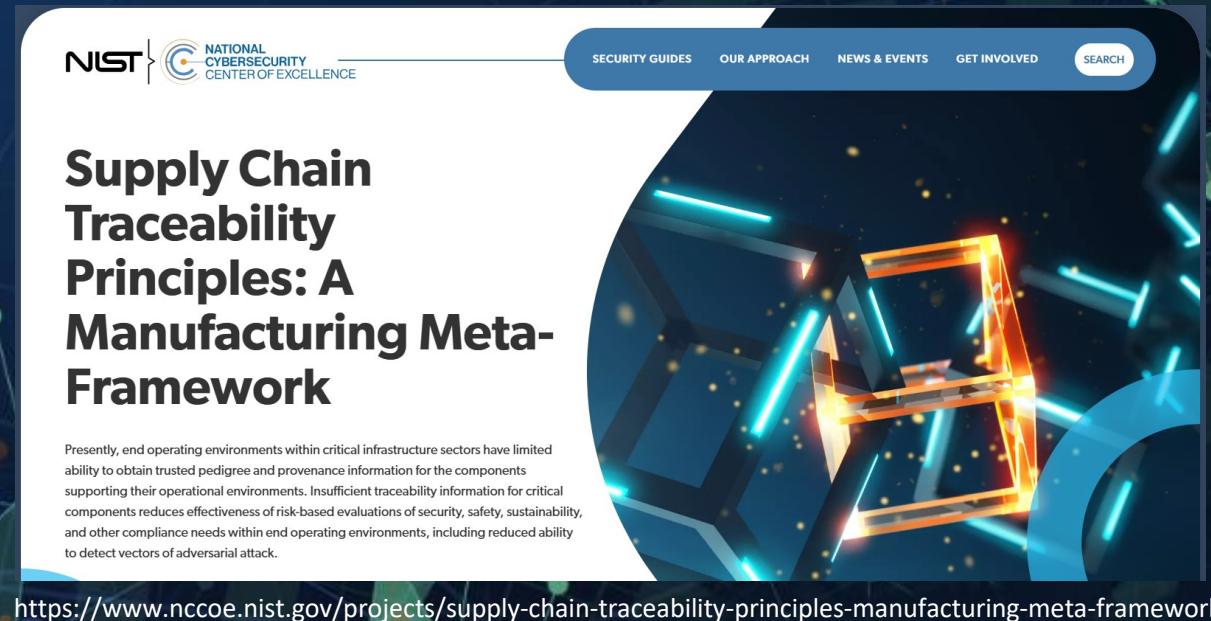


NIST IR 8536: Supply Chain Traceability Principles: A Manufacturing Meta-Framework

Overview of NIST Internal Report (IR) 8536

Authors: Michael Pease (NIST), Evan Wallace (NIST);
Harvey Reed (MITRE), Robert Martin (MITRE),
Dr. Vivian L. Martin (MITRE), Steve Granata (MITRE)

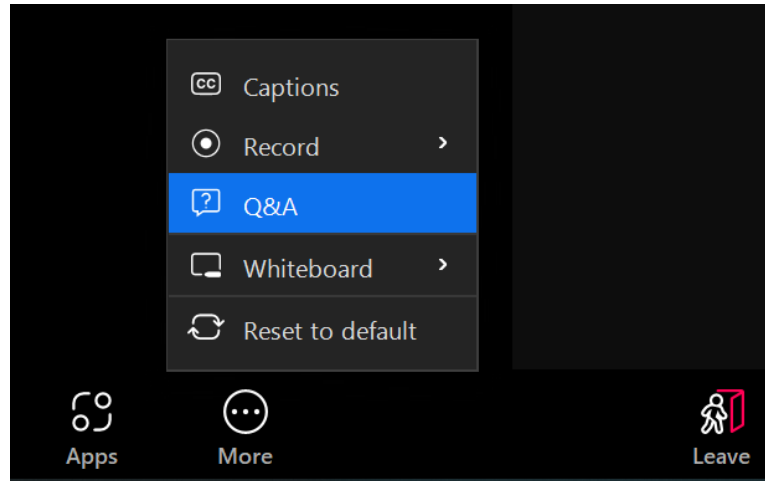
Published: September 2026



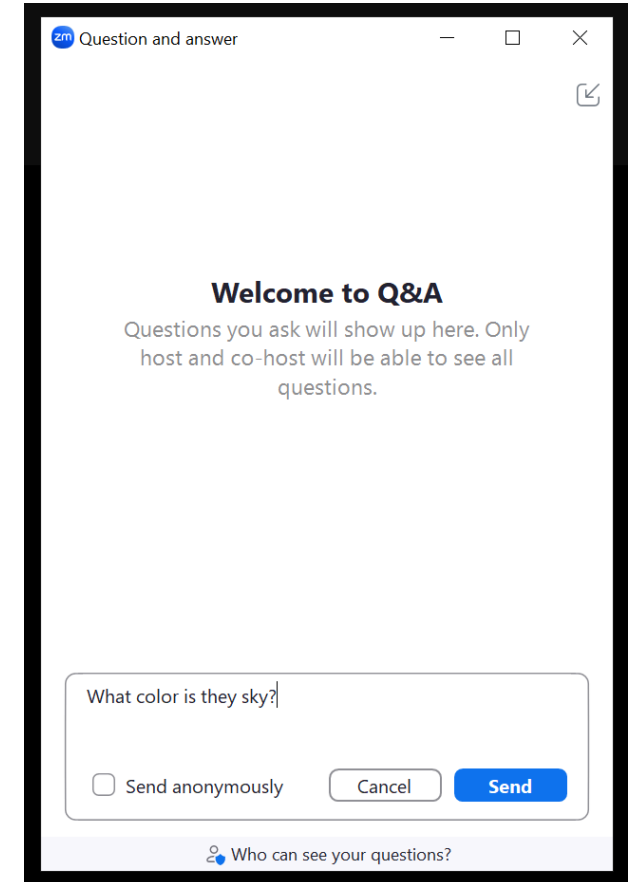
Submitting Questions

Please use the Q&A function to enter your questions.

We will do our best to answer all questions during the Q&A.



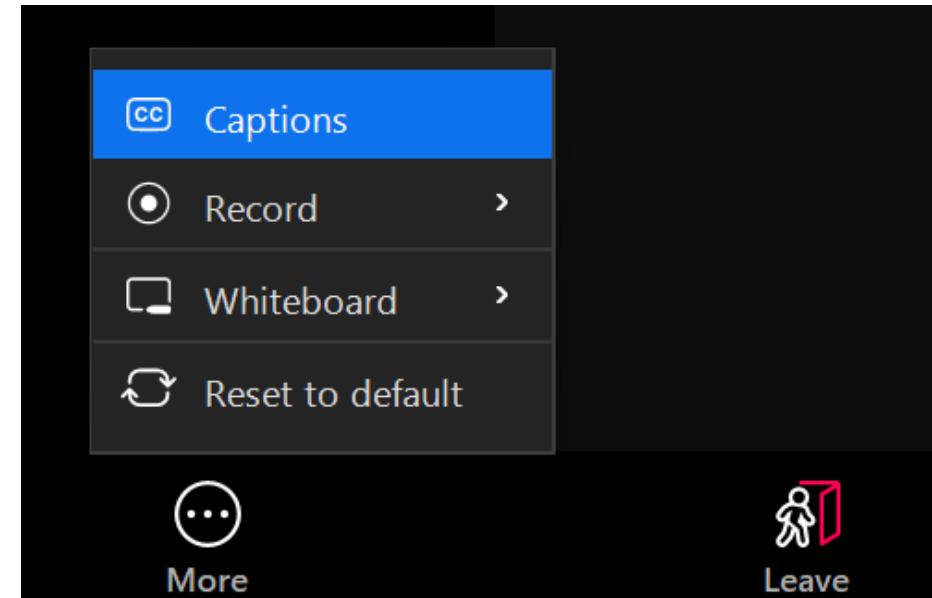
1. To open the Q&A function, click on “More” at the bottom of the screen and select the “Q&A” option.



2. Type your question in the text box and click Send

Enabling Closed Captions

To open enable captioning during the event, click on “More” at the bottom of the screen and select the “Captions” option.



Agenda

- 01** Quick Overview of the NCCoE
- 02** Project Overview
- 03** Overview of Supply Chain Traceability Principles
- 04** Overview of the Manufacturing Meta-Framework
- 05** Summary/Status of the Reference Implementation
- 06** Conclusion and Discussions (Q&A)



WHO WE ARE

A solution-driven, collaborative hub addressing complex cybersecurity problems



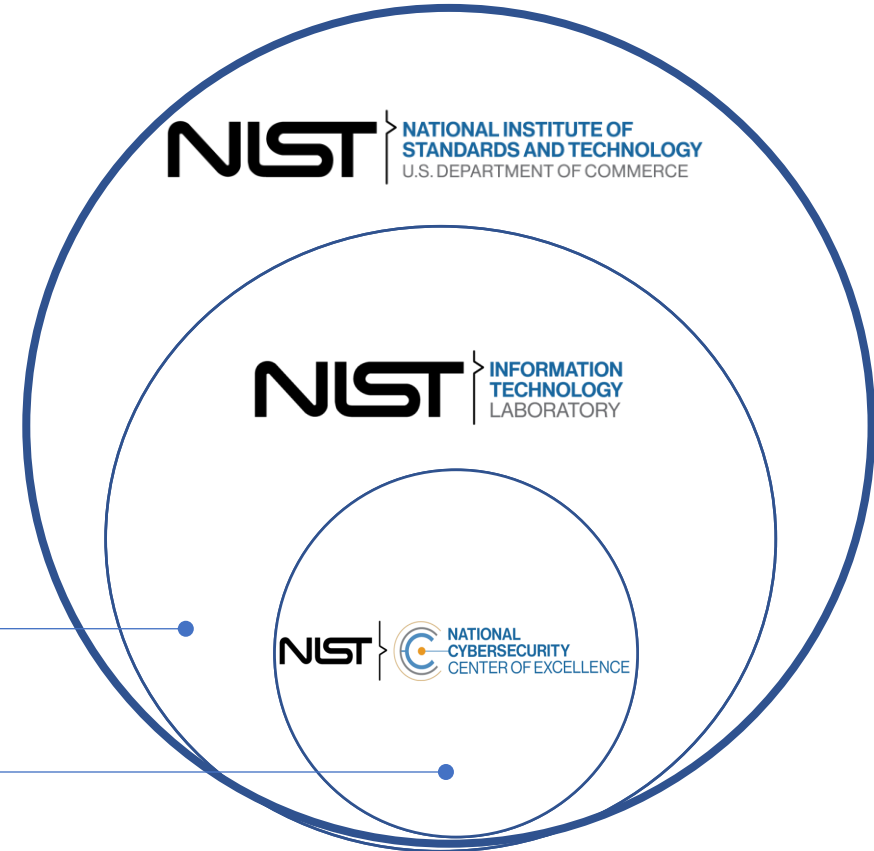
Who We Are

Part of NIST, the NCCoE has access to a foundation of expertise, resources, relationships, and experience.

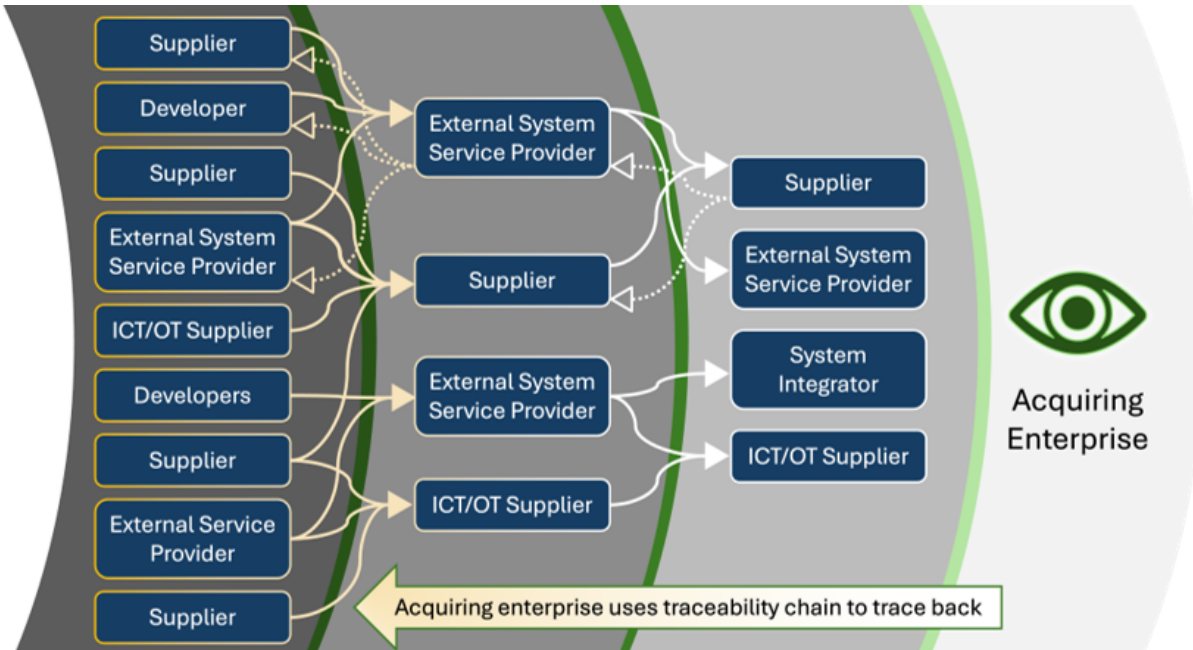
NIST is a **non-regulatory** agency. Our guidance is **voluntary**.

Information Technology Laboratory

Applied Cybersecurity Division



PROJECT HISTORY AND MOTIVATION



Modified from NIST SP 800-161r1

01

OPAQUE SUPPLY CHAIN NETWORKS

Visibility falls rapidly beyond direct suppliers.

02

SUPPLY CHAIN INFORMATION ASYMMETRY

Acquirers need evidence; suppliers must protect proprietary data.

03

INCOMPATIBLE SUPPLY CHAIN TRACEABILITY ECOSYSTEMS

Industries use different standards, repositories, and governance.

04

SCRM DECISION PRESSURE

Counterfeits, tampering, disruptions, and hidden dependencies demand defensible action.

The paper asks a practical supply chain question: how can organizations verify pedigree and provenance without centralizing every supplier's data?

DEFINING THE VOCABULARY BASELINE



Pedigree: Data that validates a product's internal composition

Example: The material composition of a component, or the specific library versions within a software application.

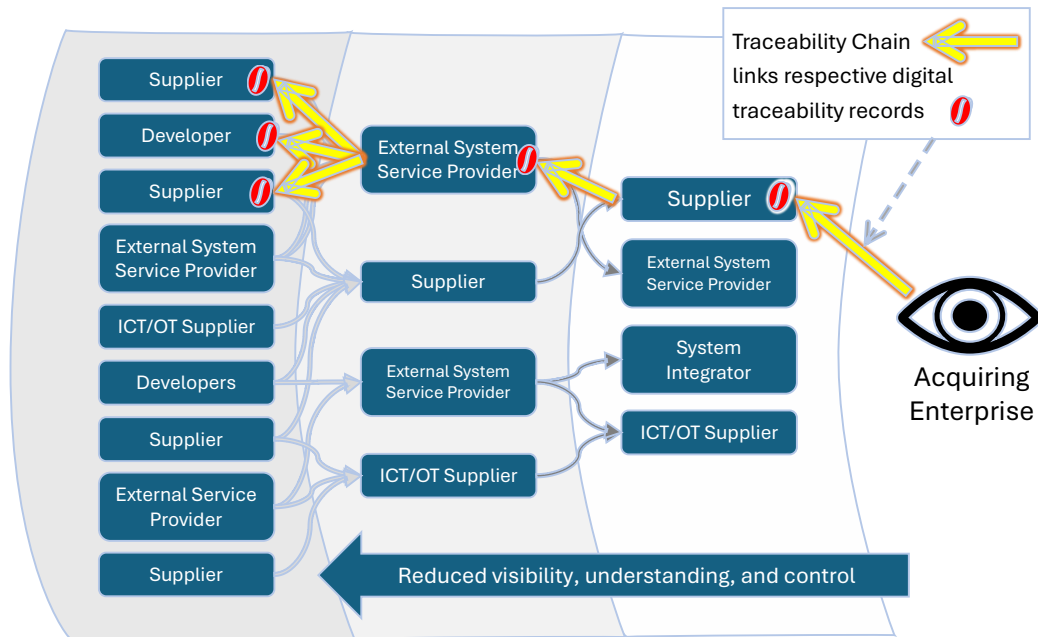


Provenance: The continuous, chronological history of an item's origin, development, ownership changes, locations, and physical transfers over time.



Traceability: The operational enabler; the underlying capability to track and verify pedigree and provenance data across distinct supply chain networks.

PROJECT CONTRIBUTION



01

PRINCIPLES

Nine cross-sector principles explain what good traceability must accomplish and why.

02

META-FRAMEWORK

Event templates, record structure, cryptographic links, and federated querying translate the principles into architecture.

03

REFERENCE IMPLEMENTATION

An open-source Python MVP demonstrates traceability across three independently governed ecosystems.

The publication is both an architectural compass and a practical starting point—not a new compliance mandate.

SCOPE AND BOUNDARIES

Use the paper as a voluntary foundation—not as a prescriptive standard

THE REPORT DOES

- Complement existing industry standards and traceability efforts.
- Focus on inter-organizational product handoffs through initial Employ.
- Provide a conceptual basis for acquirer SCRM use cases.
- Address discrete manufacturing and software most directly.

THE REPORT DOES NOT

- Replace established technical standards or industry data models.
- Create a formal regulatory or compliance mandate.
- Require a centralized repository or universal payload schema.
- Fully resolve post-deployment lifecycle and all continuous-flow use cases.

ORGANIZING THEMES:

VALUE-DRIVEN PARTICIPATION & RESILIENCE

Theme 1: Value-Driven Participation (Principles 1–3):

- **Decision-Centric Traceability:** Data sharing must focus on supporting specific organizational SCRM choices, regulatory thresholds, and risk decisions, avoiding unnecessary data hoarding.
- **Proportional Scrutiny:** The depth and resolution of traceability data should scale proportionally with an item's safety-criticality and mission impact.
- **Incentive-Aligned Participation:** Economic and operational incentives are aligned to motivate upstream participants to generate and share records without requiring uniform capabilities.

Theme 2: Pedigree and Provenance Resilience (Principles 4–6):

- **Evidence-Based Provenance:** Systems must utilize bounded disclosures and alternative evidence (such as third-party audits or certifications) when direct digital event telemetry is unavailable.
- **Measure and Communicate Traceability Gaps:** Rather than treating missing data as a catastrophic failure, frameworks should explicitly measure and communicate known data gaps (e.g., states marked as "unknown" or "withheld").
- **Lifecycle-Oriented Provenance and Accountability:** Traceability extends across the product's lifecycle to reflect modifications, firmware updates, and operational events.

Theme 3: Decentralized Trust (Principles 7–9):

- **Verifiable Organization Attribution:** Every traceability record must structurally declare the legally identifiable business entity and specific facility responsible for the event using standard identifiers (e.g., UEI, LEI, GLN), while avoiding individual employee data.
- **Cyber-Physical Linkage:** Digital records must be firmly anchored to their respective physical goods, digital assets, or batches using persistent markers (e.g., barcodes, tamper-evident seals, or cryptographic hashes).
- **Interoperability Over Uniformity:** Prioritizing data encapsulation patterns, allowing individual industry ecosystems to express internal payloads in their native formats while utilizing standardized links to bridge cross-sector boundaries.

Use the paper's vocabulary when tailoring the principles to supply chain risk and sector needs.

Principles provide context for decision-making... They serve as an architectural compass rather than a rigid compliance checklist.

VALUE-DRIVEN PARTICIPATION

Traceability should support decisions, scale with consequence, and create reasons for suppliers to participate.

PRINCIPLES IN THIS GROUP

1. Decision-Centric Traceability
2. Proportional, Risk-Scaled Traceability
3. Incentive-Aligned Participation



Principle 1. Decision-Centric Traceability

Notional Example: Continuous Process Sourcing – Treatment Chemicals for Safe Drinking Water Act Compliance

THE OLD WAY: MANUAL & OPAQUE

Manual review of unstructured, bulk compliance documentation

- ✗ Unstructured documents
- ✗ Difficult to trace
- ✗ Time-consuming
- ✗ Higher compliance risk
- ✗ Limited visibility

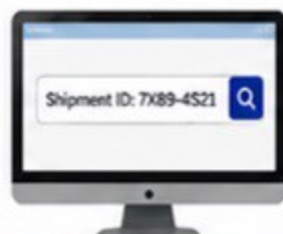


Slow. Opaque. Risky.

THE META-FRAMEWORK: QUERY, TRACE, VALIDATE

1 QUERY SHIPMENT

Query traceability records for the specific shipment.



Structured. Linked. Queryable.

PEDIGREE INFORMATION

-  Purity $\geq 99.5\%$
-  Regulatory Certifies EPA Compliant
-  Cold-Chain $2-8^{\circ}\text{C}$ Unbroken
-  Chain of Custody Unbroken
-  Test Results COA Linked

2 TRACE THE SUPPLY CHAIN

Trace links back through the supply chain to the source.



3 OBTAIN STRUCTURED HISTORICAL DATA

Historical data provided in a structured, linked format.

SHIPMENT SUMMARY	
✓ Shipment ID	7X89-4S21
✓ Product	Sodium Hypochlorite 12.5%
✓ Batch	B4F-7782
✓ Receipt Date	May 21, 2024
✓ Quantity	22,000 lbs
✓ Purity	$\geq 99.5\%$
✓ Cold-Chain	$2-8^{\circ}\text{C}$ Unbroken
✓ COA	Linked
✓ EPA Compliance	Compliant
✓ Chain of Custody	Unbroken

VALIDATE WITH CONFIDENCE

Using structured, historical pedigree data, teams efficiently validate against thresholds.



ENGINEERING

Validates purity, specifications, and handling conditions.

✓ Thresholds Met



LEGAL

Confirms regulatory documents and chain of custody.

✓ Approved



PUBLIC HEALTH

Confirms safety for public consumption and risk thresholds.

✓ Safe for the Public

PEDIGREE & PROVENANCE RESILIENCE

Useful provenance must survive protected information, missing data, analog evidence, and product change.

PRINCIPLES IN THIS GROUP

4. Evidence-Based Provenance, Not Perfect Transparency

5. Measure and Communicate Traceability Gaps and Trust Boundaries

6. Lifecycle-Oriented Provenance and Accountability





Principle 4. Evidence-Based Provenance, Not Perfect Transparency

Notional Example: Commodity Sourcing and Non-Digital Origins (Bulk Leather)



Policy Goal
Enable practical provenance.
Rely on evidence.
Strengthen responsible supply chains.

THE CONTEXT

Automotive manufacturers require provenance for materials like leather to meet quality, regulatory, and sustainability commitments.

For many bulk commodities, a fully digitized chain back to the individual ranch or farm is not practical.



DESIGN PRINCIPLES

- ✓ **Evidence over perfection.**
Accept credible, verifiable alternatives.
- ✓ **Risk-based acceptance.**
Match evidence depth to material risk and supply complexity.
- ✓ **Transparency of evidence.**
Document what evidence supports the attestation.
- ✓ **Accountability built in.**
Attestations carry responsibility and are subject to audit.

Accept verifiable evidence when perfect digital continuity is not feasible. Trust evidence. Manage risk. Support practical sourcing.



TYPICAL SUPPLY PATH (Non-Digital Origins)



EVIDENCE PROVIDED BY BULK LEATHER SUPPLIER

VERIFIED ATTESTATION OF ORIGIN

We attest that the leather supplied in this shipment originates from cattle raised in the declared country/region in compliance with applicable laws and standards.

Authorized Signatory Date: May 6, 2025

EVIDENCE REFERENCES (NOT EXHAUSTIVE)

- Tannery intake records (physical)
- Country of origin declarations
- Third-party certification(s) (e.g., LWG, ISO, SABOC)
- Veterinary / trade documentation
- Supplier due diligence files
- Audit reports (when available)

ACQUIRER VERIFICATION & ASSESSMENT

EVALUATE THE EVIDENCE

- ✓ Authenticity of attestation (issuer, signature, date)
- ✓ Relevance and coverage of referenced records
- ✓ Credibility of certifications and issuers
- ✓ Historical performance and audit results
- ✓ Consistency with known risk indicators

RISK ASSESSMENT



DECISION

Evidence is sufficient to establish acceptable provenance for this shipment based on current risk tolerance and materiality.

RECORD & TRACEABILITY CAPTURE

- Store attestation and references
- Link to shipment and lot/batch
- Record evidence type, issuer, and date
- Maintain for audits and reporting

Evidence captured.
Provenance established.
Confidence documented.

OUTCOMES BETTER DECISIONS. REAL-WORLD IMPACT.

- Practical & Scalable**
Enables provenance for materials where digital end-to-end traceability is not feasible.
- Risk Managed**
Evidence quality aligned with risk to support responsible sourcing decisions.
- Regulatory & ESG Ready**
Supports compliance, reporting, and sustainability commitments.
- Supplier Inclusion**
Allows capable suppliers to participate without prohibitive technology barriers.
- Continuous Improvement**
Encourages stronger evidence over time through engagement and incentives.

DECENTRALIZED TRUST

Trust comes from attributable records, strong item linkage, integrity validation, and interoperability.

PRINCIPLES IN THIS GROUP

7. Verifiable Organization Attribution

8. Cyber-Physical and Digital Linkage

9. Interoperability Over Uniformity





DEFENSE SUPPLY CHAIN

Many standards. One mission.

Principle 9. Interoperability Over Uniformity

Notional Example: Widget Traceability Across ISO 8000 and GS1 EPCIS



Policy Goal

Enable traceability across any two data standards by encapsulating, linking, and normalizing for trusted use across the supply chain.

THE CONTEXT

Suppliers and acquirers use different data standards based on their systems, industries, and missions. Forcing uniformity creates high costs and barriers to entry.

Interoperability over uniformity allows each party to use the standard that works for them—while still enabling seamless and trustworthy data exchange.



Widget

DESIGN PRINCIPLES

- Do not require suppliers to abandon existing standards.
- Encapsulate, do not translate at the source.
- Declare the data format explicitly in the payload.
- Enable automated parsing based on declared format.
- Preserve semantic meaning and data integrity end-to-end.
- Promote open, extensible interfaces and schemas.

END-TO-END LIFECYCLE: WIDGET TRACEABILITY ACROSS TWO DATA STANDARDS



SUPPLIER SIDE (MAKE) — ISO 8000

Example: ISO 8000 Make Record (Simplified)



```
{
  "eventType": "make",
  "widgetId": "WID-8A3F-9C71-2D4B",
  "manufacturer": "Acme Manufacturing",
  "productionTimestamp": "2025-05-15T08:30:00Z",
  "lot": "LOT-250515-001",
  "material": "7075-T6 Aluminum",
  "specification": "SPEC-WID-7075-REV-A"
}
```

Supplier systems and processes remain unchanged.

MAKE RECORD ENVELOPE — ISO 8000

ISO 8000 Make Event Envelope (Example)

```
{
  "eventId": "EVT-MAKE-2025-05-15-0001",
  "eventType": "make",
  "format": "ISO 8000",
  "sender": "Acme Manufacturing",
  "timestamp": "2025-05-15T08:30:00Z",
  "receiver": "Prime Defense Systems",
  "payload": {
    "dataFormat": "ISO 8000",
    "record": "base64-encoded ISO 8000 data"
  },
  "signature": "MEUCICQ...",
  "hash": "b41a6e2f3c9a4e..."
}
```

The payload is intact, signed, and its format is declared.

TRANSMIT SHIP RECORD — GS1 EPCIS

GS1 EPCIS Ship Event Envelope (Example)

```
{
  "eventId": "EVT-SHIP-2025-05-15-0001",
  "eventType": "ship",
  "format": "GS1 EPCIS 2.0",
  "sender": "Acme Manufacturing",
  "receiver": "Prime Defense Systems",
  "timestamp": "2025-05-15T10:15:00Z",
  "payload": {
    "dataFormat": "GS1 EPCIS 2.0",
    "record": "base64-encoded EPCIS event"
  },
  "signature": "MEUCICQ...",
  "hash": "d937fe8c1b24ec..."
}
```

The payload is intact, signed, and its format is declared.

RECEIVER PROCESSING & LINKING

Identify Both Formats
Detect ISO 8000 and GS1 EPCIS envelopes.

Parse & Extract
Use registered parsers to extract native data from each format.

Normalize to Internal Model
Map both records to a common internal schema.

Link via Widget ID
Resolve shared Widget ID and cryptographically link MAKE → SHIP.

Validate & Integrate
Validate linkage integrity and integrate into acquirer systems.

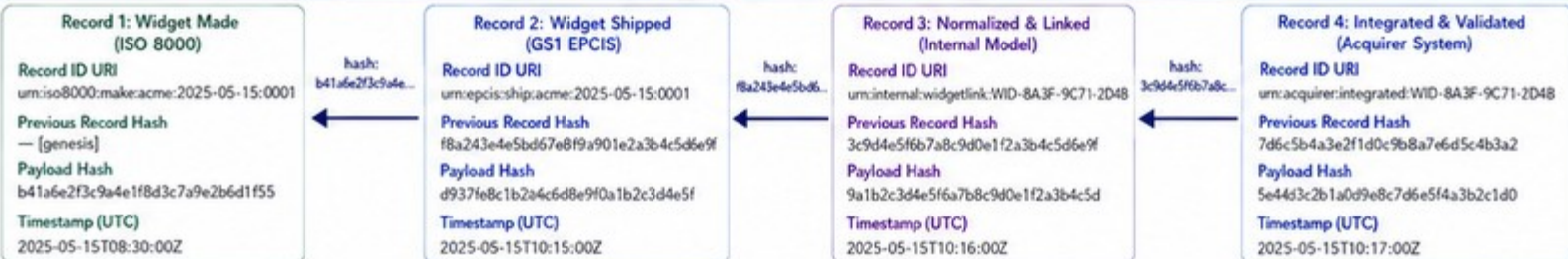
NORMALIZED DATA (INTERNAL MODEL)

Entity	Widget
Widget ID	WID-8A3F-9C71-2D4B
Manufacturer	Acme Manufacturing
Production Timestamp	2025-05-15T08:30:00Z
Lot	LOT-250515-001
Material	7075-T6 Aluminum
Specification	SPEC-WID-7075-REV-A
Sender (Ship)	Acme Manufacturing
Receiver (Ship)	Prime Defense Systems
Ship Timestamp	2025-05-15T10:15:00Z
Location (Ship)	Austin, TX, USA
Disposition (Ship)	in_transit
Linked Records	MAKE: EVT-MAKE-...0001 SHIP: EVT-SHIP-...0001

Integrated into Acquirer Systems



RESOLVABLE LINKAGE CHAIN WITH CRYPTOGRAPHIC INTEGRITY



Both native records remain intact. Cryptographic links and the shared Widget ID provide tamper-evident integrity across two different standards.

WHY THIS MATTERS

- No forced retooling of supplier systems.
- Lower cost and faster onboarding.
- End-to-end visibility across all tiers.
- Integrity proven by cryptographic links, not by storage.
- Stronger trust for patient safety and mission assurance.
- Scales to future technologies and new partners.

WHY A META-FRAMEWORK

“Meta” means common structural patterns—not one mandatory technology

PRESERVE

- Industry standards
- Internal systems
- Repository choices
- Ecosystem governance

COMMON PATTERNS

- ENCAPSULATE
- LINK
- QUERY

ENABLE

- Cross-sector retrieval
- Traceback across trust boundaries
- Cryptographic validation
- Selective disclosure

Interoperability is achieved at the record and link boundaries while payload data remains aligned with sector needs.

META-FRAMEWORK ARCHITECTURE

The Meta-Framework converts principles into four architectural components

01

EVENT RECORDS

Capture accountable supply-chain milestones and pedigree payloads.

02

TRACEABILITY LINKS

Point backward to predecessor records using retrieval data and expected hashes.

03

FEDERATED ECOSYSTEMS

Allow independent governance, storage, access, and retention.

04

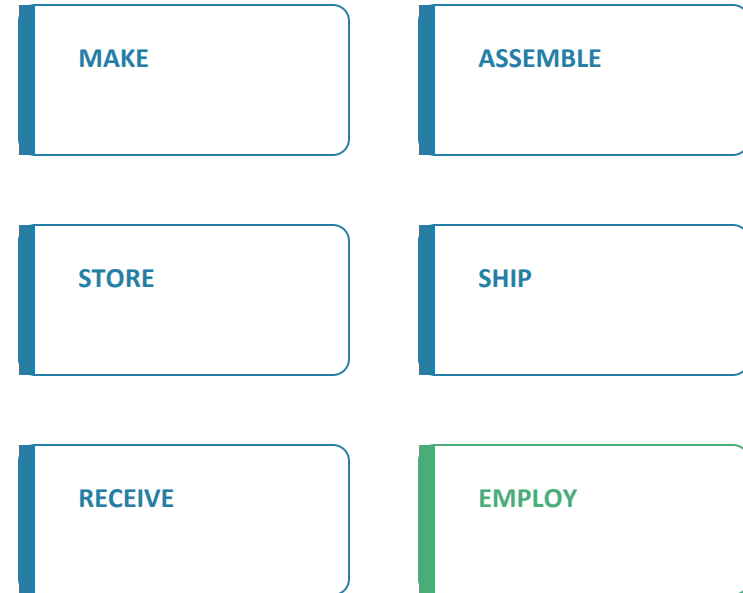
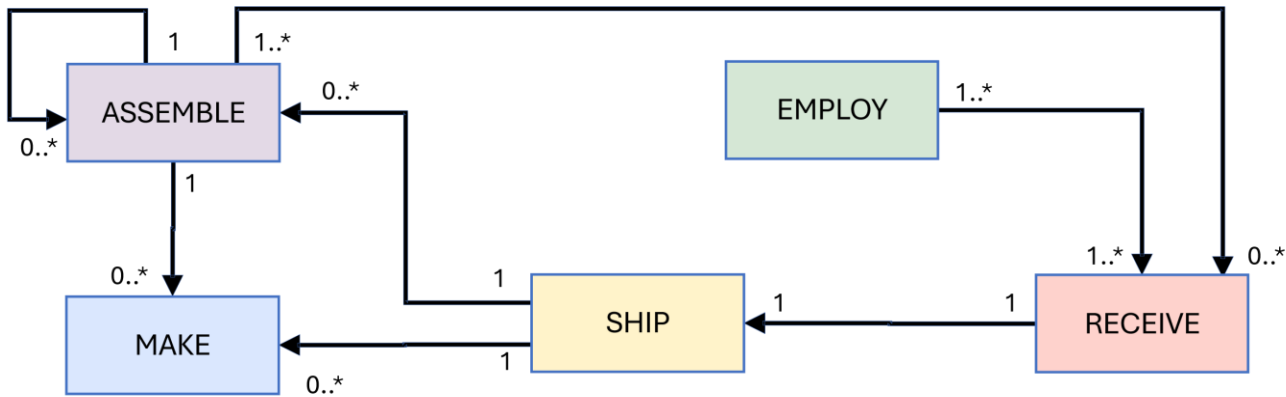
PROVENANCE QUERY

Walk and validate the chain to support an SCRM decision.

The architecture supports verifiable, accessible, and traceable records without exposing a supplier's full operational environment.

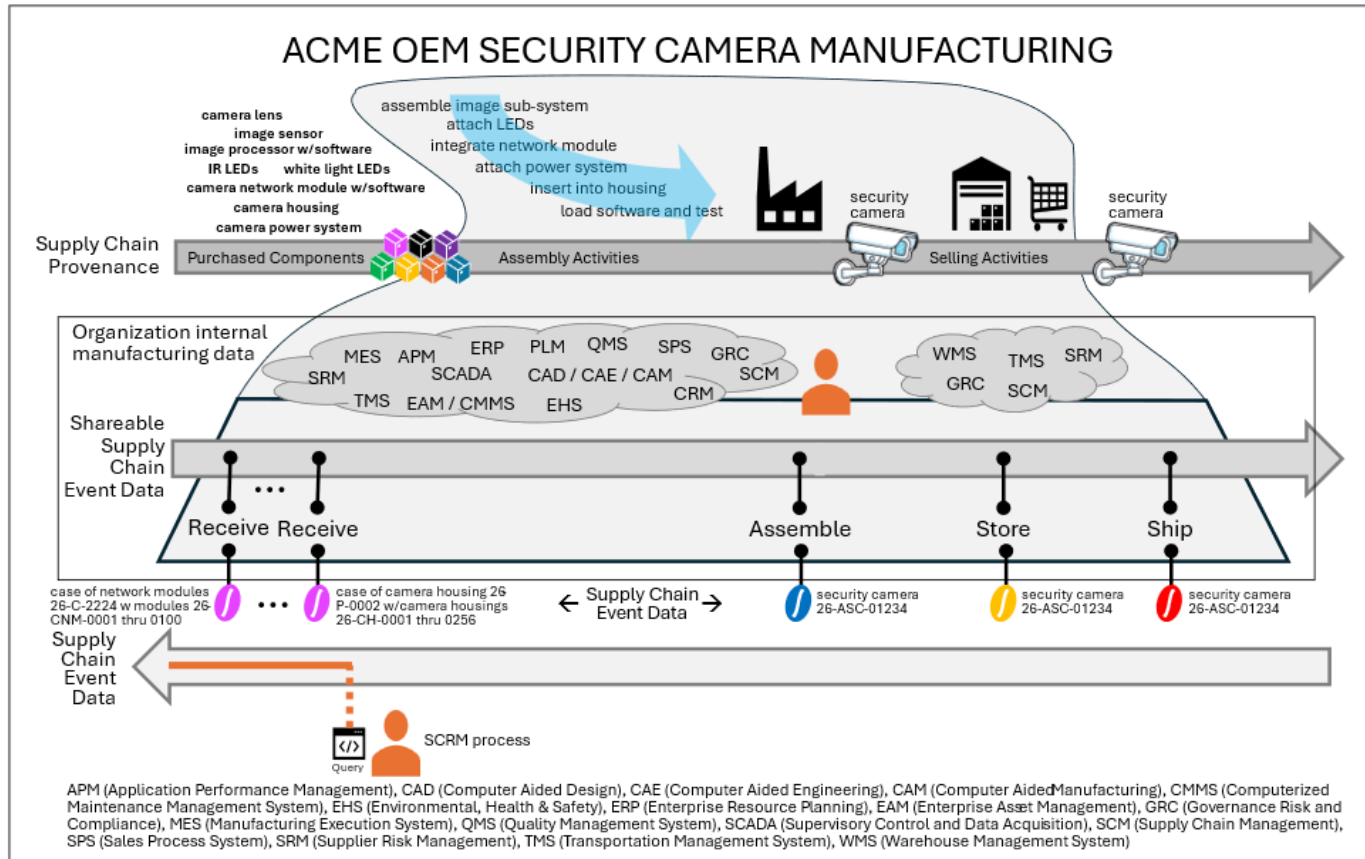
SUPPLY CHAIN EVENTS

Six event categories establish a common product-lifecycle language



Successor records point backward to the events that created, transformed, stored, transferred, or deployed the tracked entity.

STRUCTURAL ELEMENTS OF THE META-FRAMEWORK



A High-Level Blueprint: The framework leverages common structural data patterns to harmonize diverse traceability mechanisms without replacing existing standards.

Core Abstraction Pattern: Translates internal, proprietary manufacturing-execution steps into shareable, high-level supply-chain event data records.

Product-Instance Visibility: Moves beyond broad process-level audits (e.g., ISO 9001) to provide verifiable data directly to the specific instance of the acquired product.

NIST IR 8536 Figure 5: Abstracting Internal Manufacturing Data into Shareable Supply Chain Events

TEMPLATED RECORD STRUCTURE

A traceability record separates routing metadata from flexible pedigree data

RECORD ID

Precise reference

EVENT + TIME

Lifecycle and chronology

ORGANIZATION

Accountable author and facility

TRACKED ENTITY

Physical, digital, or batch anchor

TRACEABILITY LINKS

Pointers to predecessor records

DATA TYPE + PAYLOAD

Sector-specific pedigree evidence

SUPPLEMENTAL REFERENCES

Optional gated certifications and reports

Consistent envelope · flexible supply chain payload

TRACEABILITY LINK ANATOMY

Each traceability link carries what is needed to retrieve and validate its predecessor

01

LOCATION

Where the predecessor record can be obtained.

02

QUERY PARAMETERS

The precise information required to request that record.

03

CRYPTOGRAPHIC HASH

The expected hash used to detect subsequent alteration.

A link acts as a targeted retrieval mechanism—not a grant of broad access to the upstream repository.

CONCEPTUAL MECHANICS: UNIDIRECTIONAL POINTERS & GATED DATA

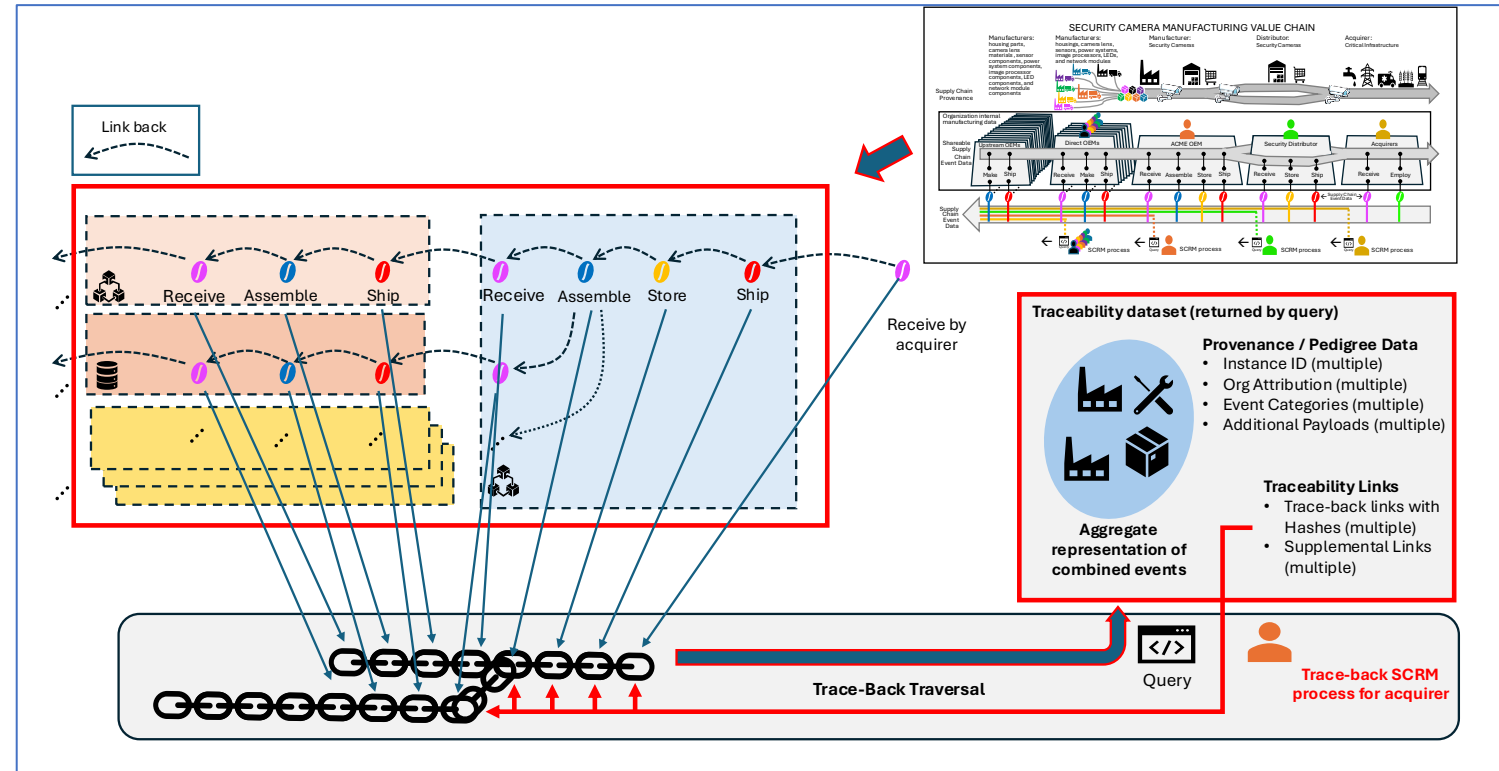
Unidirectional Linkage & Integrity: Digital links point backward to predecessor event records (e.g., a Receive points to Ship), embedding cryptographic hashes ensuring tamper-evident without exposing a supplier's downstream logistics.

Instance-Level Root of Trust: Unlike probabilistic, process-level audits, verifiable records and organizational attributions are securely anchored to the exact specific instance of the acquired component.

Repository Neutrality: There are no centralized repository requirements; data integrity is maintained within the records themselves, with access mediated seamlessly via link-based queries.

SCRM Lifecycle Utility: Traceback analysis starting at receipt informs the acquirer's 'Employ' decision, providing a living timeline for ongoing sustainment and eventual disposal.

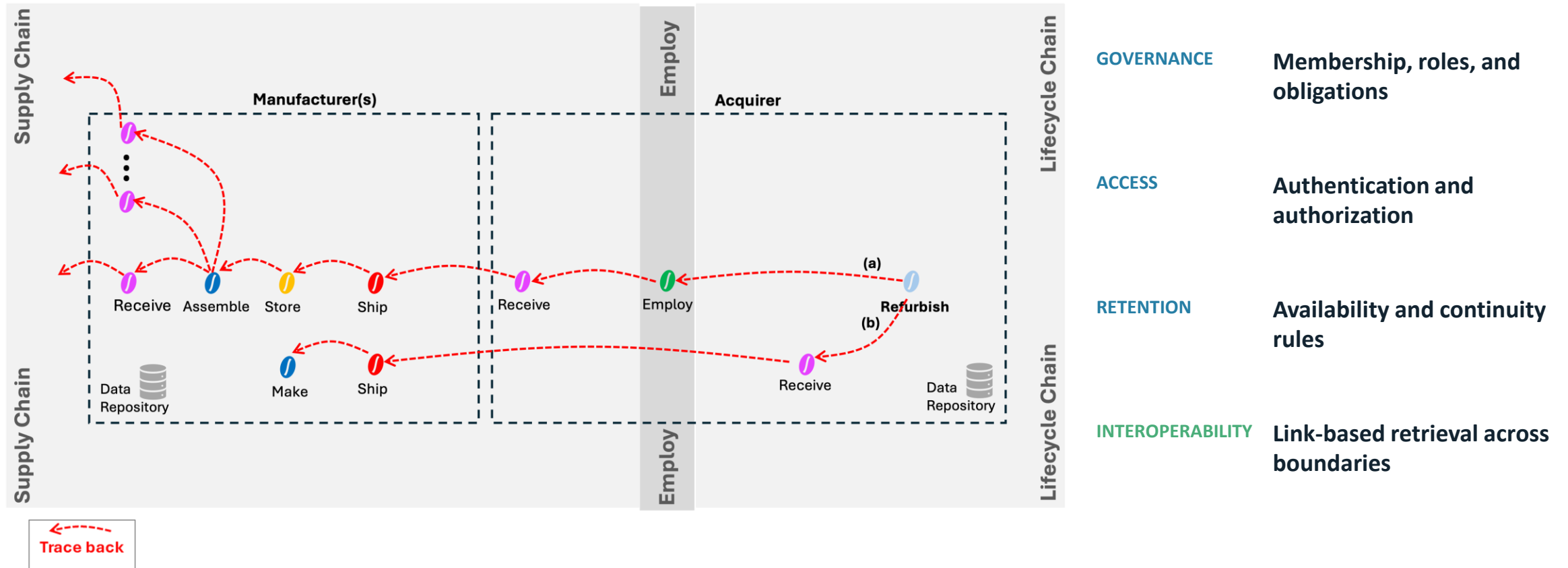
Selective Disclosure: Deep proprietary evidence (e.g., engineering models) remains protected in gated systems as 'Supplemental Data References', accessed strictly on a need-to-know basis.



NIST IR 8536 Figure 8: Traceability Chain Spanning Multiple Supply Chain Ecosystems

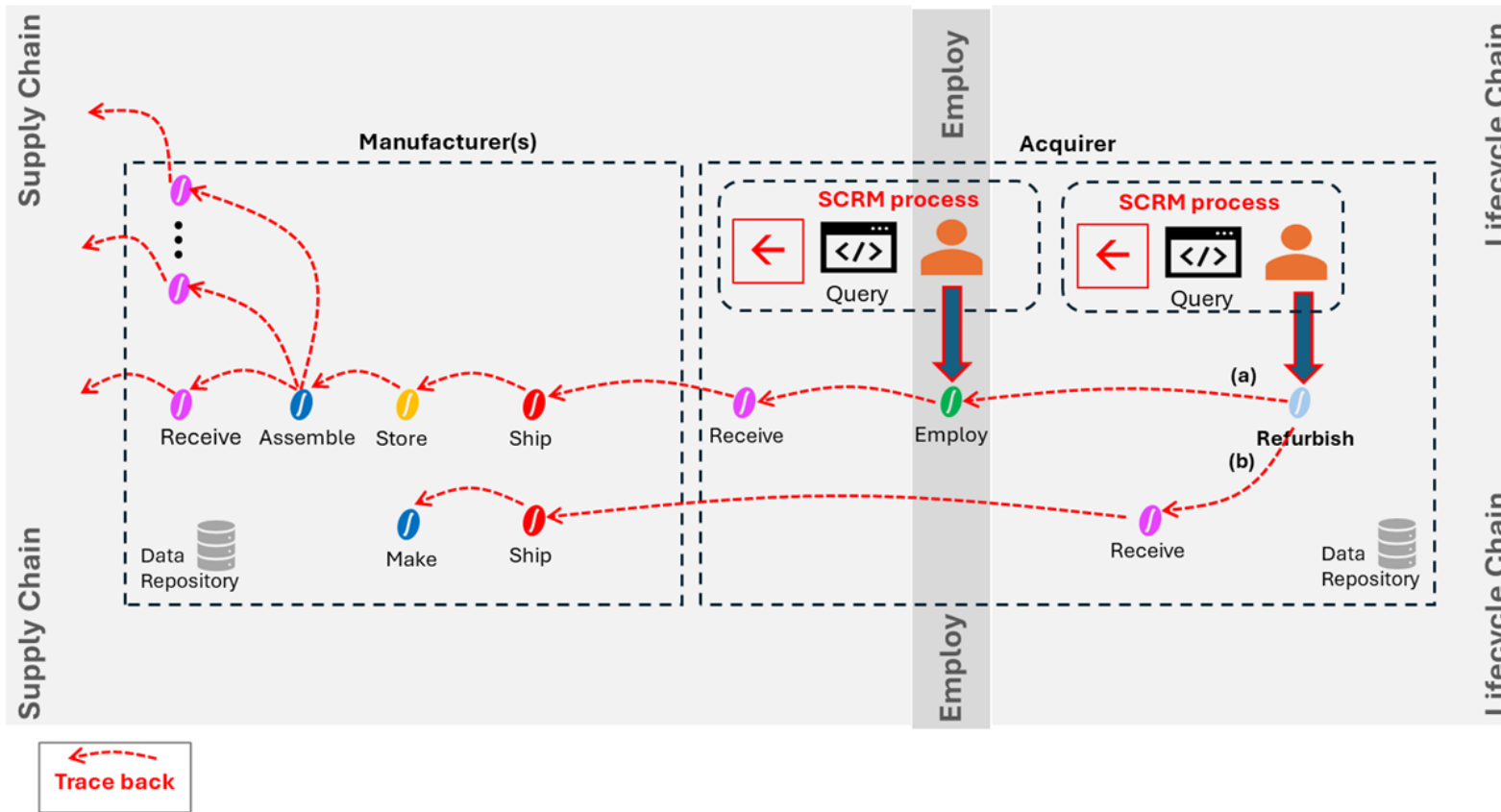
FEDERATED TRACEABILITY ECOSYSTEMS

Independent ecosystems can interoperate without surrendering local governance



FEDERATED TRACEABILITY ECOSYSTEMS

Independent ecosystems can interoperate without surrendering local governance



GOVERNANCE

Membership, roles, and obligations

ACCESS

Authentication and authorization

RETENTION

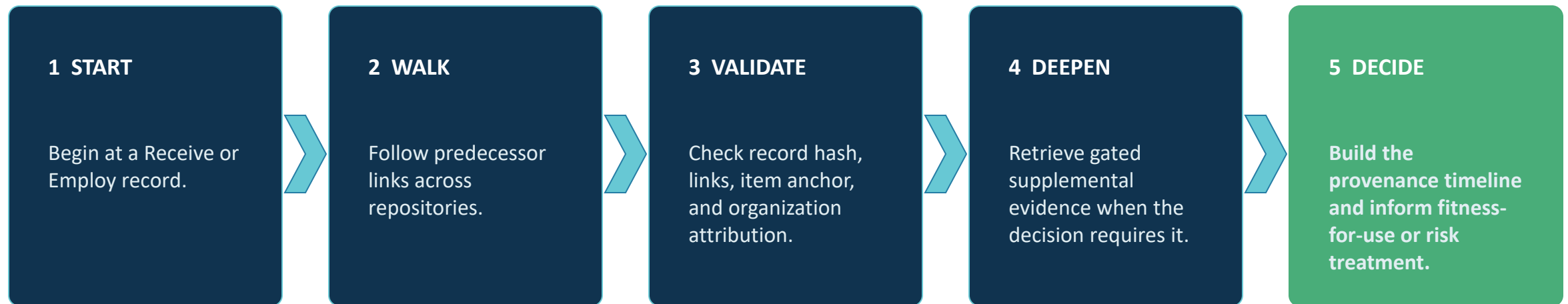
Availability and continuity rules

INTEROPERABILITY

Link-based retrieval across boundaries

OPERATIONAL EXECUTION

An acquirer walks the chain, validates evidence, and feeds the result into SCRM

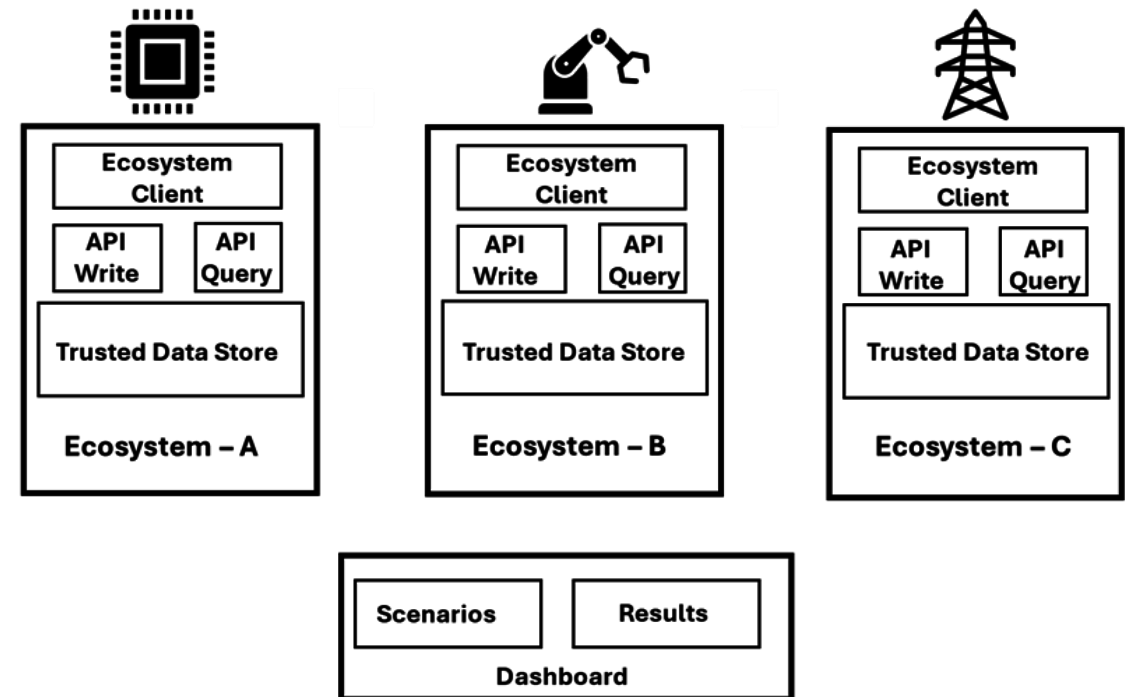


Use the same mechanism at any supply chain acquisition or manufacturing step where fitness for use must be evaluated.

REFERENCE IMPLEMENTATION

Status Update: An early-stage, Python-based Reference Implementation is currently undergoing final review and will be released as an open-source GitHub repository for community experimentation.

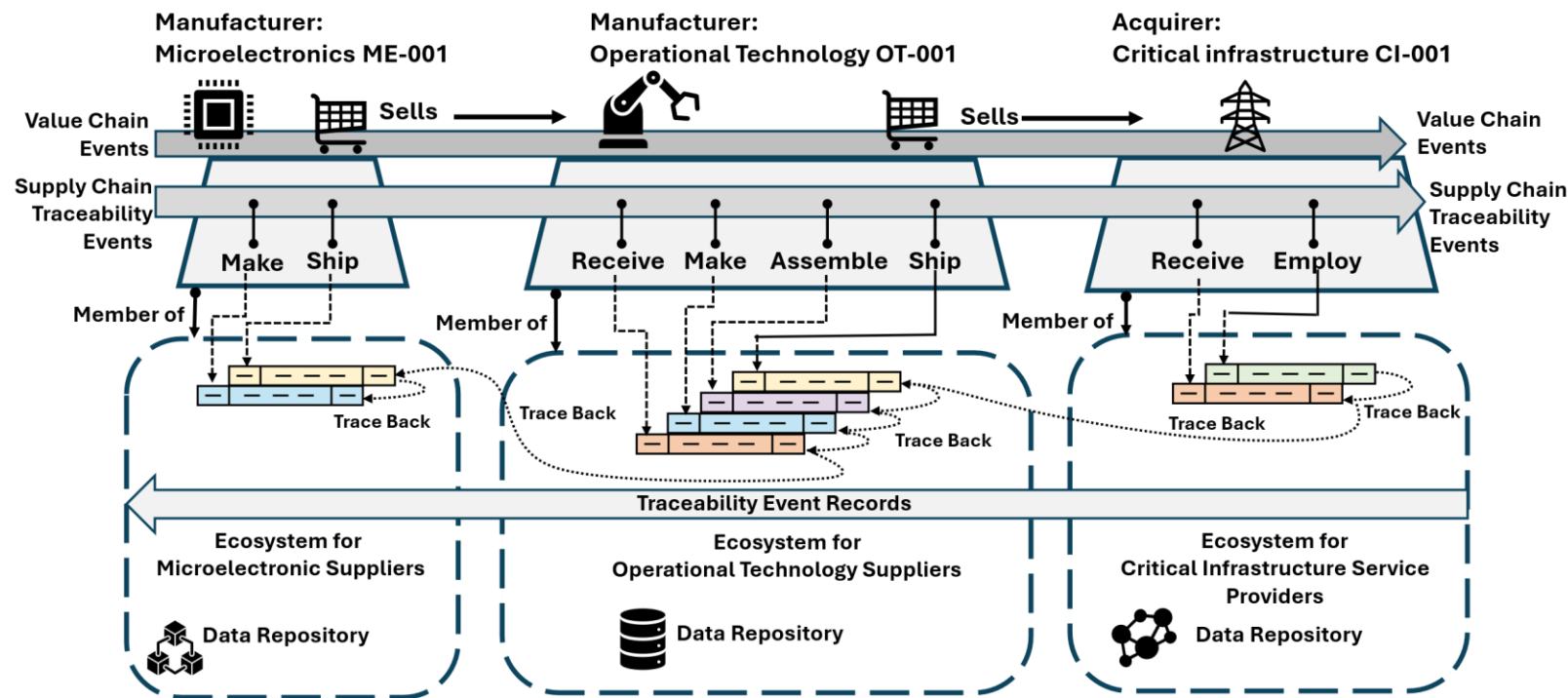
- **A Modular Lab Environment:** A controlled, virtual sandbox for deploying independent ecosystems with different technology stacks (e.g., blockchain, NoSQL, traditional databases).
- **Simulating Real-World C-SCRM:** Testing how transactions are captured across pseudo-processes (e.g., chip manufacturing to final software integration).
- **Informing the Future:** Evaluating traceability chains, refining governance issues, and testing how analysts query the data to validate pedigree and provenance.



Pending final approval for release

REFERENCE IMPLEMENTATION WALKTHROUGH

The MVP models a simplified supply chain across three example ecosystems



MICROELECTRONICS

Make · Ship

OT INTEGRATOR

Receive · Assemble · Ship

CI ACQUIRER

Receive · Employ

HOW TO APPLY NIST IR 8536

Use the work to start a structured traceability conversation

1

Choose a priority SCRM decision and define the evidence it needs.

2

Map product handoffs to the initial event categories.

3

Tailor record payloads to existing sector standards and terminology.

4

Define ecosystem governance, access, and retention expectations.

5

Prototype link creation, traceback, and validation using the reference implementation.

6

Feed implementation lessons back into standards, consortia, and future research.

FUTURE DIRECTIONS

The publication is a starting point and identifies where more work is needed

POST-EMPLOY LIFECYCLE

Return, Recall, Refurbish, Transfer, and Dispose events.

ADDITIONAL MANUFACTURING EVENTS

Precursor, Process/Convert, Split, Modify, and Transport.

SECURITY & PRIVACY

Identity, authorization, purpose limitation, threat modeling, and resilience.

ECOSYSTEM EXPERIENCE

Governance, incentives, semantic interoperability, and long-term record availability.

Do you believe the framework presented today will help your organization successfully meet future regulatory mandates?

Slido.com
#NIST_SupplyChain





NCCoE “Supply Chain Traceability Principles: A Manufacturing Meta-Framework”

<https://www.nccoe.nist.gov/projects/supply-chain-traceability-principles-manufacturing-meta-framework>

meta-framework_nccoe@nist.gov



[nccoe.nist.gov](https://www.nccoe.nist.gov)



[@NISTcyber](https://twitter.com/NISTcyber)

