Chapter 4 hourglass. 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, GI attestations — are derived; the Layer 4 governance plane enforces validation rules, consent, and auditability. OATS models the global regulatory landscape along three axes: **horizontal** (baseline obligations across commodities, implemented through the core event schema), **vertical** (commodity- or claim-specific extensions to the canonical model), and **extraterritorial** (handled through Verifiable Credentials and cross-border compliance artefacts 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.

12.1 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 a 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 origin claim — OATS makes the legal claim operationally verifiable at every supply-chain event.

Three-Check Enforcement. The OATS GI Verification Module 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 suppresses the claim on downstream events, with the suppression itself recorded as an auditable EPCIS event.



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 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+).

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

Three organic regimes dominate global trade. OATS implements a **single Organic Module** parametrised by destination-market regime and equivalence chain — the operator maintains a correctly-issued certification VC chain, and the module generates destination-specific export documentation from that chain.

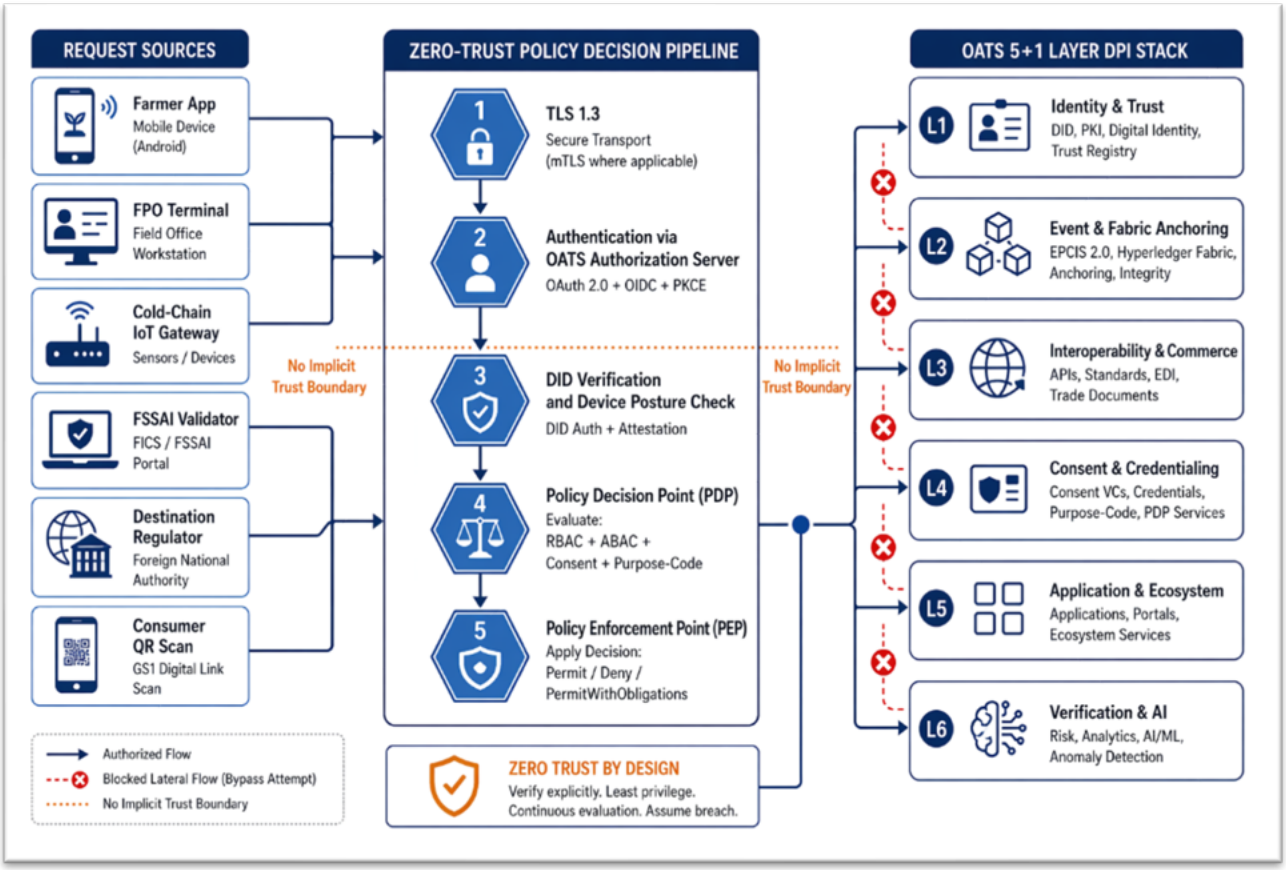
Regime	Key Specifications
India - NPOP	Statutory foundation: Foreign Trade (Development and Regulation) Act 1992. Administrative authority: APEDA. Current operational manual: 8th Edition. Certification by APEDA-accredited Certification Bodies; e-TraceNet issues Transaction Certificates.
United States - 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 — handlers, traders, brokers, and exporters previously exempt are now in scope. NOP Import Certificate required for organic imports.
European Union - Reg. (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.

13. Cybersecurity, Privacy and Data Protection Architecture

The OATS security architecture adopts a zero-trust model aligned with NIST SP 800-207 and is instantiated within the Chapter 4 hourglass as a cross-cutting control. No actor, device, network, or system component is implicitly trusted regardless of its location. 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 because the operational boundary spans heterogeneous environments — farmer devices, field infrastructure, government systems, cross-border regulatory platforms, cloud services — where traditional perimeter-based assumptions are invalid.

13.1 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.



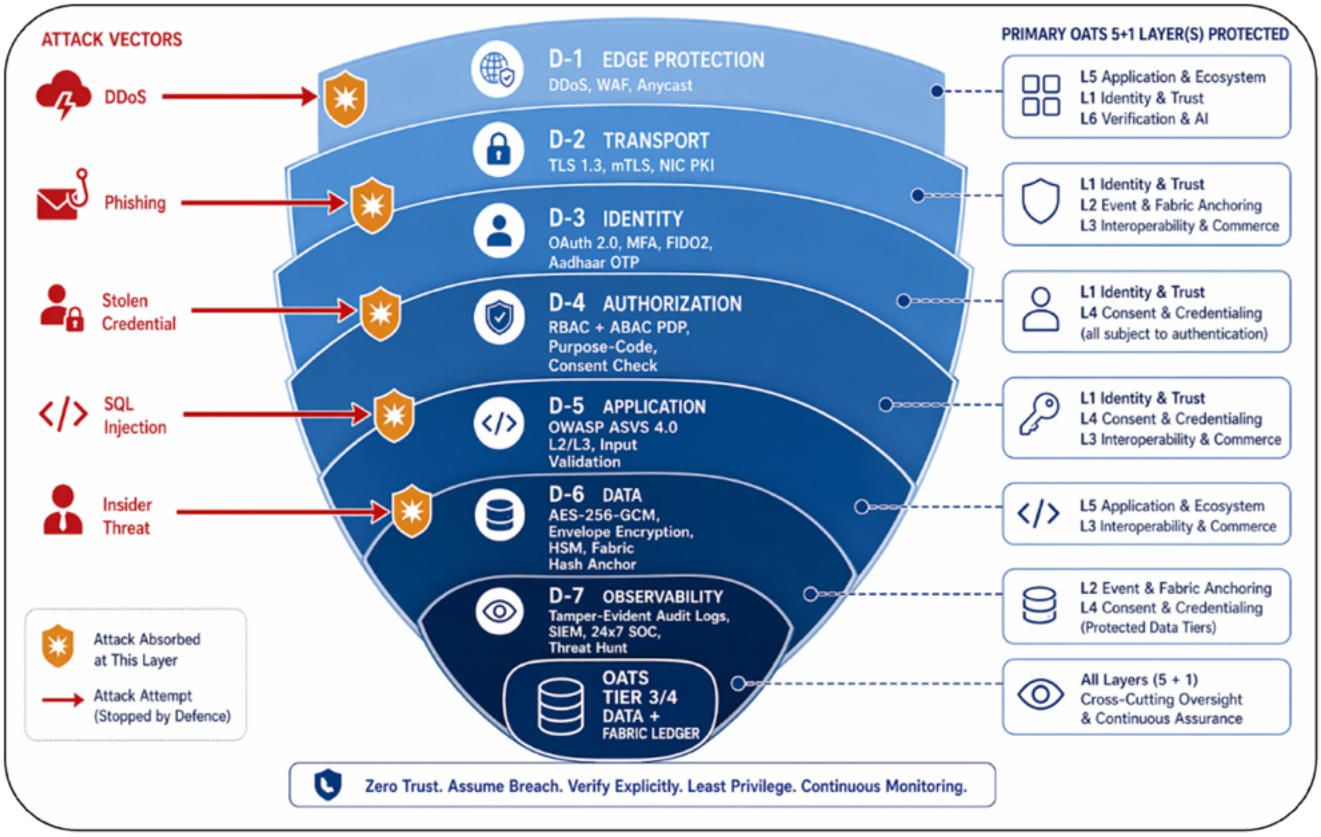
The Five Zero-Trust Tenets (NIST SP 800-207), non-negotiable for every OATS deployment:

Tenet	Principle	OATS Implementation
ZT-1	All data sources and computing services are resources.	Every OATS component (DID Resolver, VC Verification, PEVC Compliance Engine, IoT Ingest, Consumer Resolver, Fabric peer nodes) is treated as an independent protected resource with its own authentication, authorisation, and audit boundary.

ZT-2	All communication is secured regardless of network location.	TLS 1.3 across all API endpoints; service-mesh mTLS for all intra-service communication, no plaintext traffic 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 with one-hour maximum lifetime; each session evaluated independently using DID identity, purpose code, data tier, and consent posture — no carryover of trust between sessions.
ZT-4	Access is determined by dynamic policy including observable state.	Authorisation decisions executed through a Policy Decision Point using engines such as Open Policy Agent or XACML, evaluating requester attributes, resource sensitivity, and environmental context (time, geolocation, device posture, threat intelligence).
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 streamed to the Security Operations Centre with automated quarantine enforcement for any asset deviating from defined posture baselines.

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.

Seven-Layer Defence-in-Depth Stack. Zero-trust does not replace defence-in-depth — it intensifies it.



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.

13.2 Key Management and PKI

OATS operates three coordinated but distinct cryptographic infrastructures, all anchored in the same sovereign trust roots: a classical **PKI** for X.509 certificates used in TLS, mTLS, and document signing; a **W3C DID infrastructure** for decentralised identity and Verifiable Credential signing; and a **Hyperledger Fabric CA infrastructure** for Fabric peer and orderer identity within Layer 2 blockchain channels. IAM enforcement combines RBAC and ABAC at the API Gateway and consent-governance layers (canonically specified in Chapter 11).

13.3 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 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.

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.

13.4 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.

14. Consumer Transparency and Market Access

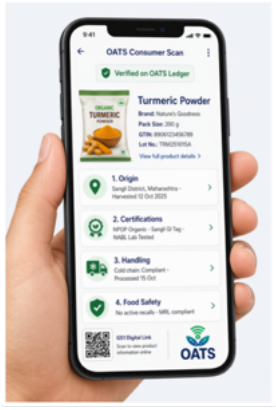
The **right to know** — rooted in Codex Alimentarius traceability principles and India's Consumer Protection Act 2019 — is that every consumer of an agricultural or food product is entitled to a **machine-verifiable, understandable, and timely disclosure** of the product's origin, certification status, 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. Consumers must be able to verify a product without creating an account, logging in, or surrendering any personal data.

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.

14.1 Consumer Transparency: The Right to Know

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, GLOBALG.A.P., 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. Conventional brand-controlled transparency produces three structural failures: each brand reinvents its own verification stack, driving compliance cost up and interoperability down; **consumers cannot trust a brand-controlled disclosure because the disclosing party is also the party with an economic interest in what is disclosed**; and smaller producers cannot afford the custom-app route. OATS resolves all three 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; 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.

14.2 GS1 Digital Link QR Code Consumer Journey Design

Grounded in the GS1 Digital Link Standard (ISO/IEC 18975) and aligned with **GS1 Sunrise 2027**. 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. The six-step flow:

- **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 the OATS Lot Registry and returns redirect to the rendered provenance page.
- **S3** — Consumer sees Four-Pillar summary 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 chain as JSON-LD.
- **S5** — Consumer optionally taps "Report Issue"; feedback captured anonymously and routed to FSSAI and producer via the OATS Grievance Module.
- **S6 — Offline fallback** — if no connectivity, QR shows cached provenance summary signed 24 h ago via PWA service worker.

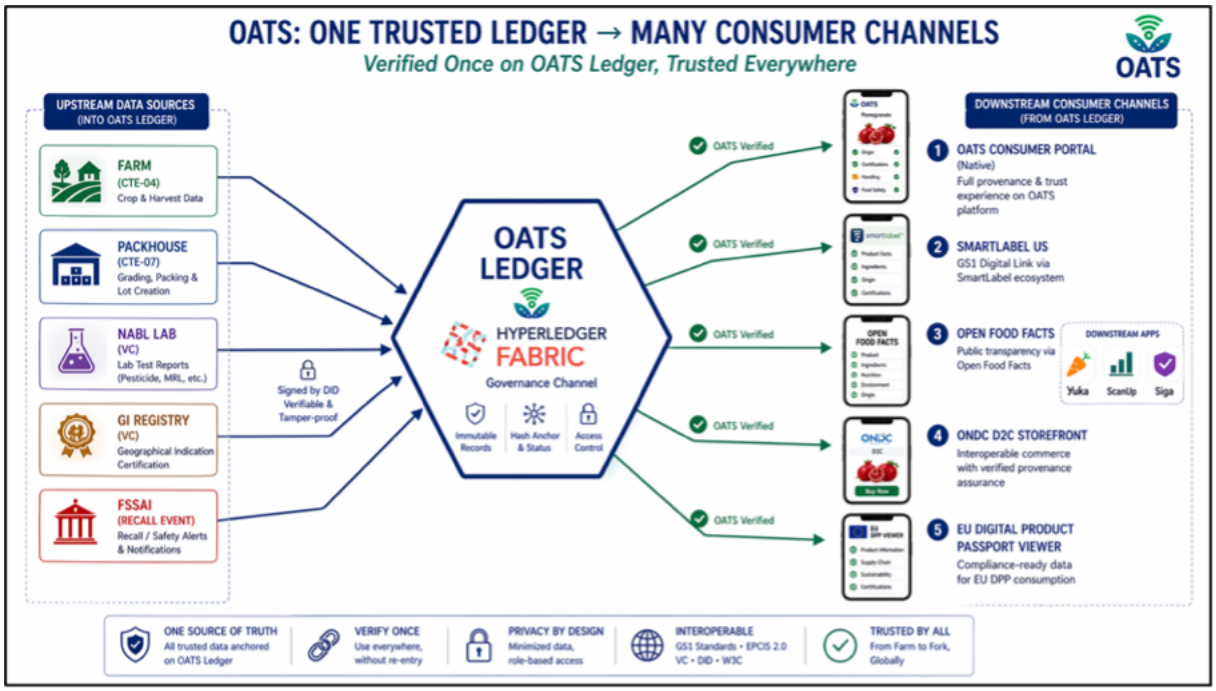
Context-Aware Resolver — One QR, Many Audiences. The same physical QR code returns different representations to different requesters via GS1 Digital Link *link-type negotiation*. OATS implements four contexts: **Consumer device (default)** — human-readable provenance in device locale, anonymous, no personal data captured; **Regulatory device** (FSSAI inspector app presenting DID) — full EPCIS event chain with all KDEs, VCs un-redacted, AI/ML anomaly flags; **Retailer ERP** (OATS API credential) — structured JSON-LD for ERP, POS, and self-checkout flows; **Export authority** (EU TRACES NT, US FDA PREDICT) — the OATS PEVC package. **A single printed QR code serves every stakeholder without privacy leakage across audiences.**

14.3 SmartLabel and Open Food Facts Integration

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

SmartLabel Integration. The OATS Layer 5 SmartLabel Adapter generates a SmartLabel-conformant Product Information JSON at CTE-07, 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 or the SmartLabel page, **byte-identical across both channels**. This eliminates the current industry problem of divergent claims between SmartLabel pages and brand websites.

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



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

Consumer transparency and smallholder income are two sides of one coin. GI and organic premium markets suffer from **information-asymmetry failure**: a consumer in Bengaluru paying a 40% premium for "Sangli Turmeric" has no independent way to verify origin — **30–60% of GI-labelled products in retail have historically been non-compliant with their stated GI zone**. The premium is captured by counterfeiters and opportunistic brands; none reaches the originating

community. OATS closes the asymmetry with a cryptographic chain-of-proof from the GI-registered farm to the consumer QR scan, satellite-verified against ISRO Bhuvan field geo-polygons. **A consumer can distinguish a genuine Sangli turmeric lot from a counterfeit with a single scan at zero cognitive cost.**

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; 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 attestation; chain-of-custody	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. ***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.***

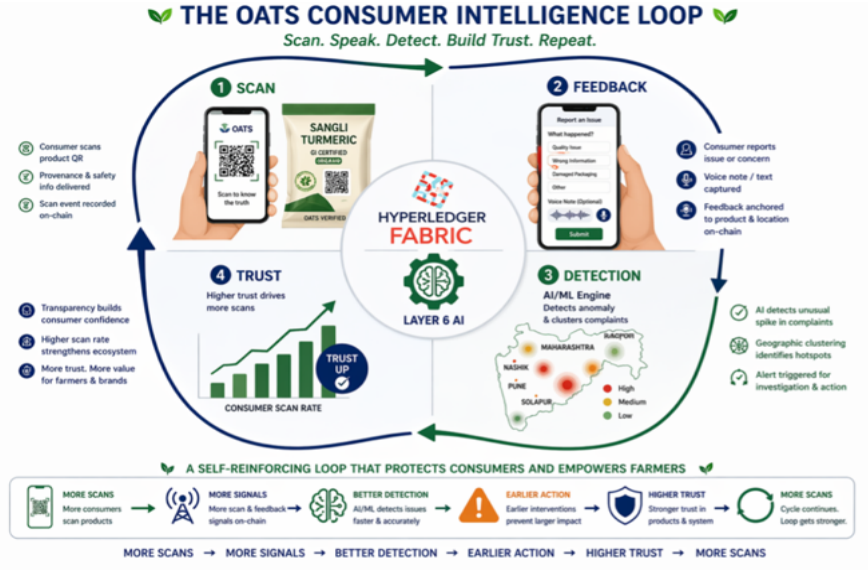
14.5 ONDC and D2C Commerce Integration for GI Products

OATS operates as a registered BPP on the ONDC Agriculture domain. Every OATS-traced consumer unit — not just export lots — is automatically catalogue-published to ONDC via the OATS-Beckn Gateway. Any ONDC-compliant BAP (Magicpin, Paytm, Mystore) 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: product name + GI qualifier (e.g., “Turmeric Powder Sangli GI”); producer FPO / farm image (DPDPA-consented); OATS LGTIN (hidden, used by BAP verification); GS1 Digital Link “See full journey” URL; list of active VC certification badges; district-level origin (per DPDPA minimisation); and a **Verified Premium** boolean badge for fraud prevention.

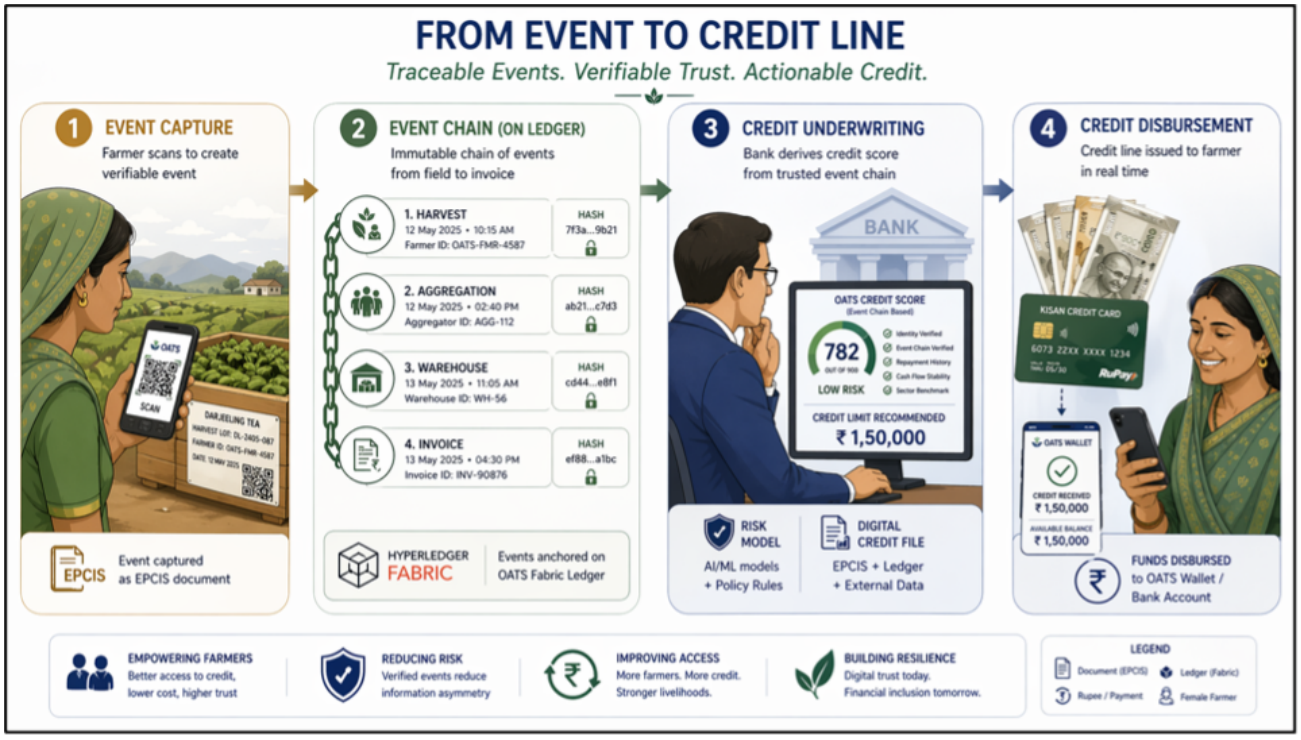
14.6 Consumer Grievance and Product Feedback Mechanisms

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.



15. Financial Inclusion and Value Chain Finance Module

The central premise of this chapter is that **an OATS event chain 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, invoice raised against a registered buyer — is available to a lender or insurer as a **verifiable, tamper-evident, machine-readable history** rather than a self-declared paper trail. The 2021 Findex Database recorded that 76% of adults globally now have a financial-institution account, 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 — and OATS directly closes that gap.



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 with India Stack Financial Rails. OATS does not replicate existing financial infrastructure — it federates with Aadhaar eKYC, UPI, eSign, DigiLocker, and the Account Aggregator (AA) framework. The **farmer's OATS Wallet becomes an AA-recognised Financial Information Provider (FIP) publishing Agricultural Activity Data** — positioning verified traceability data alongside bank statements and GST returns as a first-class underwriting input.

15.1 Digital Credit Scoring from Supply chain Event data

The OATS Credit Scoring Service produces an **Agri-Credit Score (ACS) on a 300–900 scale** compatible with CIBIL / CRIF format. **The ACS 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.

Feature Family	OATS Source Events / Credentials	Indicative Weight
Farming Consistency — seasons declared, continuity of crop plan, adherence to calendar.	ObjectEvent (declare), TransformationEvent (harvest); AgriStack parcel record.	20%
Yield Reliability — declared vs. measured yield; satellite-verified area; mass-balance.	TransformationEvent; Sentinel-2 phenology match; AggregationEvent mass-balance.	20%
Compliance Quality — PHI adherence, MRL pass rate, VC validity, calibration status.	W3C VC chain; NABL lab VC; CBI inspection VC.	15%
Market Depth — 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 GI/organic.	TransactionEvent commercial value; eNAM / ONDC price reference.	10%
Storage Discipline — eNWR deposits, cold-chain SLA adherence, warehouse audit VC.	AssociationEvent (IoT); WDRA eNWR cross-reference.	10%
Repayment Track Record — prior KCC, past OATS-linked loans, 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 every lender computes the same score from the same inputs. Lenders may layer proprietary scorecards on top of the ACS but may not substitute it with a closed replacement when consuming OATS data under the standard data-sharing agreement.

15.2 Supply Chain Finance: Invoice Discounting and Factoring

The binding constraint on FPO and mid-tier agri-processor working capital is the **30-to-90 day payment cycle** between delivery and cash realisation. The OATS Supply Chain Finance Gateway (SCFG) converts an OATS-traced invoice into a discountable instrument on the RBI's **Trade Receivables Discounting System (TReDS)** and on ONDC's Financial Services domain, unlocking same-day liquidity.

A Beckn-confirmed transaction generates an EPCIS TransactionEvent VC at the OATS-Beckn Gateway; in parallel, the supplier issues a **Commercial Invoice VC signed by the supplier's DID**. Upon delivery confirmation (an ArrivalEvent signed at the buyer's GLN), **the buyer co-signs the Commercial Invoice VC** — attesting goods delivered, buyer irrevocably accepted, invoice non-disputed. The result is a co-signed receivable credential that is intrinsically discountable. Any RBI-registered TReDS financier (banks, NBFC-Factors) may bid; OATS enables presentation only, with pricing and financing competition happening on the external rail — a direct application of **DPI as infrastructure, not platform**.

15.3 Smart Contract Payment Triggers at Delivery Milestones

Where the deployment includes Hyperledger Fabric, the Traceability Chaincode is extended with a **Milestone Settlement module** that binds escrow release to the successful commit of defined EPCIS events. **Functionally equivalent to a letter of credit** with delivery-event verification replacing the document-examination step — but executes in minutes rather than days, at a fraction of the cost.

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.

15.4 DBT and CBDC Integration

India's Direct Benefit Transfer architecture is mature but **blind** — the disbursing agency confirms a rupee reached a bank account but cannot confirm it reached the correct farming activity. OATS closes the assurance loop in two modes:

- **Pattern A - Traceability-Conditional DBT on APBS.** The disbursing scheme publishes an OATS-integrated eligibility rule; OATS provides a real-time attestation API consumed by PFMS workflow; **APBS release occurs only on a positive attestation**. No change to existing CBDC architecture required.
- **Pattern B - Programmable CBDC with Outcome Binding.** In the retail e₹-R pilot, OATS provides the **outcome-verification oracle**: a PMFBY settlement is issued as a programmable token spendable with no restriction, but with a post-hoc verification hook — if the claim is later found fraudulent against OATS event data, compensating clawback triggers automatically. Preserves consumption freedom while closing the fraud window.

15.5 Crop Insurance Integration with Traceability Events

PMFBY Revised 2023 Guidelines explicitly move the scheme toward yield-based and weather-indexed settlement. OATS delivers the technology layer - satellite yield verification, IoT-attested weather event capture, farmer-declared loss events making this operationally feasible at scale.

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.
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 event.

The insurer, on enrolling a farmer, receives a consented OATS event subscription for the insured parcel. **This transforms agricultural insurance from a post-loss inspection model to a continuous-monitoring model** — fraud detection is instantaneous; legitimate claims settle automatically against a rule published in the scheme's OATS Regulatory Parameter Registry entry. A farmer with three seasons of OATS-verified good agricultural practice qualifies for a lower premium under the scheme's technology-driven risk-adjustment provision.

15.6 Warehouse Receipt Finance: Integration with eNAM and WDRA

OATS supports the existing eNAM and WDRA infrastructure with one architectural extension: the **electronic Negotiable Warehouse Receipt (eNWR) 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. A lender financing against the eNWR can verify in a **single chained VC presentation** the warehouse's authority to issue, the depositor's title to the goods, the underlying provenance, and the regulatory and quality certifications applicable. The **eNWR-as-VC pattern is a Phase-0 deliverable** — 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.

15.7 Gender-Responsive Finance Design for Women Farmer

Women account for 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.

15.8 Financial Sustainability and Private sector Participation

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**. TaaS is delivered to non-producer counterparties on a fee-paying basis while smallholders, FPOs, and cooperatives remain zero-rated. Four commercial verticals:

- **Regulatory Compliance Attestation** — per-lot provenance VCs issued to importers, customs authorities, and brand owners to satisfy EUDR, EU CSDDD, US FSMA, UK Environment Act, FSSAI Recall, and Japan / Korea / Gulf equivalents (largest near-term revenue opportunity).
- **Premium Quality and Specialty Provenance** — verifiable origin and cultivar credentials for high-margin classes (single-estate specialty coffee, single-origin cocoa, Darjeeling first-flush, single-varietal Basmati, single-source spices).
- **Organic and Regenerative Certification Anchoring** — NPOP / USDA-NOP / EU 2018/848 / Naturland / Bioland / JAS / KOFA certificate chains cryptographically anchored.
- **Geographical Indication Proof of Provenance** — tamper-evident proof for the 600+ GIs registered under the Indian GI Act 1999, addressing the multi-billion-dollar annual counterfeit-GI problem and WIPO Lisbon Agreement / TRIPS Articles 22–24 obligations.

Three non-negotiable guardrails across all commercial participation 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; and 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. The financing path follows a **four-phase blended glide-path** — Ignition (100% concessional) → Co-Investment → Blended Operations → Self-Sustaining — gated by Key Sustainability Indicators rather than elapsed time alone. At no point does the model contemplate user fees for smallholders accessing core traceability functions.

APPENDICES & REFERENCES

APPENDIX A — STANDARDS INDEX AND REFERENCES

The Blueprint is mapped to authoritative standards across identity, traceability, food safety, regulatory compliance, infrastructure, security, and DPI governance. Standards are grouped by domain; each standard name is a clickable link to its primary source. Version histories and the full digital catalogue are maintained in the OATS Standards Registry.

1. Foundational Identity, Credentials, and Web Standards

W3C: DID Core v1.0 (2022); VC Data Model v2.0 (2025); VC Status List 2021; PWA Manifest (2024); WCAG 2.2 Level AA (2023); ARIA 1.2 (2023); Web Speech API (2020); VoiceXML 2.1 (2007); JSON-LD 1.1 (2020). DIF: Presentation Exchange 2.0; BBS+ Signatures (DIF / IRTF CFRG, 2023). Indian DPI identity: MOSIP (IIIT-B / MOSIP Foundation); AgriStack Farmer Registry API (MeitY / NeGD, 2024); DEPA Consent Artefact v1.1 (Sahamati / NITI Aayog, 2022); Sahamati Account Aggregator AA-1.1.2 (2022–2025); UIDAI AUA/KUA APIs; STQC L1 Biometric Devices Certification; DigiLocker Issuer APIs; TPM 2.0 Attestation (Trusted Computing Group, 2019).

2. GS1 Standards Family

Core: EPCIS 2.0 (ISO/IEC 19987:2024); CBV 2.0; General Specifications v24 (2024); Digital Link Standard v1.3 (ISO/IEC 18975, 2022); EPC Tag Data Standard 2.0 (2024). Implementation guidance: EPCIS 2.0 REST Bindings Implementation Guideline (2022); GS1 US FSMA 204 Recommendations (2023); GS1 Sunrise 2027 Programme (2021–2027); GTIN Allocation Roadmap (GS1 India, 2024).

3. ISO/IEC Standards (Food, Security, Identification, Data)

Food and supply chain: ISO 22000:2018 Food Safety Management (TC 34/SC 17); ISO 22005:2007 Traceability; ISO 23412:2020 Temperature-Controlled Refrigerated Delivery; ISO 8000 Data Quality; ISO 14021 Self-Declared Environmental Claims; ISO/IEC 17065 Conformity Assessment (2012). Security and privacy: ISO/IEC 27001:2022 ISMS; 27035:2023 Incident Management; 27701:2019 Privacy Information Management. Identification carriers: ISO/IEC 18004:2015 QR Code; 16022:2006 DataMatrix; 18000-63:2015 RFID UHF (EPC Gen2); 14443 NFC Type A/B; 15693 NFC Type 5.

4. International Food Safety and Trade Conventions

Codex Alimentarius (FAO/WHO): CAC/RCP 1-1969 Rev. 2020 Food Hygiene (HACCP); CAC/GL 60-2006 Traceability; CAC/GL 32 Rev. 1999 Organic. WHO/FAO: INFOSAN (190+ countries); WHO PQS Cold Chain Equipment Specifications (2024). IPPC (FAO): ePhyto Hub XML; ISPM 7 and ISPM 12 Phytosanitary Certificates. WTO/WIPO: WTO SPS Agreement (1994); TRIPS Agreement Art. 22–24 (Geographical Indications, 1995); WIPO Lisbon Agreement Geneva Act (2015).

5. European Union Regulatory Architecture

Food and trade: Reg. (EC) 178/2002 General Food Law; (EC) 396/2005 MRLs Pesticides; (EU) 1151/2012 GI Quality Schemes; (EU) 1169/2011 Consumer Food Information; (EU) 2017/625 Official Controls; (EU) 2018/848 Organic; (EU) 2021/1935 Accreditation; (EU) 2023/1115 EUDR; (EU) 2024/1143 Unified GI; (EU) 2024/1781 ESPR / DPP; Directive (EU) 2024/1760 CSDDD. Data protection: GDPR (EU) 2016/679; EDPB Guidelines 05/2020 on Consent. Platforms: TRACES NT (DG SANTE); iRASFF (since 2021); CIRPASS DPP Common Data Model (2024); eTranslation (DG CNECT).

6. United States, United Kingdom, Japan, GCC, and Other Jurisdictions

United States: FSMA §204 Final Rule (21 CFR Part 1 Subpart S, 87 FR 70910); FSVP (Subpart L); PREDICT; OASIS; Reportable Food Registry; USDA NOP (7 CFR Part 205, SOE Final Rule 88 FR 17748, 2024); Uyghur Forced Labor Prevention Act (PL 117-78, 2021). United Kingdom: UK Retained EU Law; BRCGS; Environment Act forest-risk schedules; IPAFFS; UKCA. Japan: Plant Protection Act; Positive List System; JAS Organic. UAE/GCC: SFDA; GSO Standards; Halal Certification. Other: Brazil LGPD (Law 13,709/2018); Kenya Data Protection Act 2019; South Africa POPIA (Act 4/2013); Singapore–Australia Digital Economy Agreement (2020); EU–Japan Mutual Adequacy Decision (2019); APEC Cross-Border Privacy Rules System (2011 Rev.).

7. India — Regulatory, DPI, and Finance

Food and GI: FSS Act 2006; FSS (Recall) Regs 2017 + draft 2024; FSS Import Regs 2017; FSSAI Schedule 4; GI Act 1999; NPOP 8th Ed.; APEDA Act 1985 (e-TraceNet / HortiNet); FT(D&R) Act 1992. Data protection: DPDPA 2023 (Act 22 of 2023); DPDP Rules 2025; IT Act 2000 (§§43A/72A/79); CERT-In Directions §70B(6) (2022). Consumer and disability: Consumer Protection Act 2019; Rights of Persons with Disabilities Act 2016. DPI: InDEA 2.0 (NeGD / MeitY, 2022); Bhashini (MeitY, 2022); AgriStack Farmer Registry API. Finance: RBI AA Master Directions (2016 Rev. 2023); TReDS; V-CIP; e₹-R CBDC Concept Note. Agri-finance: PMFBY Revised 2023 Guidelines; WDRA eNWR Regulations; eNAM (SFAC); PM-KISAN; DBT-F (Fertiliser); MSP Procurement (NAFED/FCI). Telecom: WPC/DoT UHF RFID 865–867 MHz Spectrum Allocation (2021); TRAI Commercial Communication Regs + DLT Registration.

8. Certifications and Sustainability Schemes

GLOBALG.A.P. IFA v6 Smart / CoC v6 (2023); Better Cotton Initiative Production P&C; Rainforest Alliance / UTZ-merged; Fairtrade International / Fairtrade India; SMETA / Sedex (2- and 4-pillar audit); GRI 13 Agriculture, Aquaculture and Fishing Sector Standard (2022); Regenerative Organic Certified; Naturland; Bioland; Fair for Life; EOA Africa.

9. API, Infrastructure, Security, and Cryptography

APIs and schemas: OpenAPI 3.1 (2021); AsyncAPI 2.6 (2022); GraphQL (October 2021); JSON Schema 2020-12. IETF RFCs (datatracker.ietf.org): RFC 8446 TLS 1.3; 6749 OAuth 2.0; 7636 PKCE; 9457 Problem Details; 7946 GeoJSON; 3161 Time-Stamp; 5280 X.509 PKI; 2119 Requirement Keywords. CNCF: CloudEvents v1.0; Apache Kafka; Kubernetes; Istio; OpenTelemetry. Hyperledger: Fabric v2.5; Besu (QBFT / IBFT 2.0). IoT: FIWARE NGSI-LD v1.6 (ETSI GS CIM 009); OGC SensorThings API Part 1 (OGC 15-078r6); MQTT v5.0. Security and cryptography: NIST SP 800-207 Zero Trust; NIST SP 800-162 ABAC / 800-61 Incident / 800-204A/B Microservices; FIPS 140-3 Crypto Modules; FIPS 203/204/205 Post-Quantum Cryptography (2024); TIBER-EU Framework; OWASP API Security Top 10 (2023) / ASVS 4.0.

10. DPI Frameworks, International Bodies, Licences, and Foundational Instruments

DPI frameworks: GovStack Building Block Specification v2.0 (ITU / DIAL); Universal DPI Safeguards Framework v2.0 (UNDP / UN Tech Envoy); CDPI Architecture Principles (2023); G20 DPI Principles (DEWG, August 2023); Digital Public Goods Standard v1.0 (DPGA); X-Road v7 (NIIS). International bodies: OECD Principles on PPPs / Privacy Guidelines; G20 Principles for Quality Infrastructure Investment (2019); World Bank PIM Guidance / DPI 2025 White Paper; IFAD Rural Finance Policy; IFC Banking on Women Measurement Framework; ICMA Green Bond Principles (2021). Open-source licences: Apache 2.0; EUPL; MIT License; ODbL (Open Database Licence); Open Government Licence. Human rights and foundational: UDHR Art. 12 (1948); UNGA Resolution A/RES/68/167 (Right to Privacy in the Digital Age, 2013); UN Guidelines for Consumer Protection (A/RES/70/186) (2016); Charter of Fundamental Rights of the EU (Art. 7/8); Puttaswamy v. Union of India (2017) 10 SCC 1.

APPENDIX B — SCHEMA AND API REFERENCE INDEX

C.1 OATS Verifiable Credential Schemas

Credential Name	Issuer (DID Domain)	Defining Chapter (in elaborated blueprint)
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

OATS

IDENTIFY — CAPTURE — SHARE

GS1 Standards for Identification

COMPANY & LOCATION
- Global Location Number (GLN)

PRODUCT
- Global Trade Item Number (GTIN)
- Serialized Global Trade Item Number (SGTIN)

LOGISTICS & SHIPPING
- Serial Shipping Container Code (SSCC)
- Global Shipment Identification Number (GSIN)
- Global Identification Number for Consignment (GINC)

ASSETS
- Global Individual Asset Identifier (GIAI)
- Global Returnable Asset Identifier (GRAI)

SERVICES & MORE
- Global Service Relation Number (GSRN)
- Global Document Type Identifier (GDTI)
- Global Coupon Number (GCN)

GS1 Standards for Barcodes & EPC/RFID

GS1 BARCODES

EAN/UPC | ITF 14 | GS1-128 | GS1 DataBar | GS1 DataMatrix | GS1 QR Code | GS1 Composite Barcode

GS1 BARCODES

Electronic Product Code (EPC) RFID | EPC HF Gen 2 | EPC UHF Gen 2

GS1 Standards for Data Exchange

MASTER DATA
- Global Data Synchronization Network (GDSN)

TRANSACTIONAL DATA
- eCom (EDI): EANCOM, GS1 XML

EVENT DATA
- EPC Information Services (EPCIS)

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