NIST Internal Report
NIST IR 8536 2pd

Supply Chain Traceability:

Manufacturing Meta-Framework

Second Public Draft

Michael Pease
Evan Wallace
Harvey Reed
Dr. Vivian L. Martin
Steve Granata

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8536.2pd

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Internal Report
NIST IR 8536 2pd

Supply Chain Traceability:

Manufacturing Meta-Framework

Second Public Draft

Michael Pease
Smart Connected Systems Division
Communications Technology Laboratory

Evan Wallace
System Integration Division
Engineering Laboratory

Harvey Reed
Dr. Vivian L. Martin
Steve Granata
MITRE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8536.2pd

July 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

NIST Technical Series Policies
[Copyright, Use, and Licensing Statements]
[NIST Technical Series Publication Identifier Syntax]

How to Cite this NIST Technical Series Publication
Pease M, Wallace E, Reed H, Martin VL, Granata S (2025) Supply Chain Traceability: Manufacturing Meta-Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8536 2pd. https://doi.org/10.6028/NIST.IR.8536.2pd

Author ORCID IDs
Michael Pease: 0000-0002-6489-2621
Evan Wallace: 0000-0001-9368-5616
Harvey Reed: 0000-0002-4589-2677
Vivian L. Martin: 0009-0000-8698-4730

Public Comment Period
July 31, 2025 – ~~September 1, 2025~~ October 3, 2025

Submit Comments
blockchain_nccoe@nist.gov

National Institute of Standards and Technology
Attn: Smart Connected System Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8200) Gaithersburg, MD 20899-8200

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8536/2pd, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of information other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, as well as its collaborative activities with industry, government, and academic organizations.

Note to Reviewers

NIST welcomes feedback and input on any aspect of NIST IR 8536 2pd and additionally proposes a list of non-exhaustive questions and topics for consideration:

1. How well does the Meta-Framework data model relate to existing supply chain management and security practices and your organization? Are there significant gaps between your current practices and the Meta-Framework that this paper should address?
2. How do you expect this white paper to influence your future supply chain traceability practices and processes?
3. How do you envision using this white paper? What changes would you like to see to increase/improve that use?
4. What suggestions do you have on changing the format of the information provided?
5. Is the guidance here sufficient to identify and address supply chain traceability? Are there changes or additional guidance that the authors should consider?

All comments are subject to release under the Freedom of Information Act.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) Assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend to hold any essential patent claim(s); or

b) Assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication, either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: blockchain_nccoe@nist.gov

Abstract

Manufacturing and critical infrastructure supply chains are vital to the security, resilience, and economic strength of the United States. However, increasing global complexity makes tracing product origins more difficult, exposing vulnerabilities to logistical disruptions, fraud, sabotage, and counterfeit materials.

This report introduces a meta-framework designed to enhance end-to-end supply chain traceability. The framework organizes, links, and queries traceability data across diverse manufacturing ecosystems, enabling stakeholders to verify product provenance, support fulfillment of external stakeholder obligations (e.g., legal, contractual, or operational requirements), and supply chain integrity.

The Meta-Framework builds on previous NIST research (IR 8419) and reflects input from industry, standards organizations, and academic collaborators. By improving supply chain transparency and risk mitigation, this framework supports national security, economic stability, and resilience in U.S. manufacturing operations.

Keywords

pedigree; provenance; supply chain traceability; traceability chain.

Acknowledgments

The authors would like to acknowledge the contributions from the community of interest (COI) and their suggestions and comments to improve the paper. They would additionally like to thank Robert Harder, MITRE, for his efforts in technically checking the Meta-Framework's data model and use cases.

Disclosure

This effort is funded by the U.S. National Institute of Standards and Technology (NIST).

This manuscript was edited with the assistance of NIST Enterprise subscription to Grammarly, which includes Generative AI tools, developed by Grammarly Inc. Grammarly was used to refine language, improve clarity, and enhance readability in accordance with the authors' instructions. All content, scientific claims, and conclusions have been reviewed and verified by the authors to ensure accuracy and originality.

Table of Contents

Executive Summary 1
1. Introduction 2
1.1. Supply Chain Traceability Needs and Challenges 3
1.2. Approach 4
1.3. Goals 5
1.4. Audience 5
1.5. Considerations and Limitations 6
2. Meta-Framework Overview 7
2.1. Traceability Records and Core Components 7
2.2. Trusted Data Repositories and Ecosystems 9
2.2.1. Controlled Access and Data Retention 9
2.2.2. Ensuring Data Integrity 10
2.2.3. Ecosystem Governance and Role in the Meta-Framework 10
2.3. Traceability Chain Across Supply Chain Ecosystems 10
2.4. Example Traceability Chain Across Ecosystem Boundaries 10
3. Meta-Framework Data Model 12
3.1. Traceability Records Overview 12
3.2. Traceability Record Structure 12
3.3. Traceability Record Subclasses 13
3.4. Traceability Links and Supplemental Data References 14
3.5. Ensuring Data Integrity and Interoperability 15
3.5.1. Common Data Models 15
3.5.2. Traceability Chain and Data Integrity Mechanisms 15
3.5.3. End-to-End Trust and Component Validation 16
3.5.4. Notional Traceback Scenario 17
3.5.5. Controlled Access and Authentication 18
4. Meta-Framework Use Cases 19
4.1. Creating and Recording Traceability Data 22
4.1.1. Sequence Diagram 1: Manufacturer of Microelectronics Make Traceability Events 22
4.1.2. Sequence Diagram 2: Operational Tech with Receive, Make, Assemble, and Ship 23
4.1.3. Sequence Diagram 3: Critical Infrastructure Acquirer with Receive and Employ 24
4.2. Querying and Retrieving Traceability Records 25
4.2.1. Sequence Diagram 4: Operational Technology with Traceback to ME 25
4.2.2. Sequence Diagram 5: Critical Infrastructure Acquirer with Traceback to ME and OT 26

4.2.3. Sequence Diagram Summary 27
5. Conclusion 29
References 30
Appendix A. List of Symbols, Abbreviations, and Acronyms 31
Appendix B. Glossary 33
Appendix C. Security, Privacy, and Access Control Considerations 35
C.1. Identity, Authentication, and Access Control 35
C.2. Privacy Measures 36
C.3. Balancing High-Assurance Identity and Privacy Risks 36
C.4. Threat Modeling and Ecosystem Risk Posture 37
C.5. Other Considerations 38
Appendix D. Future Directions for the Meta-Framework 39
D.1. Expanding Traceability to Sustainment and Lifecycle Phases 39
D.2. Additional Supply Chain Traceability Record Subclasses 40
Appendix E. Key Challenges in Achieving Interoperable Traceability 42
E.1. Challenge #1: Information Stored in Disjointed and Isolated Repositories. 42
E.2. Challenge #2: Inconsistent semantic and data definitions. 43
E.3. Challenge #3: Ensuring Traceability Data Integrity 44
E.4. Challenge #4: Balancing Confidentiality and Privacy in Traceability 45
Appendix F. Technical Data Model and Class Structures 48
F.1. UML Class Structure of Traceability Records 48
F.2. Traceability_Record Superclass 49
F.3. Traceability Record Supporting Data Objects 50
F.3.1. Key-Value Pair Data Objects 51
F.3.2. Traceability Link Data Object 51
F.3.3. Supplemental Link Data Objects 53
F.4. Event-Specific Subclasses 54
F.4.4. Make Record Subclass 54
F.4.5. Assemble Record Subclass 56
F.4.6. Ship Record Subclass 57
F.4.7. Receive Record Subclass 58
F.4.8. Employ Record Subclass 59
F.5. Conclusion 60
Appendix G. Technical Details and Governance Considerations 61
G.1. Serialization and Data Formats 61

G.2. Cryptographic Validation and Security 61
G.3. Governance and Data Retention Policies 62
G.4. Interoperability Mechanisms........ 63

List of Tables

Table 1: Traceability Record Description 12
Table 2: Record Subclass Descriptions 13
Table 3. Candidate New Sustainment Chain Traceability Record Subclasses 40
Table 4. Candidate New Supply Chain Traceability Record Subclasses 40
Table 5: Traceability Record Attributes 49
Table 6. Key_Value_Pair Attribute Definitions........ 51
Table 7. Traceability Link Attribute Definitions........ 52
Table 8. Supplemental Link Attribute Definitions 53
Table 9. Make Record Attribute Definitions 55
Table 10. Assemble Record Attribute Definitions 56
Table 11. Ship Record Attribute Definitions........ 58
Table 12. Receive Record Attribute Definitions 59
Table 13. Employ Record Attribute Definitions........ 60

List of Figures

Figure 1. Challenges of Component or Assembly Verification Across Stakeholder Tiers 4
Figure 2. General Construct of Traceability Records 8
Figure 3. General Construct of Traceability Chain 9
Figure 4. Value and Supply Chain Traceability Events Across Ecosystems 11
Figure 5. Overview Class Model 14
Figure 6: Traceability Chain through Ecosystems 16
Figure 7: End to End Trust Enables Component Validation........ 17
Figure 8. Sequence Diagrams in Context of Supply Chain Events 20
Figure 9. Ecosystem Example Actions and Interfaces 21
Figure 10. Manufacturer: Microelectronics ME-001 Writes Make and Ship Event Records........ 22
Figure 11. Manufacturer: Operational Technology Writes Receive, Make, Assemble, and Ship Event Records........ 24
Figure 12. Acquirer: Critical Infrastructure CI-001 Writes Receive and Employ Event Records........ 24
Figure 13. Acquirer: Operational Technology Manufacturer Invokes Traceback........ 26
Figure 14. Acquirer: Critical Infrastructure CI-001 Invokes Traceback........ 27

Figure 15. Sustainment Chain Opportunity for Future Research 39
Figure 16. Overview Class Diagram for Traceability Record 48
Figure 17. Traceability_Record Attribute Structure 49
Figure 18. Key_Value_Pair Attribute Structure 51
Figure 19. Traceability Link Attribute Structure 52
Figure 20. Supplemental Link Attribute Structure 53
Figure 21. Make Record Attribute Structure 55
Figure 22. Assemble Record Attribute Structure 56
Figure 23. Ship Record Attribute Structure 57
Figure 24. Receive Record Attribute Structure 58
Figure 25. Employ Record Attribute Structure 59

Executive Summary

This paper introduces a meta-framework designed to enhance traceability across diverse supply chains by enabling structured recording, linking, and retrieval of traceability data. Through trusted data repositories, stakeholders can access supply chain information needed to verify product provenance, demonstrate compliance with external stakeholder requirements and contractual obligations, and assess supply chain integrity. The framework establishes several key principles to ensure visibility, reliability, and integrity in supply chain traceability:

- **Common Data and Ontologies:** Stakeholders are empowered to establish traceability consistency, ensuring that data remains structured, interoperable, and understandable across industries.
- **Trusted Repositories and Ecosystems:** The Meta-Framework supports the use of secure, trusted data repositories within industry ecosystems to manage traceability records.
- **Traceability Record Model:** Traceability is built from records created from supply chain events (e.g., manufacturing, shipping, receiving). These are linked using cryptographically verifiable connections to form traceability chains—sequentially linked records that allow stakeholders to validate product history and movement across the supply network.

Offering a scalable solution for improving traceability across industry sectors, the Meta-Framework enables organizations to exchange required supply chain data securely. As global supply chains grow more complex, this approach strengthens supply chain integrity, supports fulfillment of external obligations (e.g., legal, contractual, operational), and fosters stakeholder trust.

Crucially, the design allows organizations to share only the traceability data necessary for external validation, while retaining control over sensitive intellectual property and proprietary information. This principle of controlled disclosure balances transparency with confidentiality, helping stakeholders mitigate business risk while promoting accountability.

Successful implementation depends on effective ecosystem governance, risk-informed identity management, and data integrity safeguards. Readers are advised to consult Appendices C and G for additional guidelines and security considerations.

1. Introduction

The security, resilience, and assurance of national manufacturing and critical infrastructure[1] supply chains are vital to maintaining economic strength and national security. As global supply chains become increasingly complex and interdependent, ensuring the traceability of components, materials, and products is essential for mitigating risks, preventing counterfeit products, and supporting external stakeholder requirements, such as legal, contractual, and industry-defined obligations.

The importance of traceability is also reflected in national guidelines, including Cybersecurity Supply Chain Risk Management for Systems and Organizations, NIST Special Publication 800-161r1 [1]. Pedigree and provenance data can help meet these external obligations while supporting continuous supply chain risk monitoring and lifecycle assurance.

From a research perspective, traceability is often viewed within the broader context of supply chain transparency. In Supply Chain Transparency: A Bibliometric Review and Research Agenda [2], the authors identify "Cluster 5: Supply Chain transparency for traceability" as closely related to this NIST IR's goals. However, these existing studies primarily focus on organizational processes and do not sufficiently address cross-ecosystem traceability. The Meta-Framework addresses this gap and enables traceability across diverse manufacturing environments, allowing authorized stakeholders to discover, retrieve, and interpret supply chain event data.

Despite the importance of traceability, many organizations struggle with fragmented data storage, inconsistent data models, and a lack of interoperability between supply chain participants. Traditional supply chain management practices often rely on data within siloed systems, making it difficult for stakeholders to verify product authenticity, assess risk, or meet external accountability requirements [3].

The Meta-Framework provides a structured approach to supply chain traceability, enabling interoperable and secure data exchange between organizations. It is designed to address a wide range of traceability drivers, including:

- **External Stakeholder Accountability and Compliance:** Organizations may need to demonstrate product origin and conformance to standards or obligations defined by external stakeholders, such as customers, industry groups, or contractual agreements.
- **Counterfeit Prevention and Stakeholder Assurance:** Manufacturers, consumers, and partners may require assurance of product authenticity and that sourcing complies with agreed requirements.
- **Interoperability and Supply Chain Risk Management:** Supply chain participants, including suppliers, integrators, and government bodies, may require visibility into upstream and downstream risk factors via trusted traceability mechanisms.

Many organizations already maintain internal traceability systems (e.g., digital thread solutions) to manage lifecycle data and improve operations. The Meta-Framework is designed to work in

[1] U.S. critical infrastructure as defined by DHS CISA: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

concert with these systems, allowing organizations to publish only the traceability data necessary to support external validation while maintaining control over sensitive intellectual property and proprietary information. This approach integrates reporting and assurance capabilities into operational workflows rather than being implemented as separate systems.

1.1. Supply Chain Traceability Needs and Challenges

Modern manufacturing supply chains span a complex web of globally distributed stakeholders, processes, and systems. While traceability is increasingly vital for reducing risk and demonstrating compliance, many organizations lack the mechanisms to align their internal traceability practices with external reporting needs.

A major barrier is the absence of a unifying mechanism for linking traceability records across disparate ecosystems. Supply chain participants typically maintain internal records, such as process logs, shipment details, quality assurance reports, or production batch data, in formats tailored to their operational needs. While these records support internal operations, they can create challenges when organizations are asked to share or verify data across boundaries. In some cases, these records may include sensitive business or contextual information, which must be carefully managed to avoid exposing proprietary or privacy-relevant details. These limitations reduce visibility, delay verification, and introduce risk in scenarios such as product recalls, supply chain traceability reviews, or multi-party coordination across organizational boundaries.

What is needed is an interoperable framework that enables traceability information to be securely shared, discovered, and validated across diverse systems. By providing a consistent structure and linking mechanism, the Meta-Framework addresses this need without requiring supply chain participants to compromise their internal data models, proprietary information, or operational autonomy.

Figure 1 illustrates how a component's original manufacturer may be separated by multiple supply chain tiers from the final product acquirer, making it difficult to validate product history without a structured traceability framework. As supply chains become more distributed and complex, the need to securely link events across organizations and ecosystems grows more urgent.

- Supply chain stakeholders, such as product acquirers, customers, or oversight entities, may request traceability information to validate a product's origin, authenticity, or alignment with conformance expectations. ~~These~~ Stakeholder expectations may stem from their internal risk management practices, customer assurance requirements, or externally defined standards related to security, sustainability, or trade policies.
- Organizations that integrate components from multiple suppliers may need to collect traceability data from earlier-stage participants to verify product lineage, assess risk, or respond to incidents. This process can involve sensitive information, such as location data, batch or shift records, or certifications tied to specific manufacturing conditions. Without consistent governance and privacy protections, such data collection can raise

concerns about overcollection, unintentional re-identification, or inconsistent treatment of proprietary or personal data.

- Later-stage participants in the supply chain may need to reference traceability data from prior events to assess exposure to recalls, defects, or vulnerabilities.

The Meta-Framework is designed to address these visibility and interoperability gaps by enabling traceability records to be securely linked across ecosystems, with appropriate controls for privacy and access. This creates a foundation for trusted data exchange while reducing the risks associated with fragmented traceability practices.

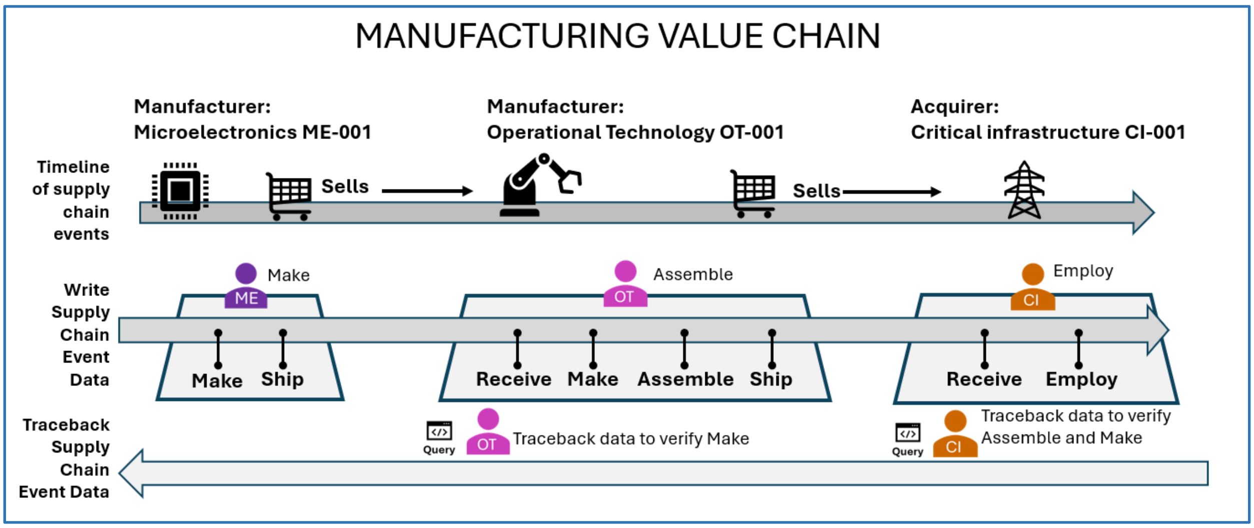

Figure 1. Challenges of Component or Assembly Verification Across Stakeholder Tiers

1.2. Approach

The Meta-Framework addresses the key traceability challenges outlined above by establishing a structured, interoperable model for recording, linking, and retrieving supply chain data across organizational and technical boundaries. It builds on foundational work, including NIST IR 8419 [3], NIST SP 800-161r1 [1], and the "Manufacturing Supply Chain Traceability with Blockchain-Related Technology: Reference Implementation" project [4], but generalizes those findings into a technology-agnostic and governance-neutral framework.

The Meta-Framework defines common principles and data structures that can be applied across a variety of ecosystems and storage technologies. This approach enables traceability records to be created consistently and exchanged securely, regardless of the underlying systems used by participants.

At its core, the Meta-Framework describes a methodology for capturing supply chain events as traceability records. These records combine fixed data elements, used to ensure consistency across all implementations, with variable data blocks that can be tailored to the needs of specific industries or event types. Once recorded in trusted data repositories governed by stakeholder-defined ecosystems, these records can be securely linked to one another to establish a verifiable traceability chain. This enables stakeholders to verify provenance and pedigree without exposing proprietary systems or internal data.

The framework also includes support for essential trust mechanisms, including authentication, access control, and cryptographic validation, to ensure that traceability data remains accurate, protected, and tamper-evident throughout its lifecycle. Later sections of this report, including Sec. 3 and the Appendices, describe implementation considerations and technical details supporting this approach.

1.3. Goals

The primary objectives of the Meta-Framework are:

- **Enhance Supply Chain Transparency:** Provide a structured approach for recording and linking traceability data to improve visibility across supply chain ecosystems.
- **Ensure Data Interoperability:** Establish a common data model enabling integration across industry participants, ecosystems, and external stakeholders.
- **Strengthen Product Authenticity and Provenance Verification:** Support mechanisms for stakeholders to verify the origin and lineage of components, materials, and finished products.
- **Support External Traceability Requirements:** Enable organizations to meet traceability requirements driven by contracts, standards, or applicable regulations through a structured data-sharing model.
- **Improve Security, Data Integrity, and Privacy Considerations:** Define best practices for authentication, access control, and cryptographic validation to ensure that traceability data remains accurate, tamper-evident, and appropriately scoped to minimize exposure of sensitive information.
- **Facilitate Ecosystem Governance:** Allow industry stakeholders to define governance rules that align with obligations and external expectations while ensuring the ability to perform traceability.

1.4. Audience

This document is intended for stakeholders responsible for designing, operating, or participating in supply chain traceability ecosystems. These may include industry consortia or sector-based working groups that define common data requirements and provide oversight for ecosystem governance, as well as technology providers and system integrators tasked with building the infrastructure to support traceability records, trusted data repositories, and participant interfaces.

The Meta-Framework is also intended to support large manufacturers and supply chain primes that may act as ecosystem anchors, encouraging adoption across their supply networks. In addition, small and medium-sized manufacturers (SMMs) and component suppliers, who may not have the resources to develop standalone solutions, would benefit from interoperable ecosystems built using the Meta-Framework.

This document provides architectural guidelines and conceptual building blocks to support organizations seeking to implement cross-organizational traceability in alignment with industry-defined and contractual requirements. It may also be of interest to standards bodies and researchers investigating scalable, secure traceability across complex manufacturing environments.

1.5. Considerations and Limitations

While the Meta-Framework is designed to enhance traceability across diverse supply chain ecosystems, there are inherent risks and limitations that must be addressed during implementation. These include:

- **Privacy Risks:** These are particularly prevalent in trace-forward use cases where high-assurance identifiers could be linked to individuals or sensitive operational data (see Appendix C.2–C.2).
- **Interoperability Gaps:** Ecosystem-specific governance and data models may introduce semantic or structural misalignment between participants.
- **Identity and Access Management Challenges:** Implementing consistent and secure authentication mechanisms across diverse ecosystems can be technically complex (see Appendix C.1).
- **Trust and Data Integrity Dependencies:** Traceability relies on the integrity of individual contributors and the infrastructure of trusted data repositories (see Appendix G).

These challenges do not diminish the framework's value but emphasize the need for robust ecosystem governance, the adoption of privacy-respecting architectures, and alignment with emerging standards and best practices.

2. Meta-Framework Overview

The Meta-Framework enhances traceability across diverse manufacturing sectors by providing a structured approach to recording, linking, and retrieving traceability data required by industry and external stakeholders. This information supports the validation of product pedigree and provenance while allowing flexibility to meet varying operational and compliance requirements. Designed to be industry-agnostic, the Meta-Framework can be adopted across a wide range of manufacturing supply chains, regardless of sector-specific technologies, products, or participants. The core components of the Meta-Framework include:

- **Data Model and Ontologies:** The Meta-Framework includes a flexible data model to enable tailored implementations for industry and externally defined traceability needs. Stakeholders can establish data dictionaries and ontologies that ensure syntactic and semantic consistency for traceability data. By allowing stakeholders to align with standards organizations and external stakeholders as needed, the framework ensures that traceability data is interoperable, comprehensible, and actionable for stakeholders across the supply chain.
- **Traceability Records:** At the heart of the Meta-Framework are traceability records, which document essential supply chain event information about product pedigree and provenance at various stages or events within the supply chain. These records are stored in trusted data repositories, ensuring accessibility, integrity, and verifiability by authorized stakeholders.
- **Traceability Links:** The Meta-Framework uses traceability links to connect individual traceability records into a traceability chain. These verifiable links enable stakeholders to follow the lineage of a product or component over time and across trusted data repositories managed by organizations within ecosystems.
- **Trusted Data Repositories and Ecosystems:** The Meta-Framework advocates for using trusted data repositories within managed ecosystems to store and manage traceability records securely. These repositories are crucial to maintaining the integrity and trustworthiness of traceability data throughout its lifecycle.

2.1. Traceability Records and Core Components

The Meta-Framework organizes traceability data into a modular and extensible model that supports diverse supply chain implementations. It defines core components that guide how traceability records are created, securely stored, and linked to one another within trusted repositories. This model enables cross-organization data exchange while preserving data authenticity, integrity, and compliance across heterogeneous ecosystems.

To support verifiable traceability, the Meta-Framework assumes that each traceability record corresponds to a uniquely identifiable item or product. Ecosystems must ensure that a persistent identifier, whether for a physical component, digital object, or virtual asset, is assigned and can be reliably associated with the tracked item throughout its lifecycle. This identifier forms the basis of the cyber-physical link and is critical for ensuring continuity and validation across traceability chains.

The model comprises fixed data elements that provide a consistent structure for all traceability records and variable data blocks that accommodate industry- or event-specific attributes. Traceability links connect these records to form a verifiable sequence of supply chain events or "traceability chain" that enables validation of product pedigree across participating ecosystems. A detailed breakdown of this data model is provided in Sec. 3, with implementation examples in Appendix F.

Figure 2 illustrates the general construct of a traceability record as it might be stored in a trusted data repository. The Meta-Framework allows traceability records to be encapsulated within a broader transaction or container record, which may include repository-specific metadata such as authentication data or contractual compliance fields. The "Trusted Data Store" shown in Fig. 2 is implementation-agnostic, allowing organizations to adopt storage technologies that best suit their operational needs while preserving secure access to traceability records.

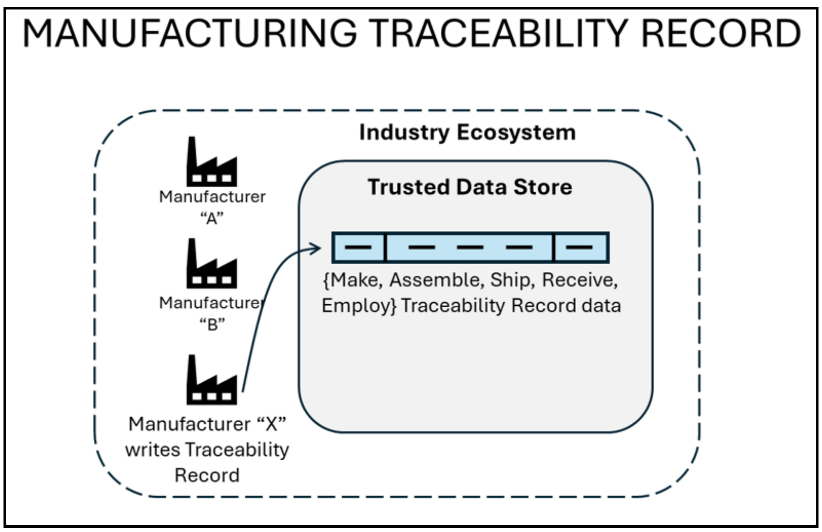

Figure 2. General Construct of Traceability Records

Figure 3 shows how traceability links connect individual traceability records to form traceability chains. These links enable stakeholders to trace the movement and transformation of components across different organizations, ecosystems, and industries. The diagram expands on the link between two records and highlights how the Traceability Link references the predecessor Traceability Record via an Ecosystem Interface.

The Meta-Framework provides common definitions for data structures, linking mechanisms, and validation approaches to ensure seamless interoperability. By incorporating consistently formed traceability links, organizations can create continuous and verifiable chains of custody across complex supply networks. These links reference predecessor records to maintain product lineage and support traceability across organizational boundaries. Combined with tamper-evident data integrity practices, the framework ensures traceability records can be trusted even when retrieved from different ecosystems.

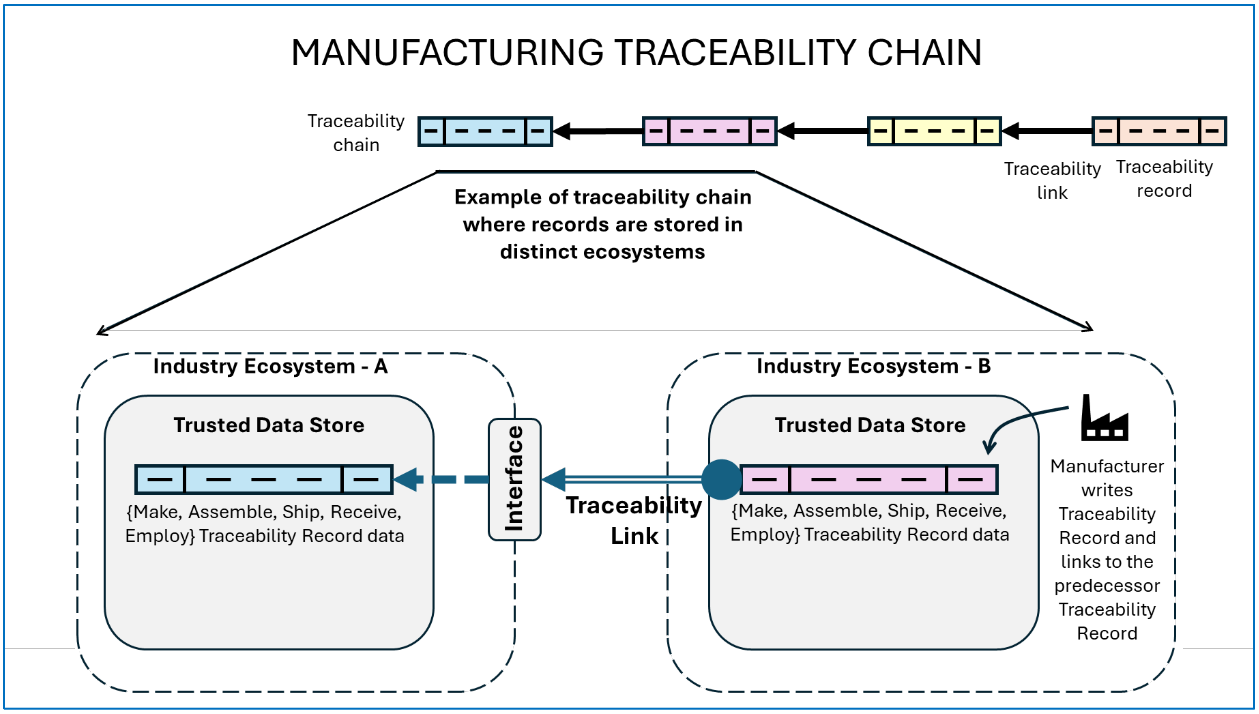

Figure 3. General Construct of Traceability Chain

2.2. Trusted Data Repositories and Ecosystems

Trusted data repositories form the foundation of the Meta-Framework by ensuring that traceability records are securely stored, accessible to authorized stakeholders, and managed according to governance policies. These repositories operate under ecosystem governance frameworks that define access control, data retention policies, and authentication mechanisms.

2.2.1. Controlled Access and Data Retention

Trusted data repositories must implement technical and procedural safeguards to ensure traceability records remain protected, verifiable, and accessible throughout their lifecycle. Key capabilities include:

- Authentication mechanisms that verify the identity of stakeholders either accessing or submitting traceability records.
- Access control mechanisms that define and enforce who can read, write, or manage traceability records, protecting supply chain data from unauthorized use.
- Data retention policies that specify how long traceability records must be stored to meet operational, contractual, and compliance obligations.

Together, these practices help maintain traceability records' integrity, availability, and long-term reliability. Appendix C provides further details on controlled access mechanisms.

2.2.2. Ensuring Data Integrity

Maintaining the authenticity and integrity of traceability records is critical for enabling trustworthy verification across supply chains. The Meta-Framework supports cryptographic validation techniques such as hash-based integrity checks, ensuring traceability records remain unaltered after creation. These mechanisms help protect against tampering and unauthorized modification while supporting secure interoperability across ecosystems. Appendix C and Appendix G provide additional technical and privacy-related guidelines.

2.2.3. Ecosystem Governance and Role in the Meta-Framework

Ecosystem governance defines the policies and rules that regulate how traceability records are created, stored, and accessed. Governance frameworks also define membership criteria, compliance obligations, and participant responsibilities, ensuring that traceability principles are consistently applied across the ecosystem.

Trusted data repositories serve as the foundation of the framework; however, their security, data retention, and governance practices must be carefully managed to mitigate risks such as unauthorized access, inconsistent record retention, and breakdowns in traceability continuity. Appendix G provides additional guidelines on Ecosystem governance considerations.

2.3. Traceability Chain Across Supply Chain Ecosystems

The Meta-Framework enables the construction of verifiable traceability chains that span multiple ecosystems, allowing stakeholders to follow the history of components and materials as they move through global supply networks. These chains are formed by linking traceability records through cryptographically verifiable references, providing continuity of product lineage even across organizational and technological boundaries.

By supporting consistent linking and retrieval mechanisms, the traceability chain enhances visibility into supply chain activity and enables stakeholders to validate critical supply chain events. This supports many use cases, including compliance auditing, counterfeit detection, and risk management, while strengthening supply chain security and transparency.

2.4. Example Traceability Chain Across Ecosystem Boundaries

Figure 4 illustrates a simplified but notional multi-tier supply chain scenario involving three stakeholders: a microelectronics manufacturer (ME-001), an operational technology supplier (OT-001), and a critical infrastructure acquirer (CI-001). The diagram highlights the progression of supply chain traceability events, including make, ship, receive, assemble, and employ, and the traceability records written at each stage by member organizations of different ecosystems.

Traceability records are captured in trusted data repositories governed by each ecosystem. As the product moves through the supply chain, each event appends to the traceability chain by referencing its predecessor using traceability links. These links allow stakeholders to “trace back” through recorded events across ecosystems to validate component lineage, verify product authenticity, and support traceability requirements defined by industry standards, contractual obligations, or applicable regulations.

This example visually demonstrates the Meta-Framework’s core principles for record creation, ecosystem-governed data management, and verifiable end-to-end traceability across organizational boundaries. Ecosystem-governed data management furthers the core principles in the illustration by highlighting the use of a variety of technologies in implementation, as is the purview of each Ecosystem.

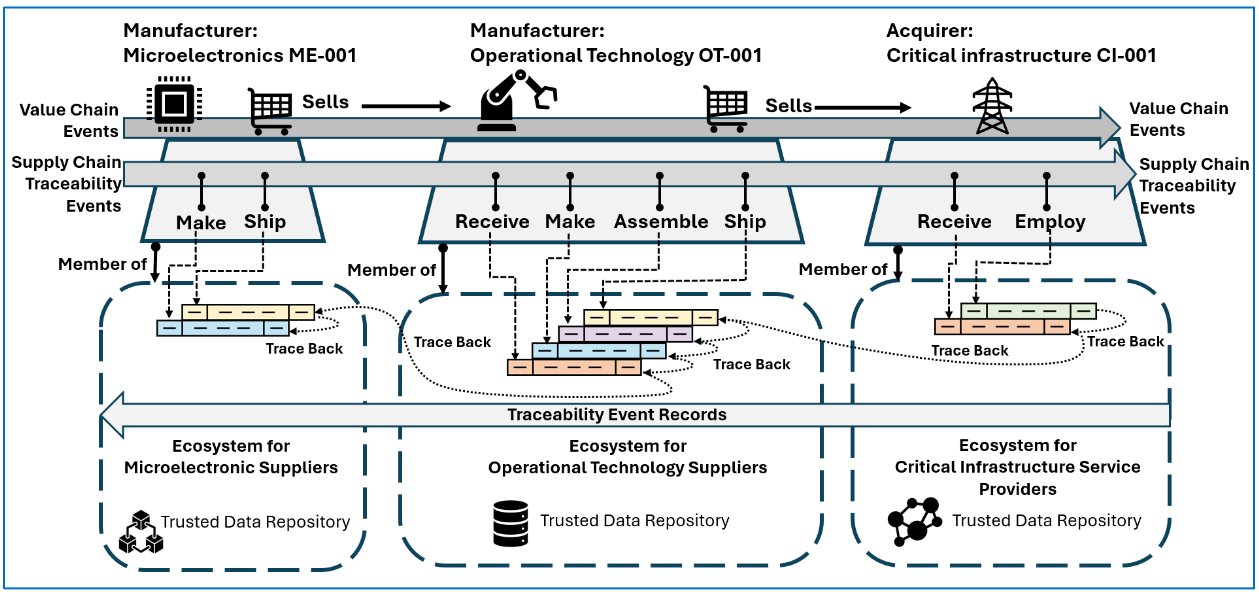

Figure 4. Value and Supply Chain Traceability Events Across Ecosystems

3. Meta-Framework Data Model

3.1. Traceability Records Overview

This section introduces the data model used to represent traceability records within the Meta-Framework. Each record captures a discrete supply chain event, such as manufacturing, shipping, receiving, assembling, or deploying, and includes structured fields to support consistent data representation, verifiable linkages, and interoperability across ecosystems. These records form the basis of traceability chains and are designed to meet traceability requirements from industry, standards, contracts, or applicable policies.

3.2. Traceability Record Structure

Each traceability record consists of:

Table 1: Traceability Record Description

Record Element	Description
Record Identifier	A unique identifier for the traceability record, ensuring that each event entry is uniquely identifiable within an ecosystem.
Event Occurrence Timestamp	The date and time the event occurred in the supply chain process.
Event Recorded Timestamp	The date and time the traceability record was officially recorded in a trusted data repository.
Record Type Identifier	A code indicating the subclass of traceability event (e.g., make, assemble, ship, receive, employ) for this record.
Organization Identifier	A unique identifier representing the organization responsible for generating a traceability event. This typically refers to a publicly identifiable business entity such as a manufacturer, supplier, or logistics provider. Organization identifiers are not intended to include personally identifiable information and should reflect entities participating in the supply chain ecosystem.
Organization Subunit Identifier	An identifier representing a specific operational unit, department, facility, or division within an organization where the traceability event occurred. Subunit identifiers provide traceability granularity and should be derived from internal organizational structures without referencing individual employees or private data.
Tracked Entity Identifier	A unique identifier is assigned to the instance(s) produced by or affected by the event. This identifier enables traceability and verification of an asset's role within the supply chain. Depending on the event type, this may represent a physical product, a digital identifier, a shipment reference, or an installed system.
Traceability Links	A set of zero or more traceability link objects providing references to precursor traceability records related to the event. These links establish lineage and historical tracking between supply chain events.

Record Element	Description
Tracked Entity Data Type Identifier	A standardized value defined by industry consortia, standards organizations, or external compliance authorities that categorizes the expected schema for the tracked entity data and supplemental data. This identifier ensures that traceability records follow structured definitions, aligning with sector-specific compliance, manufacturing standards, and operational requirements.
Tracked Entity Data	A variable-length data structure containing key-value pairs that provide detailed event-specific data. The requirements for this field are defined in the ecosystem data dictionary entry based on the Event Type Identifier. This block captures the minimum required data for verifying product provenance, operational status, or compliance.
Supplemental Data	A set of zero or more supplemental link objects that provide references to other data sources related to the event. These references may include certifications, test reports, quality inspection results, operational logs, audit summaries, compliance attestations, or digital representations for engineering models or configuration baselines. Unlike traceability links, these references may not be persistent or universally accessible, as they may reside in stakeholder systems with gated access.

These elements ensure consistency across ecosystems while allowing flexibility for industry-specific extensions. Technical details regarding serialization formats and cryptographic validation are further discussed in Appendix F and Appendix G.

3.3. Traceability Record Subclasses

The Meta-Framework defines five initial event types, each captured as a subclass of the generic traceability record:

Table 2: Record Subclass Descriptions

Subclass	Description
Make Record	Captures the creation of a product or component with supplemental linking to raw material or prior assembly data when applicable.
Assemble Record	Represents the combination of multiple components into a new product, linking to preceding make, assemble, or receive events as applicable.
Ship Record	Documents the transfer of materials or products between supply chain entities, linking to the originating make or assemble event.
Receive Record	Captures the receipt of a shipment from another entity and links to the corresponding ship event.
Employ Record	Records the deployment or activation of a product within an operational environment, typically linking to a receive or assemble event.

These initial subclasses ensure that traceability records capture key supply chain milestones while preserving flexibility for industry-specific implementation. The full class structure and implementation details are provided in Appendix F.

Note: Shipment and receipt events may involve individuals (e.g., drivers, warehouse staff), but the Meta-Framework does not require or encourage the inclusion of personally identifiable information (PII) in traceability records. Ecosystems should avoid capturing direct personal identifiers (e.g., names, license numbers) unless clearly justified by operational or legal needs. Where traceability of roles is necessary, pseudonymous identifiers or event metadata may be used to maintain accountability while protecting privacy. For additional guidance, see Appendix C.

Figure 5 depicts the traceability record subclasses in the context of their traceability link relationships. These subclasses represent distinct supply chain events in the progression along manufacturing supply chain activity timelines.

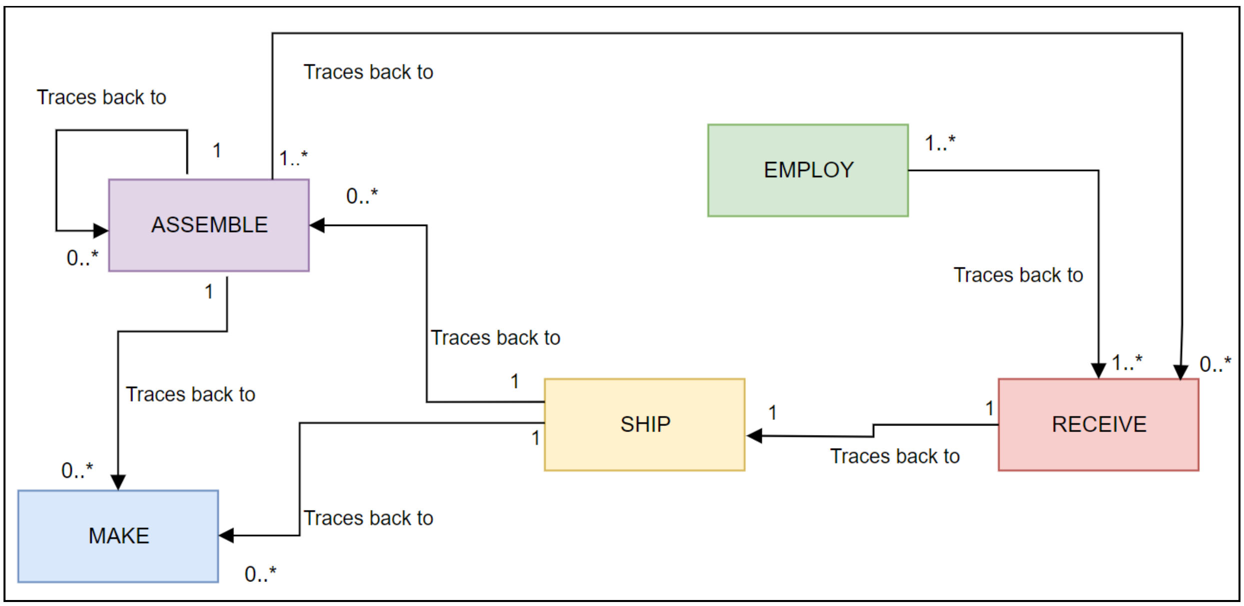

Figure 5. Overview Class Model

3.4. Traceability Links and Supplemental Data References

Traceability links form the foundation of the Meta-Framework's interoperability model, connecting individual records to maintain an unbroken traceability chain. These links ensure that stakeholders can track a product's lineage as it moves through the supply chain. A ship record links to the make or assemble record that created the product. A receive record links to the corresponding ship record, maintaining visibility into material transfers. When an assemble record is created, it may reference one or more receive records to document the sources of its components. Employ records, used for deployment or activation, typically reference the last known assemble or receive record to maintain visibility into final product usage.

Supplemental data references provide additional, non-mandatory details that stakeholders may request for compliance or risk assessment purposes. Unlike traceability links, which are integral to product lineage, supplemental data references are external records that provide further validation, such as certifications, test reports, quality inspection results, operational logs, audit summaries, compliance attestations, or digital representations for engineering models or configuration baselines. Appendix F provides a detailed breakdown of traceability links and supplemental data references, including possible structures and attributes.

3.5. Ensuring Data Integrity and Interoperability

The Meta-Framework ensures the integrity and interoperability of traceability records across supply chain ecosystems through a combination of consistent data models, cryptographic validation, and controlled access mechanisms. These principles establish a foundation for supply chain transparency and security.

3.5.1. Common Data Models

The Meta-Framework defines a consistent schema for traceability records to ensure uniform data representation across industries. By structuring traceability records with consistent attributes and relationships, stakeholders can interpret and exchange traceability data reliably across different ecosystems. An example schema and attribute structures of traceability records are detailed in Appendix F.

3.5.2. Traceability Chain and Data Integrity Mechanisms

The trust mechanisms within the Meta-Framework connect traceability records into a traceability chain, allowing stakeholders to validate and trace components back through the supply chain. As shown in Fig. 6, each record is linked to its predecessor, forming an immutable record of product lineage.

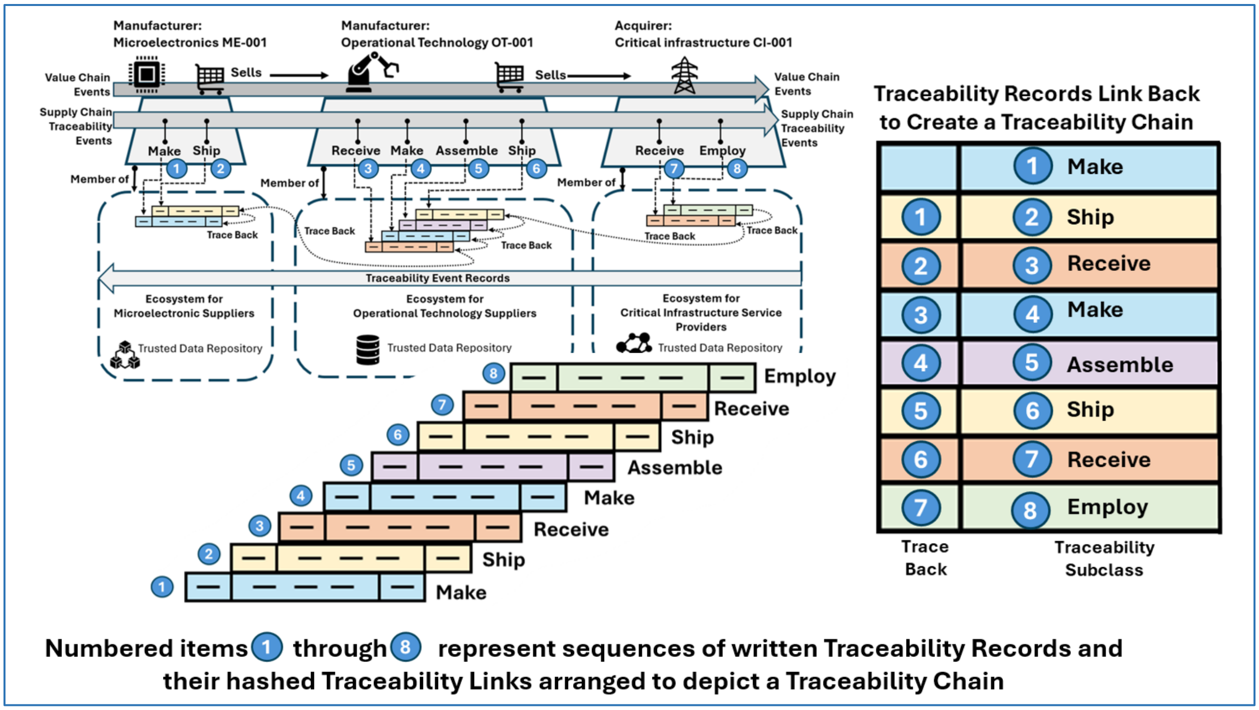

Figure 6: Traceability Chain through Ecosystems

Traceability links serve as the foundational structure for maintaining trust within supply chains by:

- Associating a traceability record with its predecessors using a linking mechanism that references earlier events.
- Storing cryptographic hash values of linked records to ensure data integrity and detect unauthorized modifications.
- Allowing query-based retrieval of previous records, ensuring efficient access across distributed repositories.

These mechanisms ensure that stakeholders can validate the authenticity of supply chain events while maintaining an unbroken record of product lineage.

3.5.3. End-to-End Trust and Component Validation

The Meta-Framework enables end-to-end trust, allowing stakeholders to verify the integrity and authenticity of products using traceability data. Figure 7 illustrates how a manufacturer or acquirer can use traceability records and traceability links to verify the authenticity of individual components.

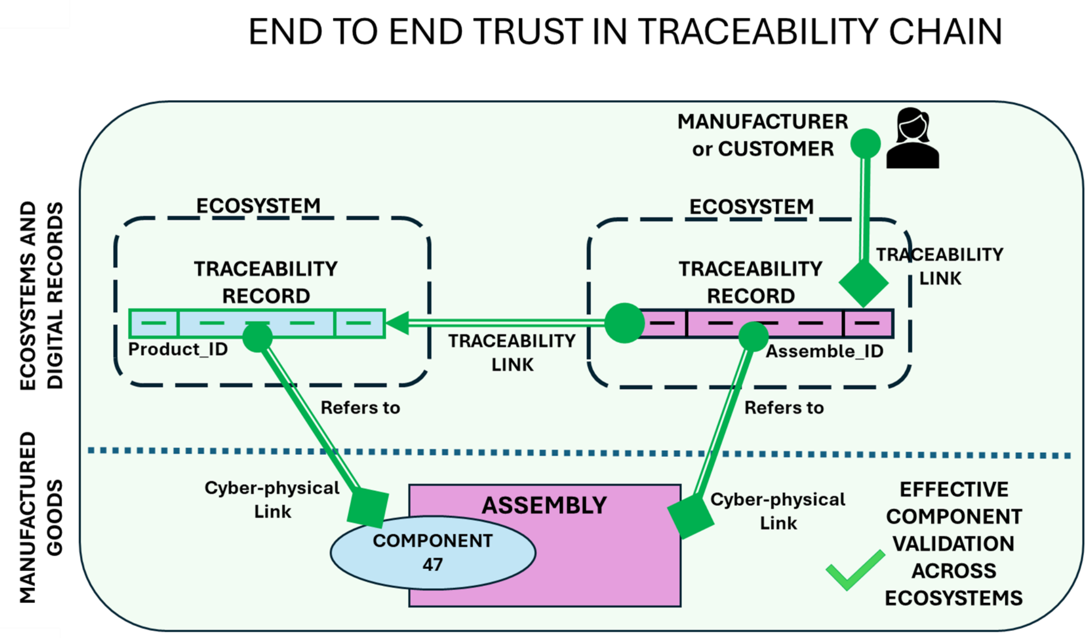

Figure 7: End-to-End Trust Enables Component Validation

By leveraging traceability records and cyber-physical links, organizations can:

- Validate a component's provenance using traceability records and associated hashes.
- Ensure correct cyber-physical linkages between traceability records and real-world items.
- Maintain confidence in the security and reliability of supply chain transactions.

The cryptographic validation and linking mechanisms within the Meta-Framework provide the necessary assurances to mitigate traceability risks while supporting industry compliance and security requirements. Additional cryptographic considerations for data integrity validation are provided in Appendix G.

3.5.4. Notional Traceback Scenario

The notional traceback scenario in Fig. 7 starts with a manufacturer or end customer possessing a traceability link. That traceability link is used to retrieve the corresponding assemble record. The assemble record, in turn, has a cyber-physical link (Assemble_ID) to refer to the physical assembly. The assemble record also has a Traceability Link to the predecessor make record corresponding to Component 47, which has a cyber-physical link, this time to Component 47. Thus, all the relevant traceability records can be retrieved by following the traceability links, including the applicable cyber-physical links. The traceability records include hashes for the predecessor traceability records, so the data integrity is assured for the whole traceability chain. The cyber-physical links (e.g., Assemble_ID, Product_ID) are unique, so the customer, for example, can trace back along the traceability chain and be assured of correct cyber-physical links to the corresponding manufactured products.

3.5.5. Controlled Access and Authentication

Access to traceability records must be managed to ensure that only authorized stakeholders can retrieve supply chain data. The Meta-Framework supports:

- **Access Control Policies** to restrict data retrieval based on requirements from industry, standards, contracts, or applicable policies.
- **Authentication Mechanisms** to verify users accessing traceability records.
- **Traceability Link-Based Querying** to allow users to retrieve data without requiring direct authentication to upstream ecosystems.

Further details on cryptographic validation, access control, and implementation considerations are provided in Appendix C.

4. Meta-Framework Use Cases

The Meta-Framework use cases illustrate how the traceability goals in Sec. 1.3 are achievable. The use cases are:

- **Recording Supply Chain Event Data:** This involves capturing and storing traceability records, which include supply chain event data, traceability links, and supplemental links as applicable. These records document key events within the supply chain, ensuring that essential information about components, assemblies, or other manufactured products is securely recorded. A recorded traceability event establishes a traceability link.
- **Tracing and Retrieving Traceability Records:** The Meta-Framework enables stakeholders to trace back through the traceability records to construct a comprehensive traceability picture. This process allows for retrieving relevant supply chain event data and providing supporting information to verify the pedigree and provenance of components, assemblies, or other manufactured products.

In this section, sequence diagrams capture the Meta-Framework use cases as interactions between stakeholders and interfaces, illustrating the recording and retrieval of traceability records.

A traceability chain is formed by linking traceability records across supply chain ecosystems, establishing an unbroken sequence of events. This ensures stakeholders can validate a product's lineage from its initial creation (make) to its final deployment (employ). Section 3.5 and Appendix G provide more details on traceability chain construction and validation.

Figure 8 maps thumbnails of the sequence diagrams to value and supply chain points. The sequences are examples of how recording and retrieving traceability records may align with the progression of business interactions, moving products between providers and acquirers. In representing the traceability records sequentially, in the context of the overall supply chain, the diagrams anchor discrete instances of events to a linked status.

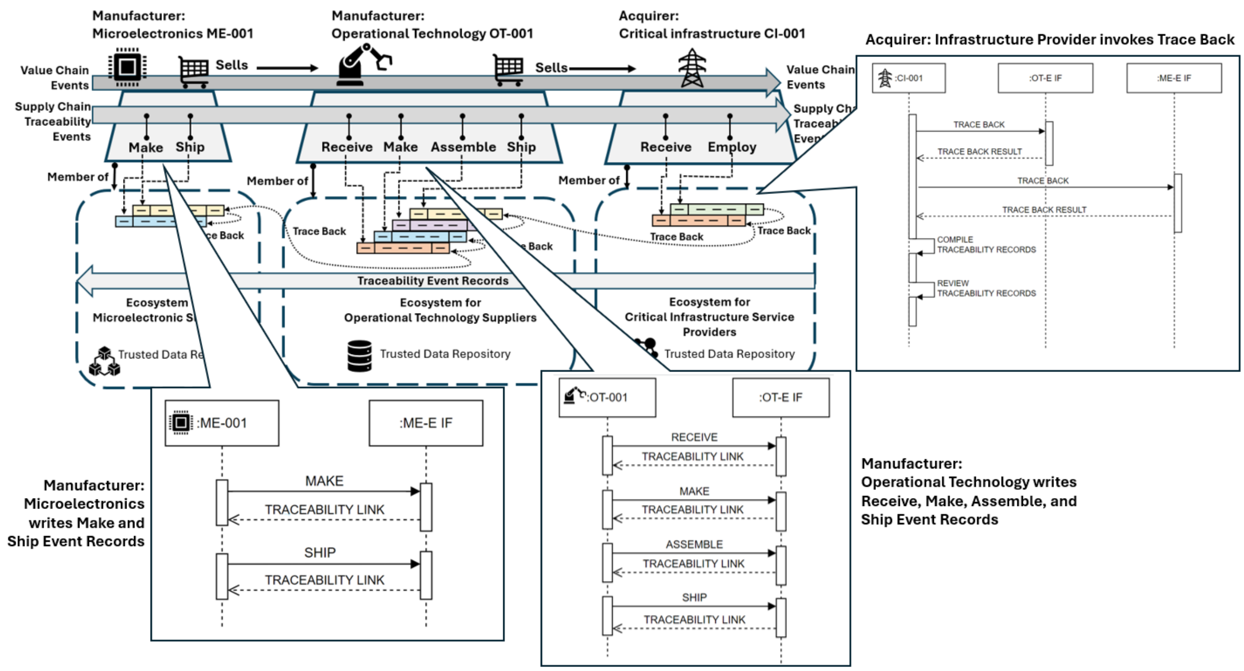

Figure 8. Sequence Diagrams in the Context of Supply Chain Events

Figure 9 provides examples that aid in the interpretation of the sequence diagrams that follow. Those examples include the actions written for an ecosystem from traceability events (e.g., make, assemble, ship, receive, employ) as examples for demonstrating traceability links, tracebacks, and traceback results. Ecosystem interfaces facilitate controlled access to trusted data repositories, ensuring that stakeholders can write and retrieve traceability records securely. The role of these interfaces in managing ecosystem interactions is described in detail in Sec. 2.4.

Three example ecosystem interfaces are also depicted for a microelectronics ecosystem, an operational technology ecosystem, and a critical infrastructure ecosystem. The actors are as follows:

- **Microelectronics Manufacturer, designated as ME-001.** This actor is a manufacturing concern and a stakeholder in the advantages of supply chain traceability.
- **Micro-electronics Ecosystem, designated as ME-E.** This actor is responsible for providing an accessible interface to both members and non-members of its ecosystem.
- **Operational Technology Manufacturer, designated as OT-001.** This actor is a manufacturer specializing in the fabrication and assembly of operational technology.
- **Operational Technology Ecosystem, designated as OT-E.** This actor, like ME-E, is responsible for providing accessible interfaces to members and non-members of its ecosystem.

- **Critical Infrastructure Acquirer, designated as CI-001.** This actor is a provider and operator of a critical infrastructure service.
- **Critical Infrastructure Ecosystem, designated as CI-E.** As with ME-E and OT-E, this actor is responsible for providing accessible interfaces to members and nonmembers of its ecosystem.

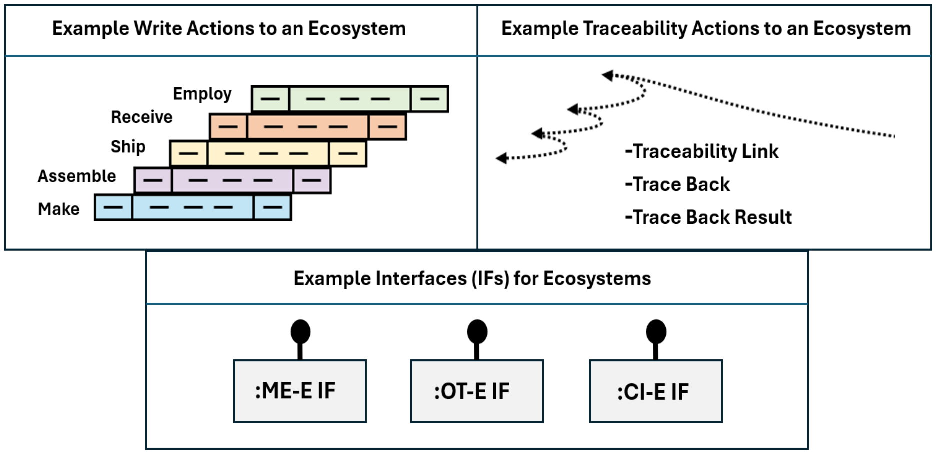

Figure 9. Ecosystem Example Actions and Interfaces

As depicted in the sequence diagrams that follow, an ecosystem's interface minimally addresses:

- Write requests for traceability event records from manufacturing and receiving actors and assign responsibility for these records reaching the trusted data repository and returning a traceability link.
- Traceback requests from acquiring actors and return of traceback results.

Each of the next sections provides a unified modeling language (UML) sequence diagram depicting each example actor's interactions with an interface to read or write data in the interoperable ecosystems. The final two sequence diagrams depict the traceback invoked by the acquirer requesting the records that constitute linked traceability. The diagrams are as follows:

- Sequence Diagram 1: Manufacturer of Microelectronics Make Traceability Event
- Sequence Diagram 2: Operational Technology with Receive, Make, Assemble, and Ship Events
- Sequence Diagram 3: Critical Infrastructure Acquirer with Receive and Employ
- Sequence Diagram 4: Operational Technology with Traceback to ME
- Sequence Diagram 5: Critical Infrastructure Acquirer with Traceback to ME and OT

For this set of sequence diagrams, ecosystem interfaces provide indirect access to the trusted data repository; therefore, the trusted data repository is not explicitly depicted in the diagrams. Depiction, in this way, abstracts out ecosystem-specific choices for the trusted data repository.

Additionally, the Critical Infrastructure Acquirer's position and the Operational Technology Receiver's position are chosen as examples of executing a traceback request.

4.1. Creating and Recording Traceability Data

The following sequence diagrams represent recording supply chain event data via traceability records. Appendix F provides further details on the traceability record schema and event attributes.

4.1.1. Sequence Diagram 1: Manufacturer of Microelectronics Make Traceability Events

Figure 10 illustrates a sequence of traceability events for ME-001. ME-001 is a member of ME-E, the ecosystem for microelectronics. In this sequence, a make event record contains the information that characterizes this make as a unique event. This includes multiple key-value pairs in accordance with the ecosystem's data dictionary and optional supplemental links. At the establishment of the make event in the trusted data repository, the traceability link data is returned to ME-001, depicted by the dashed arrow indicating a return flow.

Likewise, a ship event is written, and its structure and data comply with the ecosystem data dictionary to describe the event, including other contents of the shipment beyond the product written in the make event depicted. In both cases, the traceability links capture the relationship between the make and ship events. This pattern is present for all writes of traceability event records, allowing trusted data repositories to support the traceability chain for the product.

At the completion of this sequence, ME-001 submitted a traceability event for producing a product and a traceability event for shipping the product, and the corresponding traceability links from the ecosystem interface (ME-E IF) were obtained. In the next sequence diagram, the receive event corresponding to the ship event concluding here begins the next series of writes.

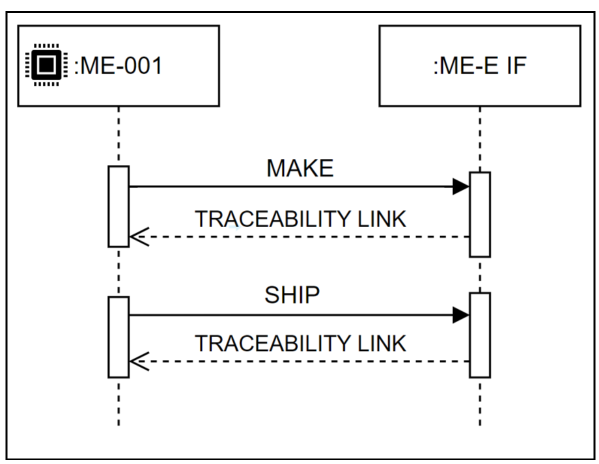

Figure 10. Manufacturer: Microelectronics ME-001 Writes Make and Ship Event Records

4.1.2. Sequence Diagram 2: Operational Tech with Receive, Make, Assemble, and Ship

Figure 11 illustrates a manufacturing sequence in which an entity integrates a received product from another ecosystem with a locally produced component to create an assembled product. The resulting assembly is then prepared for shipment.

This scenario is representative of a manufacturer producing an assembly that consists of:

- A received product that was shipped from another ecosystem (e.g., a microchip).
- A product manufactured internally by the current ecosystem (e.g., firmware or another physical component).

The sequence of events is as follows:

- **Receive Event:** This event establishes a link between the received product and its origin (ME-001's ship event). The traceability link references the ship event from Sequence Diagram 1 (Figure 10), allowing stakeholders to track the received product's provenance. This receive event ensures that its origins remain verifiable when the product is later used in an assembly.
- **Make Event:** This event records the manufacture of a second product (e.g., firmware) by OT-001. Since this product is created within this ecosystem, it does not have a prior traceability link (as make events are originating events). However, it generates a traceability link so that it can be referenced in future supply chain activities.
- **Assemble Event:** This event documents the integration of both the received product and the internally manufactured product into a final assembly. The assemble record includes traceability links to the receive and make events, ensuring a verifiable relationship between the sourced and manufactured components. Since the received product already maintains a backward reference to its shipment event, this creates a complete traceability chain for the assembly, linking it to its components and their respective sources.
- **Ship Event:** This event records the shipment of the completed assembly. The ship record includes traceability links to the assemble event (to show what was built and is being shipped) and the original receive and make events, indirectly linking back to the received product's ship event.

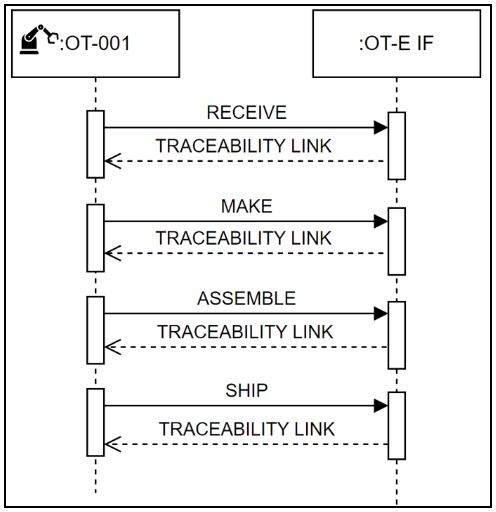

Figure 11. Manufacturer: Operational Technology Writes Receive, Make, Assemble, and Ship Event Records

This concludes Sequence Diagram 2 (Figure 11), with a ship event that will pair with the first traceability link of Sequence Diagram 3 (Figure 12), which is a receive.

4.1.3. Sequence Diagram 3: Critical Infrastructure Acquirer with Receive and Employ

In Fig. 12, Sequence Diagram 3 picks up from Diagram 2 by writing a receive to the ecosystem that CI-001 is a member of. As an acquiring entity, the critical infrastructure provider writes the receive and, upon deciding to employ the product in their environment, writes an employ. As in previous diagrams, each write is followed by a corresponding traceability link returned from their supporting ecosystem. Tapping into the traceability events to support the decision to install the received product is the subject of Sequence Diagram 5 (Figure 14).

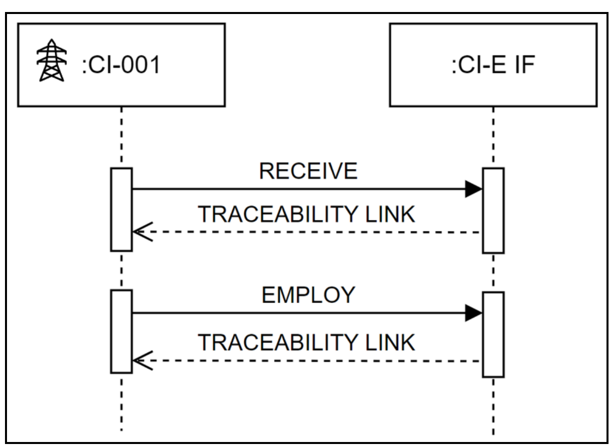

Figure 12. Acquirer: Critical Infrastructure CI-001 Writes Receive and Employ Event Records

4.2. Querying and Retrieving Traceability Records

For cryptographic validation and retrieval integrity mechanisms, refer to Appendix G. During retrieval, a pattern for using the traceability links depicted in the Record Traceability Use Case comes into the sequence. The traceability links are used in the following way to retrieve the corresponding traceability records. These details are omitted from the sequence diagrams:

- To retrieve the traceability record, an Internationalized Resource Identifier (IRI) such as a Uniform Resource Locator (URL) is used to access the interface.
- The traceability link parameters are also stored in the traceability record and passed to the interface. The parameters uniquely identify the traceability record in the destination ecosystem's trusted data repository.
- The implemented interface locates and returns the requested traceability record.
- The retrieved traceability record can then be hashed. That hash is compared to the stored hash in the traceability record to ensure data integrity from the time of original linking to the present time.
- The retrieved traceability record can be used to further retrieve the next traceability record(s). A Traceability Record Set is a group of traceability records related through traceability links.

Two sequence diagrams illustrate, first, a simple retrieval involving one ecosystem and, second, a complicated retrieval involving two ecosystems. The number of ecosystems whose interfaces receive retrieval requests depends on the traceability links referenced and the traceability picture that following the links illuminates. In Sequence Diagram 4, the Operational Technology manufacturer, having received a shipment, inspected the contents and initiated a traceback. In Sequence Diagram 5 (Figure 14), the critical infrastructure acquirer initiates the traceback at the example time of the decision to employ a received assembly. The traceback results are used in both cases to support decision-making about part or assembly integrity.

4.2.1. Sequence Diagram 4: Operational Technology with Traceback to ME

The retrieval process follows a structured approach using traceability links to query trusted data repositories. Each retrieved record undergoes integrity verification using cryptographic hashing. Appendix G provides a detailed breakdown of query parameters, record verification methods, and secure retrieval mechanisms.

Sequence Diagram 4 (Figure 13) illustrates a traceback sequence supporting the acquirer's decision to accept a received microelectronics product for future use in an assembly or otherwise. The acquiring operational technology manufacturer may be in the position of the earlier described activities: the need to validate purchased products' IDs, components, and assemblies, including software when needed, or validate that purchased products are ethically sourced.

In this example, the operational technology manufacturer has received a shipment from a microelectronics supplier. Recall that in Sequence Diagram 2 (Figure 11), the sequence begins with a receive event and a corresponding traceability link. As a matter of business practice, OT-001 may desire to validate the product's source as a condition of accepting the shipment. OT-001 initiates a traceback via the microelectronics ecosystem interface and reviews the traceback result.

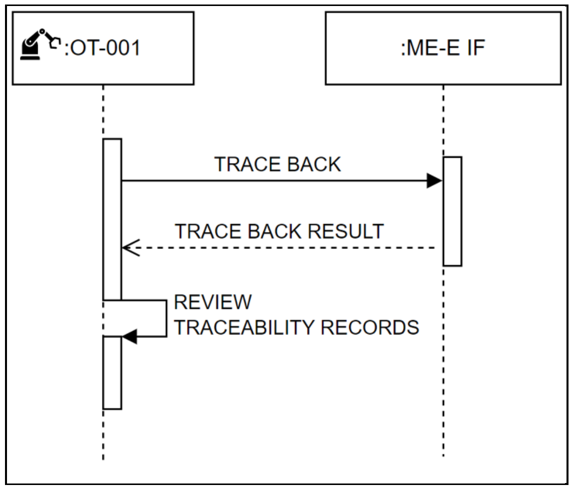

Figure 13. Acquirer: Operational Technology Manufacturer Invokes Traceback

This UML sequence diagram depicts a traceback request from an operational technology manufacturer to its microelectronics supplier via a single ecosystem interface, namely ME-E IF. The traceback results are shown as return transmissions. Additionally, these returned results are directed to a review traceability records function.

4.2.2. Sequence Diagram 5: Critical Infrastructure Acquirer with Traceback to ME and OT

Sequence Diagram 5 (Figure 14) illustrates a traceback sequence supporting the acquirer's decision to put a received product into service. The acquiring critical infrastructure provider may be in the position of either of the two earlier described activities: the need to validate purchased products' IDs, components, and assemblies, including software, or the need to validate that purchased products are ethically sourced.

Actors in this sequence include two interfaces in recognition that for CI-001 to have a complete set of traceability events, traceback requests must be made to their suppliers. The ecosystem interfaces, OT-E IF and ME-E IF, will provide a traceback result. The parameters included in the traceback request enable queries of the indirectly accessed trusted data store via each ecosystem interface. The returned traceback results may be compiled in a linked user presentation to support validation efforts and decision-making about supply chain characteristics. Once compiled, the traceback results may be reviewed in a presentation style.

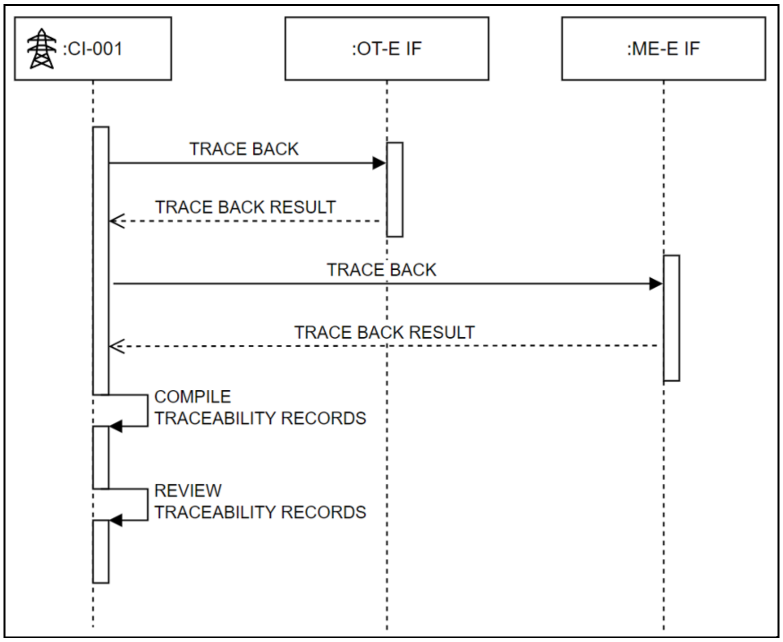

Figure 14. Acquirer: Critical Infrastructure CI-001 Invokes Traceback

This sequence diagram illustrates performing successive traceback requests, compiling retrieved traceability records, and reviewing them for validation. Additionally, it allows for the possibility that ecosystems, whether through dedicated interfaces or external service offerings, may play a role in presenting traceability validation data to stakeholders.

4.2.3. Sequence Diagram Summary

In summary, representative successions of traceability events (make, assemble, ship, receive, employ) are illustrated in Diagrams 1-3. Diagrams 4-5 depict reverse-constructing traceability events through traceability link requests, enabling validation activities.

The roles of multiple traceability ecosystems as trusted data repositories are highlighted through their externally accessible interfaces, demonstrating how traceability information is retrieved across ecosystems. While these five sequence diagrams illustrate fundamental interactions, a real-world supply chain would be significantly more complex. However, the traceability patterns captured here can scale efficiently across diverse supply chain scenarios.

Beyond validation, traceability records retrieved through these processes serve multiple supply chain use cases, including:

- **Informing a Bill of Materials (BOM)**: Organizations can extract traceability records to construct or verify a comprehensive BOM, ensuring that sourced components align with traceability requirements from industry, standards, contracts, or applicable policies.
- **Assisting in Fault Analysis and Root Cause Investigations**: When a component failure or supply chain disruption occurs, traceability records provide historical insight into manufacturing, shipping, and assembly events. While insufficient for root cause analysis, this data significantly improves investigative accuracy.

- **External Accountability and Compliance:** Supply chain stakeholders may use traceability records to demonstrate supplier integrity and fulfillment of obligations related to product origin, material sourcing, or conformance with contract terms, industry standards, or applicable policies.
- **Counterfeit Detection and Risk Mitigation**: By following traceability links to their sources, organizations can identify discrepancies in supplier-provided data, reducing the risk of counterfeit or non-compliant materials entering critical supply chains.

These examples are not exhaustive, as traceability-enabled validation supports a wide range of operational, security, and assurance activities across the supply chain. The Meta-Framework is designed to benefit end users seeking product transparency, industry stakeholders focused on supply chain management, and ecosystems working to maintain integrity and accountability.

5. Conclusion

Tracking products and components across the supply chain is essential for ensuring product integrity, building stakeholder trust, and supporting accountability throughout manufacturing ecosystems. However, collecting and verifying this data remains a significant challenge, especially in complex, multi-tiered supply chains with fragmented systems and inconsistent data practices.

The Meta-Framework improves traceability by defining a structured, interoperable model for recording, linking, and retrieving supply chain event data. It enables stakeholders to:

- Sequence traceability records and relevant supply chain event data;
- Interpret retrieved information in its appropriate ecosystem-defined context; and
- Rely on the integrity and authenticity of the data to validate product pedigree and provenance.

Traceability chains are formed by linking records created from supply chain events (e.g., manufacturing, shipping, receiving) using cryptographically verifiable connections. These links allow stakeholders to construct a coherent sequence of events that reflect product movement and transformation across the supply network.

Trust is supported by cryptographic validation mechanisms that allow participants to confirm the authenticity and integrity of traceability records. Hash-based traceability links ensure that each record is tamper-evident and verifiably connected to the previous one, enabling consistent validation over time.

The Meta-Framework supports verifiability through controlled disclosure to promote transparency without compromising sensitive information. Organizations can publish only the traceability data necessary for external validation while maintaining control over sensitive intellectual property, personally identifiable information (PII), and other sensitive or proprietary information.

Understanding is enhanced using ecosystem-specific data dictionaries and schema definitions, which constrain how data is structured and interpreted. By aligning with externally defined traceability requirements, such as those from industry groups or contractual agreements, the Meta-Framework ensures consistency and interoperability across diverse environments.

While this framework establishes a strong foundation for cross-ecosystem traceability, several areas require further development. Ongoing research will focus on expanding interoperability models, refining integrity validation methods, supporting privacy-enhanced mechanisms, and introducing new subclasses of traceability records and event types to reflect emerging operational needs. For additional discussion on future directions, see Appendix D.

References

[1] J.M. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, and Matthew Fallon. "Cybersecurity Supply Chain Risk Management for Systems and Organizations." National Institute of Standards and Technology, Gaithersburg, MD, 2022. https://csrc.nist.gov/News/2022/c-scrm-guidance-nist-sp-800-161r1 [Accessed 6 Sep 2024].

[2] M. Montecchi, K. Plangger, and D.C. West, "Supply Chain Transparency: A Bibliometric Review and Research Agenda," International Journal of Production Economics 238 (2021): 108152. Available: https://www.sciencedirect.com/science/article/pii/S0925527321001286. [Accessed 7 September 2024].

[3] K. Stouffer, M. Pease, J. Lubell, E. Wallace, H. Reed, V. Martin, S. Granata, A. Noh, and C. Freeberg, "Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability: Needs and Industry Perspectives," National Institute of Standards and Technology, Gaithersburg, MD, 2022. Available: https://doi.org/10.6028/NIST.IR.8419

[4] M. Pease, K. Stouffer, E. Wallace, H. Reed, S. Granata, "Manufacturing Supply Chain Traceability with Blockchain Related Technology: Reference Implementation," National Institute of Standards and Technology (NIST) Cybersecurity Center of Excellence (NCCoE), Gaithersburg, MD, 2023. Available: https://www.nccoe.nist.gov/sites/default/files/2023-08/mfg-sct-blkchn-project-description-final.pdf. [Accessed 12 August 2024].

[5] Joint Task Force, "Security and Privacy Controls for Information Systems and Organizations." National Institute of Standards and Technology, Gaithersburg, MD, 2020. Available: https://doi.org/10.6028/nist.sp.800-53r5. [Accessed 31 March 2025].

[6] "NIST Privacy Framework", National Institute of Standards. Available: https://www.nist.gov/privacy-framework. [Accessed 31 March 2025].

[7] "Supply Chain Assurance," National Institute of Standards (NIST) National Cybersecurity Center of Excellence (NCCoE), Gaithersburg, MD, 2022. Available: https://www.nccoe.nist.gov/supply-chain-assurance. [Accessed 31 March 2025].

Appendix A. List of Symbols, Abbreviations, and Acronyms

API
Application Program Interface

CI
Critical Infrastructure

CI-E
Critical Infrastructure – Ecosystem

CI-E IF
Critical Infrastructure – Ecosystem Interface

CISA
Cybersecurity and Infrastructure Security Agency

CSRC
Computer Security Resource Center

DHS
Department of Homeland Security

EV
Electric Vehicle

HTTP
Hypertext Transfer Protocol

ICAM

Identity, credential, and access management

IETF
Internet Engineering Task Force

IRI
Internationalized Resource Identifier

IT
Information Technology

ME
Microelectronics

ME-E
Microelectronics – Ecosystem

ME-E IF
Microelectronics – Ecosystem Interface

MIT
Massachusetts Institute of Technology

NIST IR
National Institute of Standards and Technology Internal Report

NIST SP
National Institute of Standards and Technology Special Publication

OEM
Original Equipment Manufacturer

OT
Operational Technology

OT-E
Operational Technology – Ecosystem

OT-E IF
Operational Technology – Ecosystem Interface

REST
Representational State Transfer

SCITT
Supply Chain Integrity, Transparency, and Trust

SCRM
Supply Chain Risk Management

UML
Unified Modeling Language

URL
Uniform Resource Locator

W3C
World Wide Web Consortium

Appendix B. Glossary

Cyber-Physical Link
A unique identifier that digitally associates a traceability record with a physical or virtual item ensures that the item can be tracked and verified throughout its lifecycle.

Ecosystem
A coordinated group of stakeholders, such as manufacturers, suppliers, technology providers, or data custodians, who operate under shared governance principles to manage, exchange, and validate traceability data. Ecosystems define policies for data storage, access control, and participant authentication, typically using trusted data repositories to ensure consistency, integrity, and authorized access across the supply chain.

Event Type
A classification that describes the kind of supply chain activity being recorded, such as make, assemble, receive, or employ. Event types define the structure of the associated variable data block.

Governance
A set of policies, rules, and enforcement mechanisms that are defined by an ecosystem to ensure the integrity, security, and proper management of traceability records and participant interactions.

Paywalling
Paywalls are a method of restricting access to content or features on a website or app, requiring users to pay or subscribe to access them. They generate revenue for content creators.

Pedigree
The validation of the composition and provenance of technologies, products, and services is referred to as the pedigree. For microelectronics, this includes the material composition of components. For software, this includes the composition of open source and proprietary code, including the version of the component at a given point in time. Pedigrees increase the assurance that the claims suppliers assert about the internal composition and provenance of the products, services, and technologies they provide are valid. [NIST SP 800-161 Rev. 1]

Personally Identifiable Information
Information that can be used to distinguish or trace an individual's identity—such as name, social security number, biometric data records—either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.). [FIPS 201-3]

Privacy
Assurance that the confidentiality of, and access to, certain information about an entity is protected. [NIST SP 800-130]

Provenance
The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data. [NIST SP 800-53 Rev. 5]

Supplemental Link
A non-mandatory data reference that connects a traceability record to external data sources (e.g., certifications, test reports, quality inspection results, operational logs, audit summaries, compliance attestations) stored outside the traceability repository. These are used to support additional validation or compliance requirements.

Traceability
The ability to trace the lineage, application, or location of what is under consideration. [ISO 21931-2:2019, adapted]

Traceability Chain
A chronological series of linked traceability records that document the history, movement, and transformation of a product or component across the supply chain.

Traceability Link
A reference mechanism within a traceability record that connects it to a prior record, enabling the reconstruction of the product’s history. Links typically include record identifiers, query parameters, and cryptographic hashes.

Traceability Record
A structured data object that captures a specific supply chain event (e.g., make, ship, receive) and includes metadata, traceability links, and optionally supplemental references. These records support the construction of traceability chains.

Trusted Data Repository
A data storage system or service designated within an ecosystem to securely store traceability records and governed by policies that control access, enforce data retention requirements, and support data integrity mechanisms such as cryptographic validation.

Variable Data Block
A flexible portion of a traceability record used to store industry- or event-specific metadata, defined according to schemas referenced by the Event Type.

Appendix C. Security, Privacy, and Access Control Considerations

The Meta-Framework introduces cybersecurity and privacy challenges due to the need to link traceability records across trusted data repositories, enforce authentication, and manage potentially sensitive personal or business information. This appendix highlights key considerations to support confidentiality, integrity, and availability, as well as predictability, manageability, and disassociability[2] of traceability data, with a focus on both adversarial and non-adversarial threat mitigation.

This is not intended to serve as a comprehensive security or privacy guide. Instead, it provides guidelines to help ecosystems and participating organizations shape their cybersecurity and privacy strategies to address operational, contractual, and supply chain-specific risks. Alignment with broader NIST guidelines, such as NIST SP 800-53 [5] and the NIST Privacy Framework [6], can further support the integrity and trustworthiness of traceability systems across diverse sectors.

C.1. Identity, Authentication, and Access Control

Identity, credential, and access management (ICAM) are essential to securing traceability records and preventing unauthorized use [5]. Ecosystems must implement mechanisms to:

- Authenticate stakeholders before allowing them to read, write, or manage traceability records.
- Authorize access to traceability data on a need-to-know basis, protecting sensitive information from internal or external threats.

Given the multi-organizational nature of most ecosystems, access should be carefully scoped to reflect participant roles and data sensitivity. While some stakeholders, such as external auditors or ecosystem coordinators, may require broader query capabilities, competitors and unauthorized parties must be restricted from accessing or inferring proprietary or sensitive information.

To safeguard against data enumeration or bulk extraction attacks, trusted data repositories should consider the following:

- Implementing parameterized access control and rate limiting.
- Preventing brute-force queries, directory crawling, or exploitation of query interfaces.
- Ensuring only records authorized for a given stakeholder are discoverable or retrievable.

Further technical guidelines on authentication and access control strategies can be found in Appendix G.

[2] The NIST Privacy Framework [6] explains the privacy engineering objectives of predictability, manageability, and disassociability.

C.2. Privacy Measures

Although traceability records primarily support product pedigree and provenance, they may contain or reference sensitive personal or organizational information. These include:

- Individuals associated with traceability events (e.g., personnel logging a shipment or authorizing a manufacturing step).
- Contact details embedded in shipping, receiving, or warranty events.
- Operational metadata that may reveal sensitive internal operations or supplier relationships.

To address privacy risks, ecosystems should adopt the following principles:

- **Data minimization:** Only collect the minimum personal data necessary to fulfill traceability use cases.
- **Redaction and anonymization:** Ensure sensitive fields (e.g., names, contact details, identifiers) are masked when shared externally or queried across ecosystems.
- **Scoped retention:** Personal data should be retained only as long as necessary to fulfill compliance or operational needs.
- **Purpose limitation:** Use personal data strictly for traceability purposes for which it was collected and shared to prevent repurposing for unrelated uses.
- **Transparency and notice:** If traceability records include personally identifiable information (PII), such as names or contact details of individuals involved in events (e.g., shipment handlers, quality inspectors), organizations should ensure those individuals are informed about how their data is collected, used, and shared. Ecosystems should limit such information unless operationally necessary and apply data minimization or pseudonymization techniques to protect privacy.
- **Governance:** Define clear roles and responsibilities for data protection across the supply chain through contracts (e.g., data sharing agreements), policies, processes, and procedures that align with applicable privacy requirements and regulations.

C.3. Balancing High-Assurance Identity and Privacy Risks

Cryptographic object identifiers (e.g., Product_ID, Assemble_ID) are foundational for verifiable traceability records, providing unique, tamper-evident references for physical or virtual items. However, when deployed into operational environments, such as during warranty claims or system maintenance, these identifiers may introduce privacy risks if correlated with end-user activity or location data.

To address this tension between integrity assurance and privacy protection, ecosystem operators should:

- Utilize privacy risk management tools, such as privacy impact assessments (PIAs) or the NIST Privacy Risk Assessment Methodology (PRAM)[3], to evaluate traceability risks in downstream use.
- Determine the appropriateness of high-assurance identifiers based on use case sensitivity.
- Apply mitigation strategies such as pseudonymization, selective disclosure, or dynamic identifier rotation to reduce long-term identifiability risks.

Additionally, ecosystems are encouraged to build privacy protection into architectural decisions. Strong access controls, careful exposure of identifier metadata, and adoption of privacy-enhancing technologies (e.g., zero-knowledge proofs, differential privacy[4]) can help balance traceability utility with individual and organizational privacy obligations.

Further exploration of privacy-aware traceability strategies is a recommended area of future research (see Appendix D).

C.4. Threat Modeling and Ecosystem Risk Posture

Implementing the Meta-Framework in real-world environments requires ecosystem operators and participating organizations to evaluate their risk posture and threat landscape. Ecosystems may vary widely in terms of industry context, operational complexity, and technology maturity. As a result, each ecosystem should perform its own threat modeling and risk analysis to identify potential attack vectors and define the appropriate level of security controls.

Threat modeling should consider both adversarial and non-adversarial risks, including:

- Unauthorized access to traceability records.
- Tampering with traceability data or traceability links.
- Misuse of identity or credentials to impersonate authorized stakeholders.
- Indirect inference of sensitive business or operational information through metadata analysis or record enumeration.
- Denial of service attacks on data repository interfaces or ecosystem services.

Key recommendations include:

- Align threat modeling practices with established frameworks such as NIST SP 800-30 for risk assessments and the NIST Cybersecurity Framework and NIST Privacy Framework [6] for structuring risk responses and privacy risk management.

[3] The NIST Privacy Risk Assessment Methodology (PRAM) helps organizations analyze, assess, and prioritize privacy risks to determine how to respond and select appropriate solution. The PRAM can be found at https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

[4] To learn more about differential privacy, see NIST Special Publication 800-226, Guidelines for Evaluating Differential Privacy Guarantees. Available at https://doi.org/10.6028/NIST.SP.800-226.

- Conduct routine assessments to adapt security controls to evolving threats, especially for ecosystems that involve sensitive national infrastructure, critical technologies, or defense-related supply chains.
- Define risk tolerance thresholds and apply appropriate safeguards based on the sensitivity and criticality of the traceability data handled by the ecosystem.
- Integrate zero trust principles, minimizing assumptions of trust across ecosystem boundaries, and enforcing strict verification before allowing access to traceability data.

By treating threat modeling as an ongoing process and not a one-time activity, ecosystems can evolve their security and privacy postures to meet both operational needs and stakeholder trust requirements. Incorporating these considerations into governance and implementation planning will help ensure that traceability records remain secure, reliable, and aligned with the Meta-Framework's assurance objectives.

C.5. Other Considerations

In addition to the specific concerns outlined above, ecosystems should consider implementing the following best practices:

- **Audit and Monitoring:** Maintain secure logs of all traceability record access and modification activity. Continuous monitoring enables early detection of unauthorized or anomalous behavior.
- **Data Encryption:** Ensure traceability records and related metadata are encrypted both in transit and at rest using industry-accepted encryption standards.
- **Incident Response:** Ecosystems should have plans in place for responding to cybersecurity incidents, including notifying affected stakeholders, preserving forensic data, and restoring trust in affected records.

Appendix D. Future Directions for the Meta-Framework

The Meta-Framework outlined in this report establishes a foundational approach to traceability across various manufacturing sectors and their supply chains, specifically focusing on manufacturing, assembly, and product delivery.

This framework serves as the basis for a more comprehensive approach to traceability. However, the initial version primarily emphasizes the traceability of supply chain event data, which is documented as linked traceability records, as shown below.

In the future, this framework can be expanded to further enhance supply chain traceability by extending the traceability record subclasses to include the sustainment chain and introducing additional traceability record subclasses within the supply chain.

Adding new traceability record subclasses to the supply and sustainment chains and refining other aspects of the Meta-Framework based on industry input can evolve into a comprehensive tool for lifecycle traceability. This appendix summarizes the potential next steps toward this broader vision.

D.1. Expanding Traceability to Sustainment and Lifecycle Phases

The Sustainment Chain starts after the manufacturing supply chain and the initial employ event of a product, illustrated in Fig. 15 below. Additional events such as product returns, recalls, refurbishments, transfers, and disposals become essential in the sustainment chain. Future research can explore how to record the sustainment chain event data to provide a complete lifecycle view of the product.

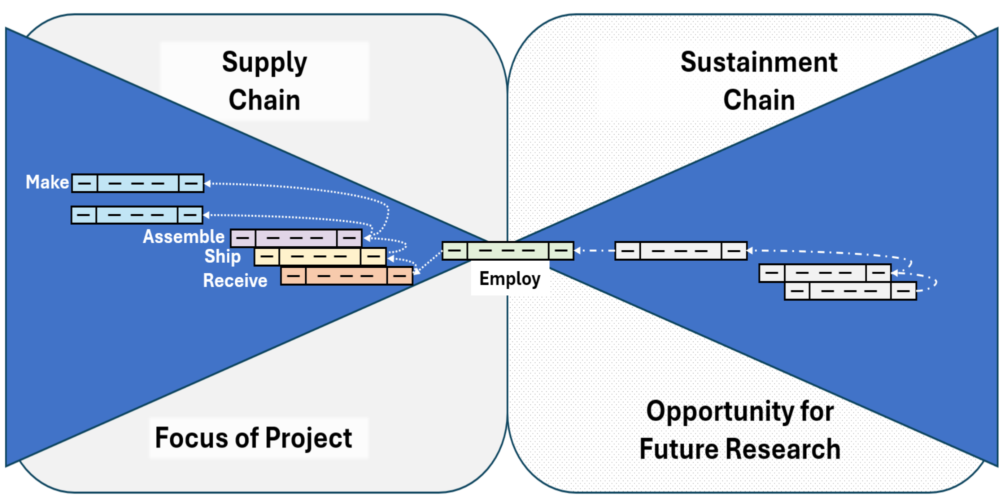

Figure 15. Sustainment Chain Opportunity for Future Research

Future research could explore introducing additional sustainment chain traceability record subclasses to record and link to sustainment chain event data, as described in Table 3. While the Meta-Framework does not directly manage the full data lifecycle of traceability records or embedded product data, ecosystems implementing the Meta-Framework should establish data governance policies addressing record retention, archival, and disposal. In cases where products being decommissioned contain embedded data (e.g., logs, user information, cryptographic credentials), appropriate system-level procedures for secure deletion or sanitization should be applied outside the traceability layer.

Table 3. Candidate New Sustainment Chain Traceability Record Subclasses

Subclass	Description
Returns	When a product is returned by an end customer for any reason, a Return Traceability Record could be created to capture this event. Recording returns as traceability events would provide proof that the product has been removed from service or is no longer in the customer's possession.
Recalls	In the event of a manufacturer-initiated recall, a Recall Traceability Record could trace the product back to the customer. If a customer is also a manufacturer, they could pass along the recall to their customers, enabling a more transparent and efficient recall process throughout the supply chain.
Refurbishment	During a product's sustainment phase, various maintenance actions, such as software updates, sensor replacements, or other refurbishments, may occur. A refurbished traceability record could capture these modifications, ensuring that all product changes are documented.
Transfer	Records the handoff of custody, ownership, or operational control of a product between organizations or environments. This event may support scenarios involving leasing, subcontracting, resale, or cross-border movement.
Dispose	Captures decommissioning or end-of-life actions for a product, such as disconnection from IT/OT systems, physical destruction, or secure disposal. This record may also confirm that the product is no longer in active use or available for redeployment.

D.2. Additional Supply Chain Traceability Record Subclasses

Future research could explore the introduction of additional supply chain traceability record subclasses to capture additional supply chain event data, as described in Table 4.

Table 4. Candidate New Supply Chain Traceability Record Subclasses

Subclass	Description
Precursor	A Precursor Traceability Record could trace raw materials, such as silica used in semiconductor manufacturing, through the production process. This could extend traceability to the origin of the materials used in products, providing a more comprehensive view of the supply chain.
Process / Convert	Future research could include continuous flow, batch, and other transformative manufacturing processes. In these cases, additional traceability records could distinguish between the continuous production of materials, the production of batches of materials, and the production of discrete components.

Subclass	Description
Split	A Split Traceability Record captures events where a single product, material, or shipment is divided into multiple distinct entities while maintaining traceability to the original source. This is particularly useful in scenarios such as cutting a silicon wafer into individual chips, repackaging bulk materials into smaller units, or distributing subassemblies. The Splitting event ensures that the relationship between the original and derived components is clearly documented, supporting traceability across fragmented supply chains.
Modify	A Modify Traceability Record documents changes made to an existing product or component without full reassembly. This could include firmware updates, rework of a defective part, or refinishing processes (e.g., anodization, coating, or heat treatment). By tracking modifications as distinct traceability events, stakeholders can verify what changes were made, when, and by whom, ensuring data integrity and compliance with industry regulations.
Transportation	Adding Transportation Traceability Records could enhance the visibility of the logistics and transport phases of the supply chain. These new Traceability Records could document specific steps taken by logistics providers between the shipping and receiving stages, adding deeper transparency and enhanced accountability regarding the product’s movement through shipping.

Appendix E. Key Challenges in Achieving Interoperable Traceability

E.1. Challenge #1: Information Stored in Disjointed and Isolated Repositories.

Challenge Overview (Situation and Context)

Supply chain pedigree and provenance information are often stored in private, fragmented, or inaccessible repositories, making it difficult for stakeholders to access critical traceability data. Original Equipment Manufacturers (OEMs) and suppliers may deliberately limit access to protect proprietary business information, intellectual property, or competitive advantages. In some cases, essential supply chain data is placed behind paywalls or shared selectively, restricting visibility for stakeholders, including customers, integration partners, or external validation authorities.

This lack of transparency can hinder due diligence efforts, supply chain risk assessments, and compliance verification, particularly when verifying product authenticity, security assurances, or country-of-origin claims. Some supply chain integrity efforts are making inroads toward specific types of other trust, such as verifying that internal components of purchased computing devices are genuine and have not been altered during manufacturing or distribution processes [7]. In contrast, this NIST IR focuses on establishing mechanisms to ensure that recorded supply chain event data remains consistent, verifiable, and tamper-evident across manufacturing sectors.

Implications and Risks (Impact)

When supply chain data is inaccessible or selectively withheld, organizations face:

- **Challenges in verifying product authenticity and origin:** Without complete traceability data, end users and acquirers cannot reliably determine whether a product meets contractual, operational, or assurance expectations.
- **Increased supply chain vulnerabilities**: Hidden or inaccessible records make risk assessment difficult, exposing organizations to counterfeit products, security and privacy threats, and sourcing concerns.
- **Gaps in external accountability:** If access to traceability data is restricted, stakeholders may struggle to meet transparency expectations or respond to external obligations related to sourcing, trade, or security.
- **Erosion of trust between supply chain partners**: A lack of data transparency and consistency undermines confidence in supplier-provided information, complicating collaboration and decision-making.

Meta-Framework Approach

The Meta-Framework mitigates this challenge by:

- **Defining Minimum Traceability Data Requirements**: Supporting the use of baseline data elements defined by industry groups, standards organizations, or contractual obligations to ensure that critical traceability information remains consistently available to authorized stakeholders.

- **Enabling Controlled and Non-Discriminatory Access**: Provide mechanisms for acquirers, customers, and other downstream stakeholders to access traceability data without arbitrary restrictions while still allowing organizations to protect proprietary information.
- **Discouraging Paywalling of Fundamental Traceability Records**: Promoting transparency by ensuring that foundational traceability data necessary for product validation and risk assessment is not monetized in ways that restrict essential access.
- **Balancing Confidentiality and Transparency**: Offering structured methods to protect sensitive business data while still making necessary traceability information available to support supply chain assurance and accountability.
- **Supporting External Oversight and Alignment:** Allowing ecosystems to align their traceability disclosures with applicable standards, legal obligations, or industry requirements, as appropriate for their sector or role in the supply chain.

Overall, the Meta-Framework establishes a structured, enforceable approach to accessing traceability data, ensuring supply chain transparency while allowing organizations to maintain necessary confidentiality protections.

E.2. Challenge #2: Inconsistent semantic and data definitions.

Challenge Overview (Situation and Context)

Supply chain participants often maintain and share traceability data using internal data formats, terminologies, and semantic rules, which may not align with industry-wide or cross-organizational standards. These semantic inconsistencies lead to gaps in understanding, making it difficult to interpret, compare, or integrate traceability records across different supply chain stakeholders.

Without consistent data models or shared definitions, organizations risk misinterpreting or misaligning critical supply chain data, reducing the effectiveness of traceability systems.

Implications and Risks (Impact)

The lack of common semantics and data structures creates several challenges:

- **Data Misalignment Across Supply Chain Records**: Different manufacturers, suppliers, and ecosystem participants may use incompatible naming conventions, metadata structures, or classification systems, causing discrepancies in traceability records.
- **Reduced Automation and Data Processing Efficiency**: Without shared definitions, organizations must manually reconcile or translate traceability data, increasing operational overhead and limiting scalability.

- **Barriers to Assurance and Collaboration**: Inconsistently structured data makes it difficult for stakeholders to validate traceability information or meet externally defined requirements, such as contractual terms or industry expectations.
- **Increased Risk of Errors and Misinterpretation**: Ambiguous or conflicting data formats increase the likelihood of incorrect traceability assessments, potentially leading to operational failures, recalls, or compromised supply chain integrity.

Meta-Framework Approach

The Meta-Framework addresses semantic inconsistencies by:

- **Supporting Adoption of Externally Defined Traceability Models**: The framework enables ecosystems to align with data models established by industry consortia, standards bodies, or sector-specific traceability initiatives.
- **Providing a Flexible but Structured Data Model:** Traceability systems built on the framework can support varying data needs while preserving consistency that enables validation and automation.
- **Enabling Shared Data Dictionaries and Ontologies**: The Meta-Framework incorporates mechanisms for defining and enforcing shared semantics, ensuring that stakeholders interpret traceability data uniformly across contexts.
- **Facilitating Cross-Ecosystem Interoperability**: The framework supports the mapping and translation of traceability data between disparate systems, reducing semantic mismatches and enhancing data quality.

By promoting consistent data models, aligned ontologies, and structured traceability records, the Meta-Framework improves interoperability, reduces operational errors, and strengthens stakeholder trust in the accuracy of supply chain data.

E.3. Challenge #3: Ensuring Traceability Data Integrity

Challenge Overview (Situation and Context)

Ensuring pedigree and provenance information integrity is a significant challenge for end customers and intermediate manufacturers. Data integrity, as defined by the Computer Security Resource Center (CSRC) glossary, is:

"The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit."

In modern supply chains, traceability data is generated, managed, and transmitted by multiple stakeholders, each using different approaches to securing and documenting data. Without a consistent and verifiable method to validate traceability record integrity across the supply chain, stakeholders may lack confidence in the authenticity and reliability of traceability records.

Implications and Risks (Impact)

Without standardized integrity mechanisms, organizations face several challenges:

- **Inconsistent quality and reliability of traceability data**: Variation in integrity controls across different stakeholders can lead to data discrepancies, misinterpretations, or gaps in supply chain visibility.
- **Difficulties in verifying pedigree and provenance information**: Without a standardized approach for integrity validation, stakeholders must rely on manual processes or incomplete records, increasing the risk of counterfeit products or unverifiable claims.
- **Increased exposure to data tampering risks**: If traceability data lacks cryptographic validation, it becomes vulnerable to unauthorized modifications, undermining trust in supply chain transparency.

Meta-Framework Approach

The Meta-Framework addresses traceability data integrity challenges by:

- **Defining Standardized Integrity Controls**: The framework establishes baseline integrity measures to ensure that traceability data remains consistent and verifiable across the supply chain.
- **Using Cryptographic Hashing for Data Validation**: Traceability records can include cryptographic hashes that enable stakeholders to validate whether data has been altered since it was recorded.
- **Enabling Verifiable Traceability Links**: Each traceability record can include a cryptographic reference to its predecessor, creating a chain of trust that prevents tampering and unauthorized modifications.
- **Supporting Distributed Validation Mechanisms**: The framework allows ecosystems to implement decentralized integrity verification methods, ensuring that supply chain data remains trustworthy, even when shared across multiple organizations.

The Meta-Framework provides a structured approach to maintaining supply chain data integrity, reducing fraud risks, and strengthening stakeholder trust by incorporating cryptographic validation, practicing integrity methods, and ensuring traceability records remain tamper-resistant.

E.4. Challenge #4: Balancing Confidentiality and Privacy in Traceability

Challenge Overview (Situation and Context)

While the Meta-Framework is designed to enhance traceability and visibility across the supply chain, it must also address confidentiality and privacy concerns to ensure that stakeholders such as OEMs, suppliers, external auditors, and end-users can securely access traceability data for pedigree verification, compliance enforcement, and risk assessment without compromising sensitive business or personal information.

Traceability records may contain critical supply chain data, including proprietary business information, operational details, and personally identifiable information (PII) related to production, shipping, and receiving events. Uncontrolled disclosure of traceability data can introduce several risks, including:

- Exposing proprietary manufacturing processes, sourcing strategies, or supplier relationships.
- Unintended linkage of high-assurance item identifiers to end-user identities, creating potential tracking risks.
- Compliance challenges with privacy regulations, such as GDPR, CCPA, and industry-specific confidentiality requirements.
- Stakeholders restricting traceability disclosures due to competitive, legal, or strategic concerns, limiting supply chain transparency.

The challenge is balancing transparency and verifiable traceability with protecting confidential business information and privacy-sensitive data.

Implications and Risks (Impact)

Failure to properly manage confidentiality and privacy could result in:

- **Reduced industry adoption**: Stakeholders may hesitate to share supply chain data due to concerns over data exposure, competitive risks, or IP protection.
- **Increased exposure to privacy and confidentiality risks:** Organizations that do not adequately protect traceability data may face consequences related to contractual violations, reputational harm, or nonconformance with applicable privacy expectations and information-handling requirements.
- **Privacy concerns for deployed products**: If not properly managed, cryptographic object identifiers could be used to track or monitor end-user behavior, raising concerns over unintended surveillance[5].

Conversely, overly restrictive data policies may undermine traceability goals, making it difficult for stakeholders, including customers, integration partners, or external validation authorities, to verify product authenticity and assess supply chain risks.

Meta-Framework Approach

The Meta-Framework mitigates confidentiality and privacy risks while maintaining traceability integrity through the following:

- **Defining Minimum Traceability Data Requirements**: Establishing baseline data elements necessary for verification, validation, and risk assessment while ensuring that confidential business details remain protected.

[5] As part of its PRAM, NIST has created an illustrative catalog of problematic data actions, including surveillance, and problems for consideration.

- **Applying Data Minimization Principles**: Ensuring that only essential traceability information is recorded and shared, reducing exposure of sensitive data.
- **Enabling Controlled Access via Traceability Links**: While role-based access controls (RBAC) and tiered permissions manage internal access within an ecosystem, the Meta-Framework also supports controlled access to traceability records through cryptographically secured Traceability Links. This enables stakeholders, such as acquirers or auditors, to query traceability records using valid traceability links and predefined query parameters, even without direct login credentials to the ecosystem.
- **Supporting Ecosystem Flexibility for Privacy Protection**: Ecosystems and organizations are responsible for aligning their traceability practices with applicable privacy expectations, legal obligations, and sector-specific information-handling requirements. The Meta-Framework supports this flexibility by allowing ecosystems to implement tailored traceability and data-sharing solutions that meet transparency objectives while protecting confidentiality and minimizing exposure to sensitive information.
- **Implementing Governance and Audit Controls:** The Meta-Framework provides a structured foundation for ecosystems to establish governance models that support transparency, accountability, and responsible traceability data management. By adopting the framework's principles, ecosystems can define mechanisms for monitoring data access, enforcing data-handling policies, and ensuring that traceability records remain consistent, verifiable, and trustworthy. The flexible approach enables organizations to adapt governance and audit practices to align with internal policies, stakeholder expectations, and applicable contractual or information-management requirements.

By leveraging structured data controls, privacy principles, and compliance measures, the Meta-Framework supports secure and transparent traceability while minimizing the exposure of sensitive information. As privacy regulations and industry needs evolve, the framework can further integrate emerging privacy-enhancing technologies and best practices to refine the balance between traceability, integrity, and confidentiality protection.

Appendix F. Technical Data Model and Class Structures

This appendix provides an example detailed technical overview of the Meta-Framework's traceability record data model. It describes a class structure that underpins traceability records, ensuring interoperability and structured data capture across supply chain ecosystems. The information in this appendix is intended for developers, system architects, and ecosystem implementers responsible for integrating traceability mechanisms into their platforms.

The Meta-Framework defines a hierarchical class structure where all traceability records could be inherited from a common Traceability_Record superclass. Such a design would help to ensure that shared attributes, such as timestamps and organization identifiers, are consistently maintained across all event types while still allowing for event-specific extensions in subclasses.

F.1. UML Class Structure of Traceability Records

The following UML diagram (Figure 16) illustrates the class hierarchy of traceability records, demonstrating how event-specific records (e.g., make, assemble, ship, receive, and employ) inherit from a common base class, the Traceability_Record.

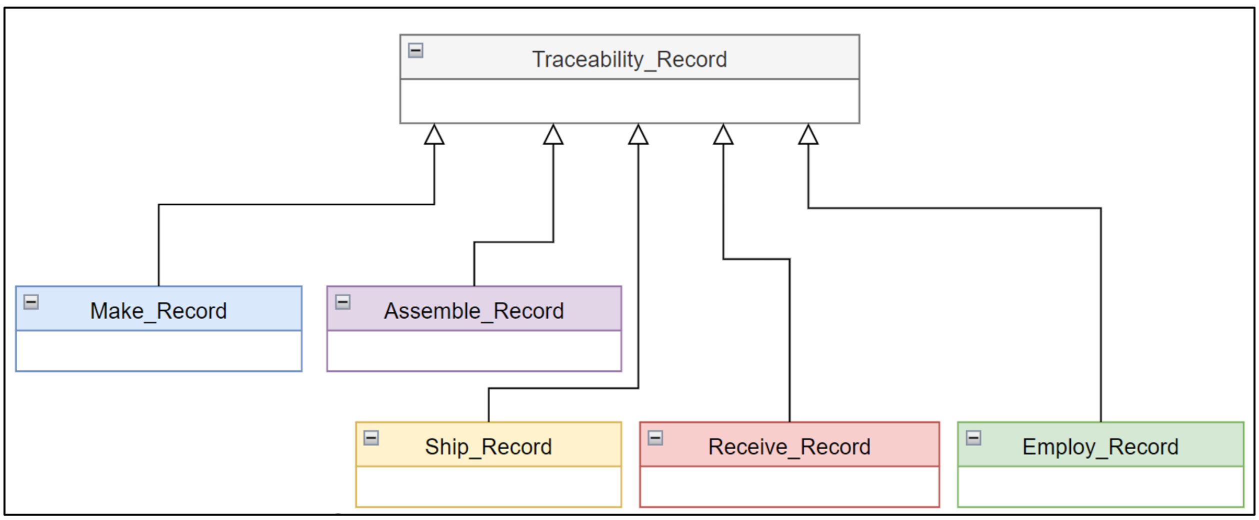

Figure 16. Overview Class Diagram for Traceability Record

F.2. Traceability_Record Superclass

The Traceability_Record superclass (Figure 17) defines the core attributes that all traceability records share. Table 5 provides definitions and example data.

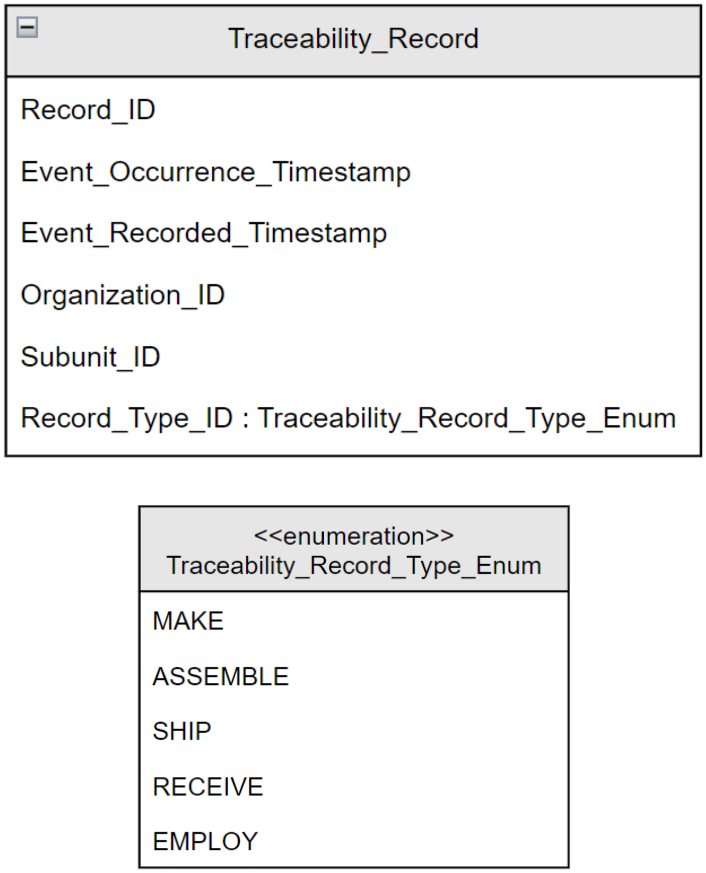

Figure 17. Traceability_Record Attribute Structure

Table 5: Traceability Record Attributes

Data Attribute	Description	Example Type / Values
Record_ID	Globally unique identifier for each Traceability Record.	UUID or similar identifier (e.g., W3C): 550e8400-e29b-5…
Event_Occurrence_Timestamp	Timestamp indicating the date and time of the traceability event occurrence.	ISO 8601 Date-Time: 2025-03-15T14:30:00Z

Data Attribute	Description	Example Type / Values
Event_Recorded_Timestamp	Timestamp indicating the date and time of the recording of the traceability event within the ecosystem.[6]	ISO 8601 Date-Time: 2025-03-15T14:35:45Z
Organization_ID	Identifier for the organization responsible for the traceability event (e.g., Company or Business Unit Registered in Ecosystem)	String, UUID: ORG-123456, 550e8400-e29b-4…
Subunit_ID	Identifier for the sub-unit of the organization where the traceability event occurred (e.g., Business Unit, Factory, or another organizational subunit where the event occurred).	String, UUID: FAB-01 DEPT-004, 550e8400-e29b-6…
Record_Type_ID	Code indicating the subclass of traceability event for this record. This code should be one of make, assemble, ship, receive, or employ[7].	Traceability_Record_Type_Enum: (e.g., MAKE, ASSEMBLE, SHIP, RECEIVE, EMPLOY)

Note: Organization and Subunit Identifiers are intended to represent publicly recognized business entities or functional units responsible for supply chain events. These identifiers are not expected to include personal or private information and should be selected to reflect traceability without compromising individual privacy.

F.3. Traceability Record Supporting Data Objects

In addition to the core attributes defined in the Traceability_Record superclass, the Meta-Framework defines several supporting data objects that enable structured and flexible traceability record construction. These supporting objects provide the mechanisms for capturing event-specific metadata, linking records across ecosystems, and referencing external resources that enhance traceability, compliance, and validation efforts.

These supporting objects include:

- Key-Value Pair objects for representing structured metadata within event-specific data blocks.
- Traceability Link objects for securely linking a traceability record to its precursors and enabling hash-based verification of record integrity.

[6] The recording of an event in the ecosystem may occur later than the event itself and may not be handled by the same system. Capturing the correct time for an event occurrence can be critical to root cause analysis, identifying tainted or at-risk product, or other uses of traceability data. To avoid ambiguity in use and interpretation of timestamps, the event occurrence time is explicitly separated from the time of recording.
[7] This list would likely expand in the future as new traceability use cases require tracking of additional phases of a product life cycle beyond those considered in this paper.

- Supplemental Link objects for referencing auxiliary data sources, such as compliance reports or external documentation that may be required to fulfill stakeholder requirements.

Each supporting object has a defined attribute structure that contributes to the traceability chain's interoperability, security, and scalability. The following subsections describe each supporting data object and its role within the broader Meta-Framework data model.

F.3.1. Key-Value Pair Data Objects

To represent a key-value pair, such as those that populate an event data block, the following data object is defined in Fig. 18 and Table 6 as:

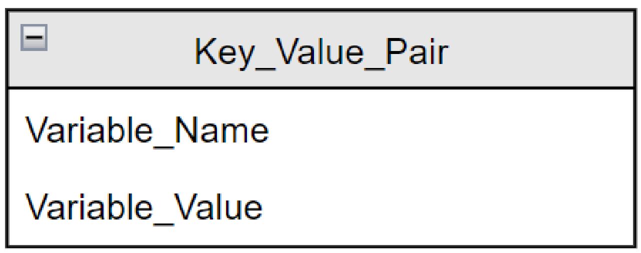

Figure 18. Key_Value_Pair Attribute Structure

Table 6. Key_Value_Pair Attribute Definitions

Data Attribute	Description	Example Types / Values
Variable_Name	A label or identifier that describes the type of information being recorded. The variable name helps clarify what specific piece of data is being captured in the record.	String: "BatchID", "Serial_Number", “Version”, "Hash"
Variable_Value	The actual data or information being captured. The variable value provides the specific details associated with the variable name.	String: MX100-BATCH-001, Number: 7.5, Boolean: true/false, Array/Object: {"componentID": "A12345", "status": "verified"}

F.3.2. Traceability Link Data Object

For supporting links to precursor traceability records, the following structure is defined in Fig. 19 and Table 7 for capturing each link. To facilitate controlled, credential-free access to traceability records, the Meta-Framework introduces the idea of utilizing an “Access Hash” mechanism. This SHA-3-based query authentication method could help ensure that only stakeholders with knowledge of the correct Record ID and a Hash generated at the time of record creation, based on some of the record fields, such as the record create and recorded timestamps, demonstrate authorization to retrieve a record.

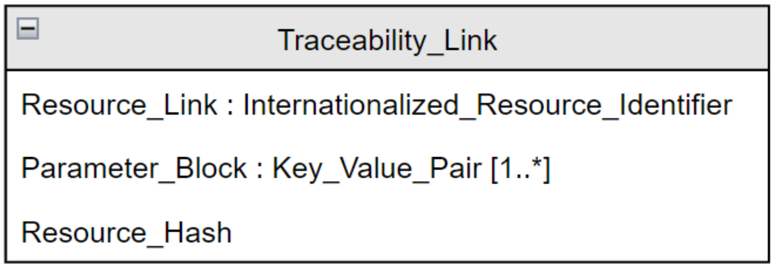

Figure 19. Traceability Link Attribute Structure

Table 7. Traceability Link Attribute Definitions

<table>
<tr><th>Data Attribute</th><th>Description</th><th>Example Types / Values</th></tr>
<tr><td>Resource_Link</td><td>A reference to direct the requestor to access an ecosystem service to retrieve the data</td><td>URI / URL:
https://example.com/traceability</td></tr>
<tr><td>Parameter_Block</td><td>A structured set of parameters is used to query and retrieve the requested traceability record. This may include a UUID for direct lookup combined with a secure hash of key record fields (e.g., UUID + timestamps) to allow verification of authority to access while preserving confidentiality.</td><td><table><tr><th>Key</th><th>Value</th></tr><tr><td>RecordID</td><td>b81f4e92-34f5-4978-9eb3-c…</td></tr><tr><td>accessHash</td><td>256:45ac89efb3c4d1a9…</td></tr></table></td></tr>
<tr><td>Resource_Hash</td><td>A hash of the full record to verify the data integrity of the returned data. This is considered essential for the use cases the meta-framework supports (i.e., where data must be verifiable).</td><td>String:
SHA3-256:abcd1234efgh…</td></tr>
</table>

Note: The Access Hash value used as part of the query parameters is different from the Resource Hash value. The Access Hash is only used for authorization to the requested record, while the resource hash is a cryptographic hash of the entire record and is used to validate that the information received has not been altered.

F.3.3. Supplemental Link Data Objects

Supplemental Link Data Objects are ***optional*** links that may include other data sources relevant to the Traceability Record, such as test data, documentation, or third-party attestations that may be too large to include within the traceability record itself. While supplemental links can provide valuable context for supply chain risk management, assurance, and compliance-related evaluations, the Meta-Framework acknowledges that this information may reside outside of the trusted data repository and may not be immediately accessible to all stakeholders without additional coordination. As such, traceability records should include all essential data needed to support pedigree and provenance validation independently of any supplemental links. This ensures that core traceability objectives can still be met, even when supplemental data is unavailable or restricted. To capture the information for supporting links to information, the following structure is defined in Fig. 20 and Table 8 for capturing an individual link:

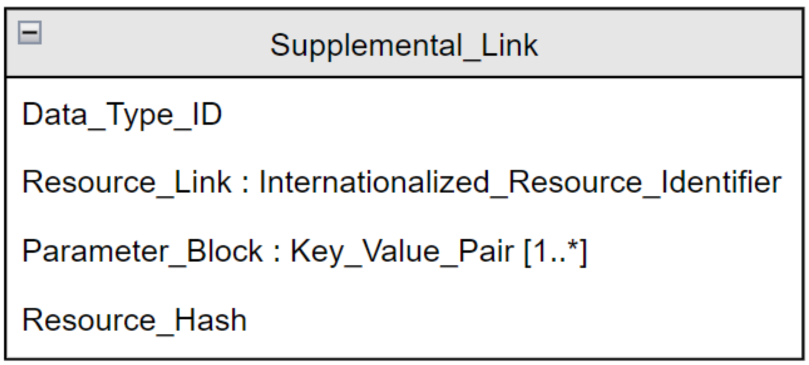

Figure 20. Supplemental Link Attribute Structure

Table 8. Supplemental Link Attribute Definitions

<table>
<tr><th>Data Attribute</th><th>Description</th><th>Example Type / Value</th></tr>
<tr><td>Data_Type_ID</td><td>A code indicating the type of data linked.</td><td>Enum:ComplianceReport, TestData, Certifications, AuditRecord</td></tr>
<tr><td>Resource_Link</td><td>A reference to direct the requestor to access an ecosystem or other service to retrieve the data</td><td>URI / URL: https://example.com/trapi/get</td></tr>
<tr><td>Parameter_Block</td><td>A structured set of parameters is used to query and retrieve the requested data record. This may include a UUID for direct lookup combined with a secure hash of key metadata (e.g., UUID + timestamps) to allow verification while preserving confidentiality.</td><td><table><tr><th>Key</th><th>Value</th></tr><tr><td>RecordID</td><td>b81f4e92-34f5-4978-9eb3-c…</td></tr><tr><td>accessHash</td><td>256:45ac89efb3c 4d1a9...</td></tr></table></td></tr>
<tr><td>Resource_Hash</td><td>A hash of the full record to verify the data integrity of the returned data. This is considered essential for the use</td><td>String:
SHA3-256: abcd1234efgh5678ijk…</td></tr>
</table>

Data Attribute	Description	Example Type / Value
	cases the meta-framework supports (i.e., where data must be verifiable).	

F.4. Event-Specific Subclasses

As shown in Fig. 16, each supply chain event type is implemented as a subclass of Traceability_Record, inheriting the common attributes while defining additional event-specific attributes. These subclasses and their roles are:

- **Make_Record:** Captures the creation of new components or products, linking to raw materials (i.e., materials that did not yet have associated Traceability_Records).
- **Assemble_Record:** Represents the combination of multiple previously tracked components into a final product. Unlike a make event, which may originate a new component from untracked or raw materials, an assemble event references input materials that have already been recorded using Meta-Framework Traceability_Records. This distinction ensures that the resulting assembly maintains continuity within the traceability chain.
- **Ship_Record:** Documents the transfer of products between entities, linking to preceding events.
- **Receive_Record:** Captures the receipt of products, linking to the corresponding ship event.
- **Employ_Record:** Represents the deployment or activation of products in operational environments.

Each subclass maps a unique Tracked Entity Identifier (e.g., Product_ID, Assembly_ID, ShipmentID) to maintain the cyber-physical link between records. Additionally, the subclasses incorporate additional traceability record data fields, including:

- **Traceability Links (List):** References to preceding records in the traceability chain.
- **Data Type Identifier (String):** Defines the schema for event-specific data.
- **Data Block (List<Key, Value>):** Captures event-specific metadata.
- **Supplemental Links (List):** External references to supplemental, non-mandatory data.

Within each subclass described in the following sections, these fields have been given subclass-specific names.

F.4.4. Make Record Subclass

A make event record includes the attributes of a traceability record and extends them with attributes peculiar to the creation of a product where no previously tracked items are used as components. Make record-specific attributes are shown in Fig. 21.

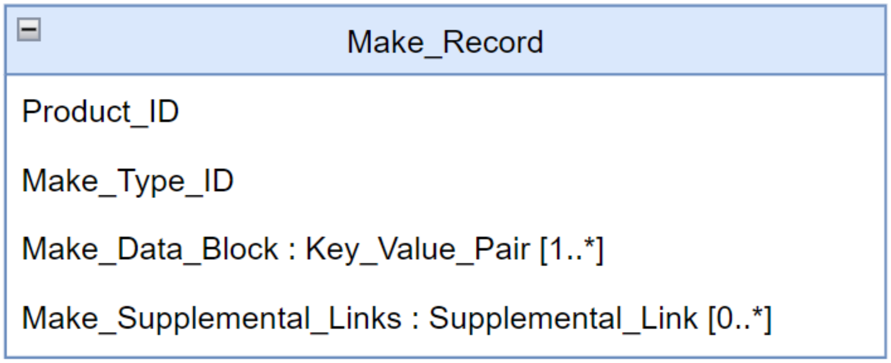

Figure 21. Make Record Attribute Structure

The attributes for a make record are defined in Table 9 below:

Table 9. Make Record Attribute Definitions

<table>
<tr><th>Data Attribute</th><th>Example Types / Values</th></tr>
<tr><td>Product_ID</td><td>String: SN-123456789, UID-987654321, DigitalTwin-UUID-001</td></tr>
<tr><td>Make_Type_ID</td><td>String: CHIP-TYPE-A, FDA-BATCH-PROCESS-TYPE-B_V01, UL-508-A</td></tr>
<tr><td>Make_Data_Block</td><td><table>
<tr><th>Key</th><th>Value</th></tr>
<tr><td>Material_Lot</td><td>LOT-2024-001</td></tr>
<tr><td>Machine_ID</td><td>CNC-45-AX</td></tr>
<tr><td>Operational_Data</td><td>Temp:48.9, Units:C,
Pressure:5, Units:bar</td></tr>
</table></td></tr>
<tr><td>Make_Supplemental_Links</td><td>See Table 8. This could link to:
Manufacturing compliance reports (e.g., ISO, FDA, UL, ITAR); Digital twin simulation records; Inspection reports or quality control certifications; Machine log files for automation tracking</td></tr>
</table>

Note: The Meta-Framework operates under the assumption that a unique product identifier (Product_ID) is assigned to each tracked item and that a reliable method exists to immutably affix or associate this identifier with the physical or virtual product. The Meta Framework does not specify the Product ID structure, which could take various forms, including but not limited to serial number, digital twin ID, batch identifier, or industry-standard tracking number. The Product_ID field captures the digital representation of the ID, while the physical part of the ID can be sensed as being associated with the object. The only requirement is that the Product_ID must be unique, at least within the applicable ecosystem. The Meta-Framework enables ecosystems to define how this identifier is assigned and maintained, ensuring that traceability records remain accurate, interoperable, and securely linked to the physical or virtual product.

This ensures that traceability records maintain a verifiable cyber-physical link, enabling stakeholders to track, authenticate, and validate product provenance with confidence.

F.4.5. Assemble Record Subclass

An assemble event record includes the attributes of a traceability record and extends them with attributes peculiar to production, with which multiple previous make, assemble, or receive events are associated. This preserves the traceability of a given assembled product at the event of its fabrication or assembly tasks. Assemble events may also provide supplemental links so that traceability may be complemented by contextual or detailed information, as shown in Fig. 22.

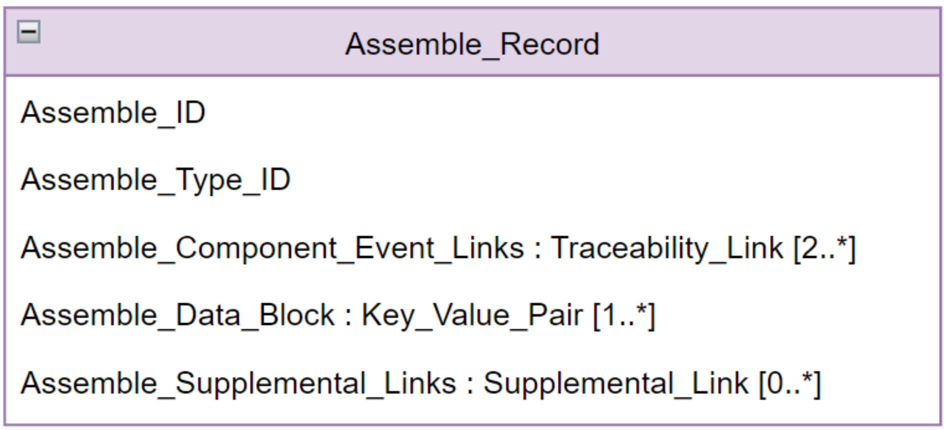

Figure 22. Assemble Record Attribute Structure

The attributes for assemble events are defined in Table 10nbelow:

Table 10. Assemble Record Attribute Definitions

<table>
<tr><th>Data Attribute</th><th>Example Types / Values</th></tr>
<tr><td>Assemble_ID</td><td>String: ASM-2024-001, UUID-987654321, Serial-ABC1234, "DigitalTwin-UUID-001</td></tr>
<tr><td>Assemble_Type_ID</td><td>String: IPC-7711/21, STD-883, UL-508</td></tr>
<tr><td>Assemble_Component_Event_Links</td><td>See Table 7
[component 1], [component 2], …</td></tr>
<tr><td>Assemble_Data_Block</td><td><table>
<tr><th>Key</th><th>Value</th></tr>
<tr><td>Assembly_Method</td><td>Automated SMT Placement</td></tr>
<tr><td>Torque_Spec</td><td>15 Nm</td></tr>
<tr><td>Temperature_Setpoint</td><td>250C</td></tr>
<tr><td>Process_Validation_ID</td><td>QA-00234</td></tr>
</table></td></tr>
</table>

Data Attribute	Example Types / Values
Assemble_Supplemental_Links	See Table 8. This could link to: Quality inspection reports Engineering CAD files Process certification documents Non-destructive test (NDT) results

Note: Like the Product_ID, the Assemble_ID functions as a unique identifier for the assembled product or subassembly, allowing stakeholders to establish a verifiable cyber-physical link between the traceability record and the actual object being tracked. This identifier may take various forms, including a serial number, digital twin ID, batch identifier, or industry-standard tracking number. The Assemble_ID field captures the digital representation of the ID, while the physical part of the ID can be sensed as being associated with the object. The only requirement is that the Assemble_ID must be unique, at least within the applicable ecosystem. The Meta-Framework enables ecosystems to define how this identifier is assigned and maintained, ensuring that traceability records remain accurate, interoperable, and securely linked to the physical or virtual product.

F.4.6. Ship Record Subclass

A ship event record includes the attributes of a traceability record and extends them with attributes peculiar to the transfer of an item, as depicted in Fig. 23. This transfer is envisioned as the movement of products from one location and/or responsible party to another location and/or responsible party.

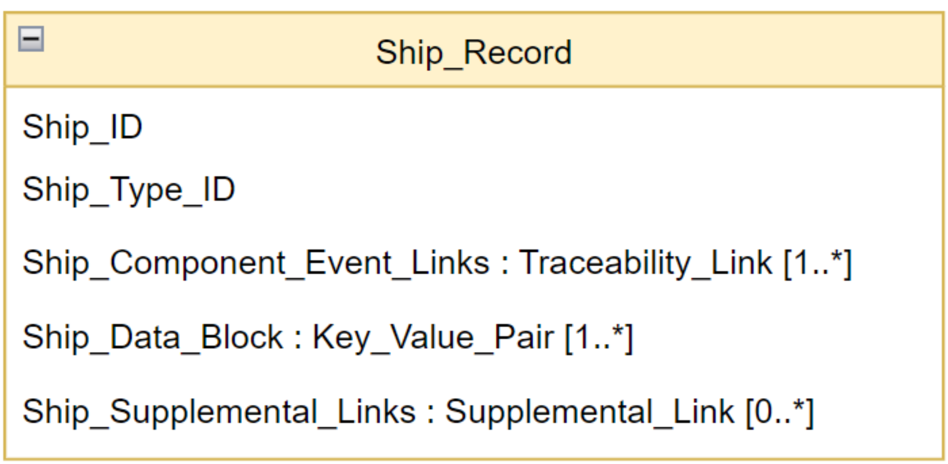

Figure 23. Ship Record Attribute Structure

The attributes for a ship record are defined in Table 10.

Table 11. Ship Record Attribute Definitions

<table>
<tr><th>Data Attribute</th><th>Example Types / Values</th></tr>
<tr><td>Ship_ID</td><td>String: SHIP-2024-001, UUID-987654321, LOGISTICS-45678</td></tr>
<tr><td>Ship_Type_ID</td><td>String: LTL-TRUCK, AIR-FREIGHT, SEA-CONTAINER</td></tr>
<tr><td>Ship_Component_Event_Links</td><td>See Table 7
[Event 1], [Event 2], …</td></tr>
<tr><td>Ship_Data_Block</td><td><table>
<tr><th>Key</th><th>Value</th></tr>
<tr><td>Carrier_Name</td><td>ShipIt</td></tr>
<tr><td>Tracking_Number</td><td>1234567890</td></tr>
<tr><td>Shipment_Mode</td><td>Refrigerated Truck</td></tr>
<tr><td>Estimated_Arrival</td><td>2024-06-10T12:00:00Z</td></tr>
</table></td></tr>
<tr><td>Ship_Supplemental_Links</td><td>See Table 8. This could link to:
Bill of Lading Documents
Customs Declarations
Proof of Delivery (POD)
Carrier Tracking System Links</td></tr>
</table>

F.4.7. Receive Record Subclass

A receive event record includes the attributes of a traceability record and extends them with attributes peculiar to the receipt of items. A ship event and a receive event are expected to match up, although time will elapse between the two events. The receive event takes place at the place of consumption of the item. That is, where the item represented in the receive event will go on to become part of an extended context. This is envisioned to include target operational environments, such as critical infrastructure, as well as more complex fabrication. Figure 24 illustrates this subclass.

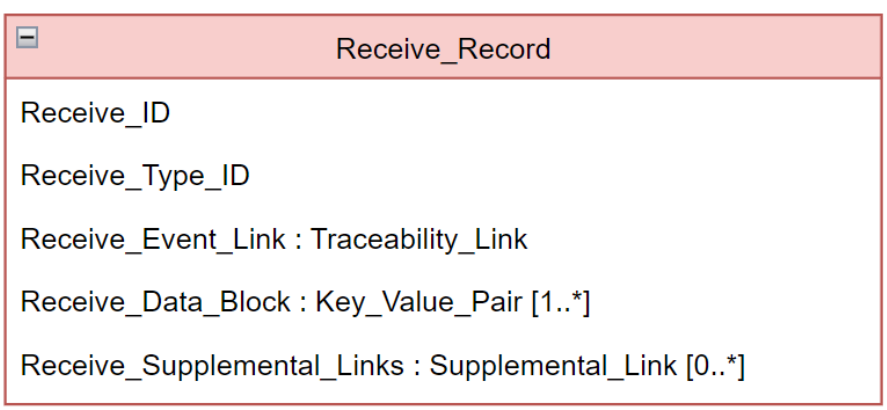

Figure 24. Receive Record Attribute Structure

The attributes for a receive record are defined in Table 12 below:

Table 12. Receive Record Attribute Definitions

Data Attribute	Example Types / Values
Receive_ID	String: RCV-2024-001, UUID-654321987, WAREHOUSE-45678
Receive_Type_ID	String: INCOMING-INSPECTION, COLD-CHAIN-RECEIPT, SECURE-TRANSFER
Receive_ Event_Link	See Table 7 [Ship Event]
Receive_Data_Block	**Key**: **Value** **Receiving_Location**: Warehouse-3A **Inspection_Result**: "Accepted" or "Rejected" **Temperature_Log**: {"Min": "-5C", "Max": "2C"} **Delivery_Condition**: Damaged Packaging
Receive_Supplemental_Links	See Table 8. This could link to: Quality inspection reports Customs clearance certificates Photographic evidence of shipment condition Proof of delivery (POD) records

F.4.8. Employ Record Subclass

In Fig. 25, an employ event record includes the attributes of a traceability record and extends them with attributes peculiar to the installation of an item into an operational environment. An employ event traces back to a receive event as an initial step into the overall traceability of pedigree and provenance of the operational environment's components.

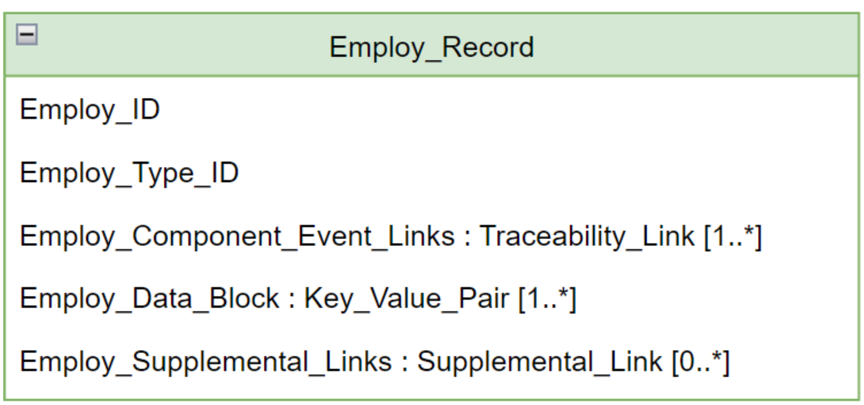

Figure 25. Employ Record Attribute Structure

The attributes for an employ record are defined in Table 12 below:

Table 13. Employ Record Attribute Definitions

<table>
<tr><th>Data Attribute</th><th>Example Types / Values</th></tr>
<tr><td>Employ_ID</td><td>String: EMPLOY-2024-001, UUID-654321987, DEPLOYMENT-45678</td></tr>
<tr><td>Employ_Type_ID</td><td>String: LOW-IMPACT-SYSTEM, MODERATE-IMPACT-SYSTEM, HIGH-IMPACT-SYSTEM</td></tr>
<tr><td>Employ_Component_Event_Links</td><td>See Table 7
[Event 1], [Event 2], …</td></tr>
<tr><td>Employ_Data_Block</td><td><table><tr><th>Key</th><th>Value</th></tr><tr><td>Deployment_Location</td><td>Data Center 3B</td></tr><tr><td>Configuration_ID</td><td>CFG-125A</td></tr><tr><td>Security_Compliance_Check</td><td>"Passed" or "POAM"</td></tr></table></td></tr>
<tr><td>Employ_Supplemental_Links</td><td>See Table 8. This could link to:
Installation and deployment logs
Configuration settings and baseline documentation
Acceptance testing and verification records
Security compliance assessments</td></tr>
</table>

F.5. Conclusion

This appendix outlines a possible technical structure. Serialization strategies and cryptographic validation mechanisms are described in Appendix G. Combined, these outline possible ways to implement traceability records within the Meta-Framework that warrant further study and experimentation. By using common traceability record structures and ensuring cryptographic integrity, the framework enables secure, interoperable, and verifiable traceability solutions across diverse supply chain ecosystems. Further implementation guidelines can be found in ecosystem-specific governance documents or technical reference materials.

Appendix G. Technical Details and Governance Considerations

This appendix provides technical guidelines and governance considerations for implementing the Meta-Framework. It serves as a reference for technical implementers, ecosystem operators, and other stakeholders by outlining key practices for serialization formats, cryptographic validation, data retention policies, and interoperability mechanisms. The details presented here support organizations in deploying traceability solutions while maintaining security, privacy, data integrity, and compliance with industry governance standards.

G.1. Serialization and Data Formats

To support cross-ecosystem interoperability and enable traceability record validation, the Meta-Framework relies on deterministic serialization—a process where structured data is consistently encoded into a canonical form such that the same input always results in the same output byte-for-byte. This consistency is critical when computing and verifying cryptographic hash values used in Traceability Links (see Appendix F), particularly when a record is retrieved based on a known hash.

The Meta-Framework does not mandate any specific serialization technology but encourages ecosystems to adopt serialization formats that support determinism, clarity, and efficiency. Example classes of serialization formats include:

- **Stored Original Serialization:** Ecosystems may choose to persist the original byte-level representation of the traceability record exactly as it was submitted. This ensures that future retrievals match the original record used to compute the associated hash value, supporting deterministic validation without re-serialization.
- **Canonical Text-Based Serialization:** Structured text formats (e.g., JSON, XML, CBOR in canonical mode) that enforce consistent ordering of attributes, encoding rules, and whitespace to ensure hash reproducibility. These formats prioritize readability and interoperability.
- **Canonical Binary Serialization:** Compact, efficient formats designed to preserve attribute ordering and structural integrity in a smaller binary footprint. These are useful in environments with bandwidth or storage constraints.

Ecosystem implementers should choose serialization strategies that align with their operational needs while ensuring deterministic hashing for traceability link validation. If a retrieved record differs in encoding from the version used to compute its hash, verification will fail. Consistent serialization is therefore essential to preserve the integrity and verifiability of traceability chains across ecosystems.

G.2. Cryptographic Validation and Security

Maintaining the integrity and authenticity of traceability records is critical to ensuring trust across the supply chain. The Meta-Framework supports cryptographic validation techniques, including:

- **Hash-based Integrity Checks:** Each traceability record includes a cryptographic hash to detect tampering and ensure data immutability.
- **Access Hash Authentication:** Enables authorized stakeholders to retrieve traceability records by using precomputed hashes as authentication tokens rather than traditional credentials.
- **Digital Signatures:** Ecosystem participants may use digital signatures to authenticate traceability records, verifying the identity of the entity that generated the record.

By implementing these security measures, organizations can prevent unauthorized modifications to traceability data and establish a trust-based traceability system.

G.3. Governance and Data Retention Policies

Trusted data repositories operate under governance frameworks that establish data retention policies, access control mechanisms, and compliance requirements. Key governance considerations include:

- **Data Retention and Lifecycle Management:** Governance frameworks should define policies for how long traceability records are retained and how data is securely archived, de-identified, or disposed of at the end of its lifecycle. These policies should balance operational traceability needs with data minimization principles, privacy protections, and contractual or stakeholder expectations, particularly when data includes personal or sensitive operational information.
- **Access Control and Authentication:** Ecosystems must implement role-based access controls (RBAC) and identity verification mechanisms to restrict unauthorized access to traceability records.
- **Audit and Compliance Mechanisms:** Governance frameworks should include periodic audits and compliance reviews to ensure traceability data is managed in accordance with established policies.
- **Data Quality, Integrity, and Accountability:** Organizations should ensure that their data governance activities across the ecosystem are accurate, consistent, complete, and trustworthy. This includes assigning clear data stewardship roles responsible for maintaining data quality, enforcing standards, and ensuring ethical and compliant data handling throughout the data lifecycle.
- **Metadata and Provenance Tracking:** Governance frameworks should require the capture of metadata (e.g., source, timestamp, access history) to enable traceability, support auditability, and manage the lineage of data across the supply chain.
- **Third Parties and Multi-Suppliers Data Handling:** Organizations should ensure that third parties and suppliers follow common governance policies through contracts, data sharing agreements, and oversight mechanisms. This includes requiring comparable security and privacy controls [5], maintaining traceability of data flows, and reporting incidents or changes that may affect data integrity or compliance.

G.4. Interoperability Mechanisms

To facilitate seamless traceability data exchange between different ecosystems, the Meta-Framework incorporates interoperability mechanisms, including:

- **Traceability Links:** Enable the discovery of predecessor traceability records, ensuring that supply chain event data remains verifiable across organizations.
- **Supplemental Data References:** Provide additional, externally linked information that may be required for risk assessment, compliance, or verification purposes.
- **Ecosystem Interface:** Defines the mechanism (e.g., Application Programming Interface (API) framework) to allow stakeholders to query and retrieve traceability records efficiently.

These interoperability mechanisms ensure that supply chain participants can securely share and retrieve traceability data while maintaining compliance with industry-specific standards and governance policies.