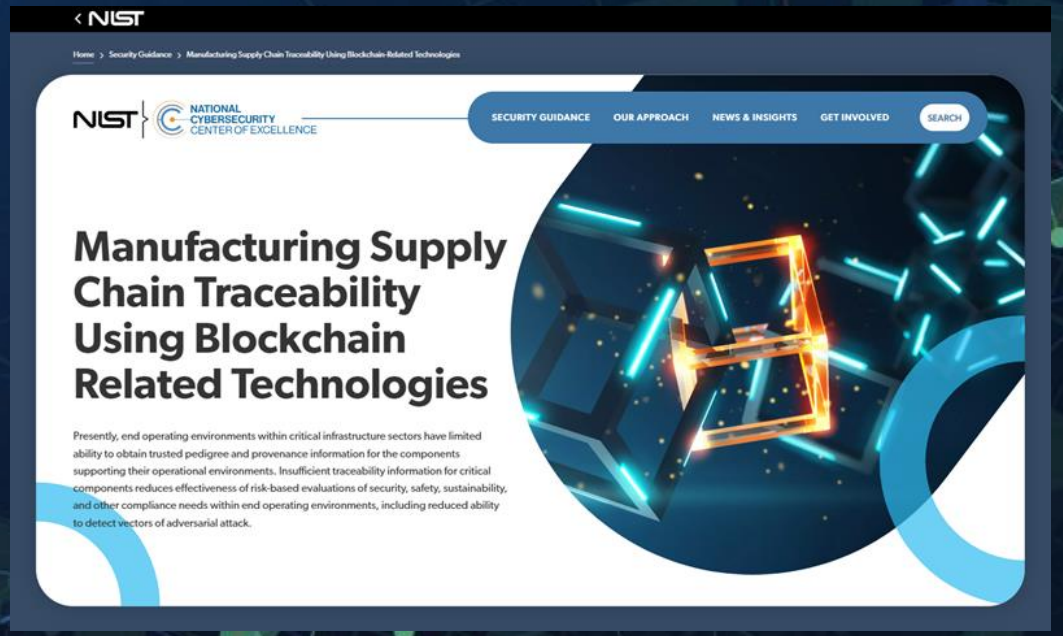
Manufacturing Supply Chain Traceability Chain Research and Reference Implementation

Manufacturing Meta-Framework

National Cybersecurity Center of Excellence

Monday, October 28, 2024



NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMERS

- **Presentation:**
  - Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Please Note:

This webinar will not be recorded, but we will capture unattributed comments and Q&A to include in the IPD Adjudication Process.

WHO WE ARE

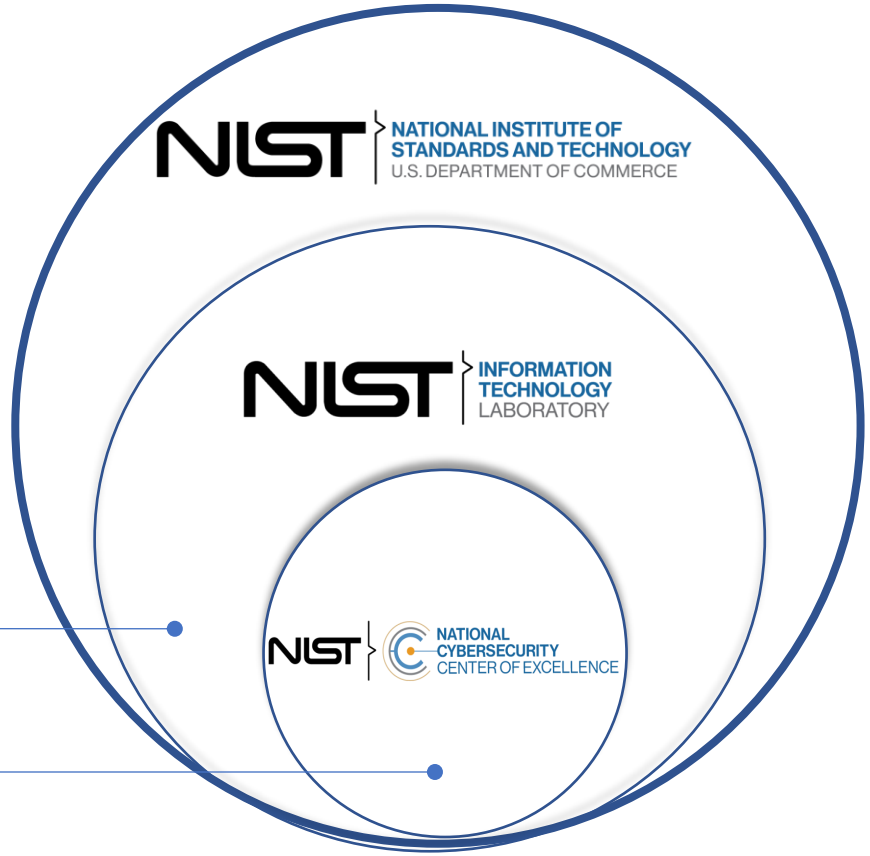
A **solution-driven**, **collaborative** hub addressing complex cybersecurity problems

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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**.



NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

AGENDA

Author Presentations and Overview of NIST IR 8536

- Introductions and Overview
- Industry Sectors / Ecosystems
- Data Structures / Traceability Links
- Use Cases

10-minute Break

Panel Session/Discussions

Closing Remarks

PROJECT TEAM

Michael Pease
(NIST)

Evan Wallace
(NIST)

Harvey Reed
(MITRE)

Dr. Vivian Martin
(MITRE)

Steve Granata
(MITRE)

TRACEABILITY SHIFT IN PERSPECTIVE

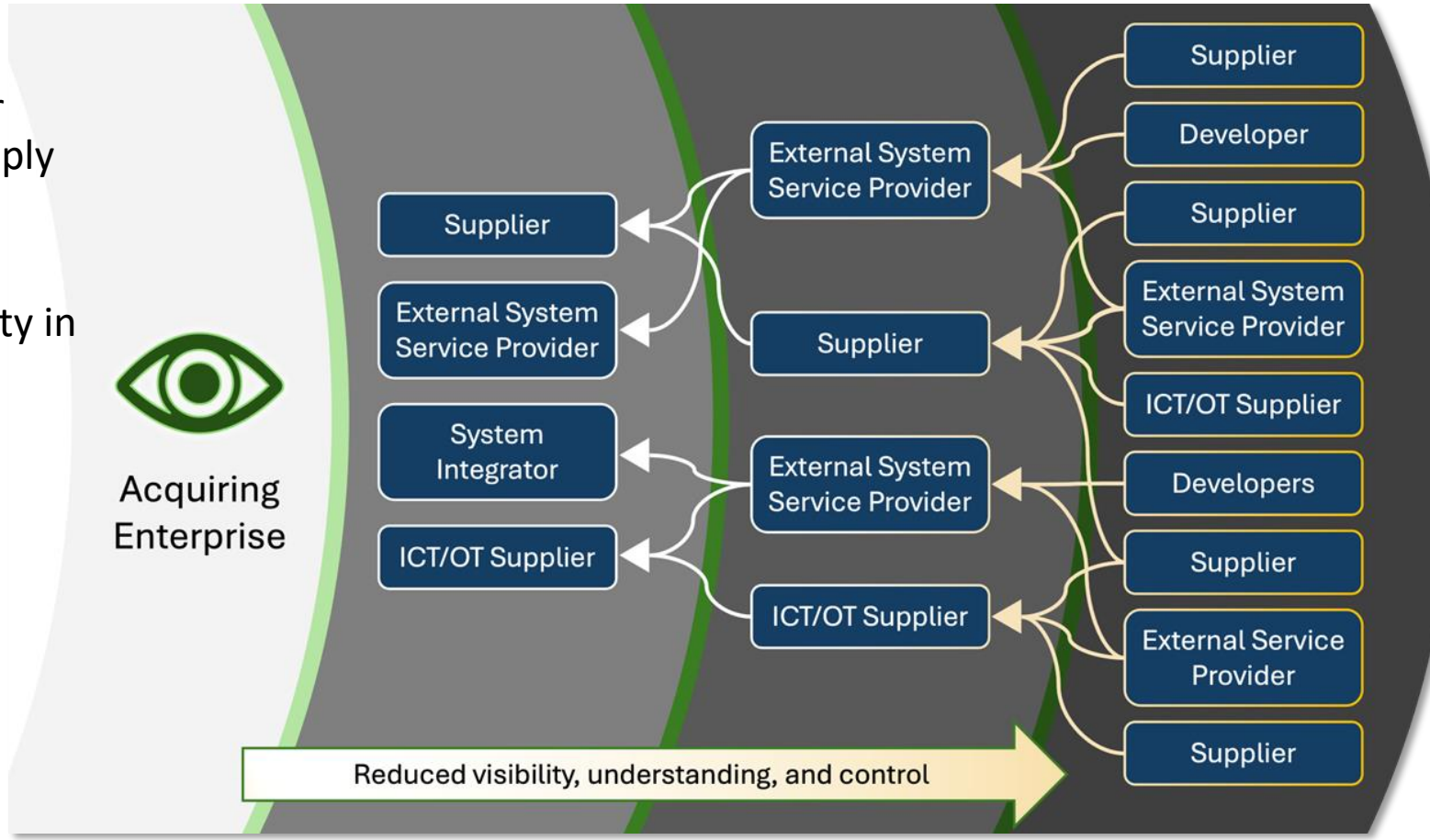
Traceability Fundamentally Enables End-to-End SCRM Capabilities

What we need/want:

- ***Traceability records*** illuminate the physical or digital flow of materials and products in a supply chain, informing product ***provenance.***
- ***Pedigree*** supports information captured in traceability records and reflects product quality in terms of:
  - Original producer authenticity
  - Adherence to specifications and standards

Primary Challenge:

- Difficulty obtaining trustworthy information



NIST SP 800-161r1

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

MANUFACTURING META-FRAMEWORK

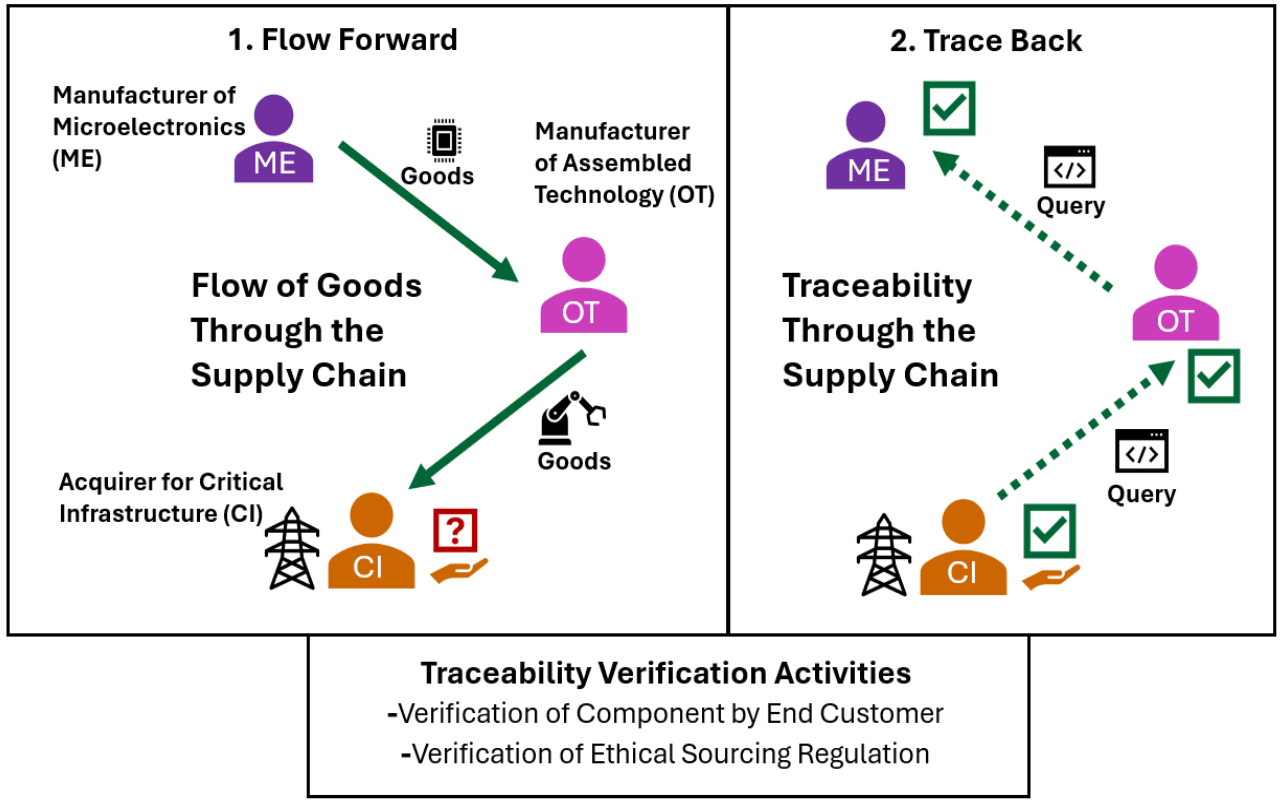
Goal: Provide a framework for capturing and linking records during the product production process (flow forward) to allow tracing backwards to collect pedigree and provenance information to support supply chain risk management.

Meta-Framework Includes Support for:

- Industry-specific/Regulatory Data Models and Ontologies
- Capturing Traceability Records for Manufacturing Events
- Linking Traceability Records both within and across data repositories
- Establishing Trusted Data Repositories or Ecosystems
- Allowing the secure reference to bulk or sensitive information to support pedigree and provenance.

Meta-Framework was targeted to address multiple supply chain and stakeholder challenges including:

- Storage of information in disjointed and isolated repositories.
- Inconsistent semantic and data definitions
- Ability to collect and validate pedigree and provenance information.

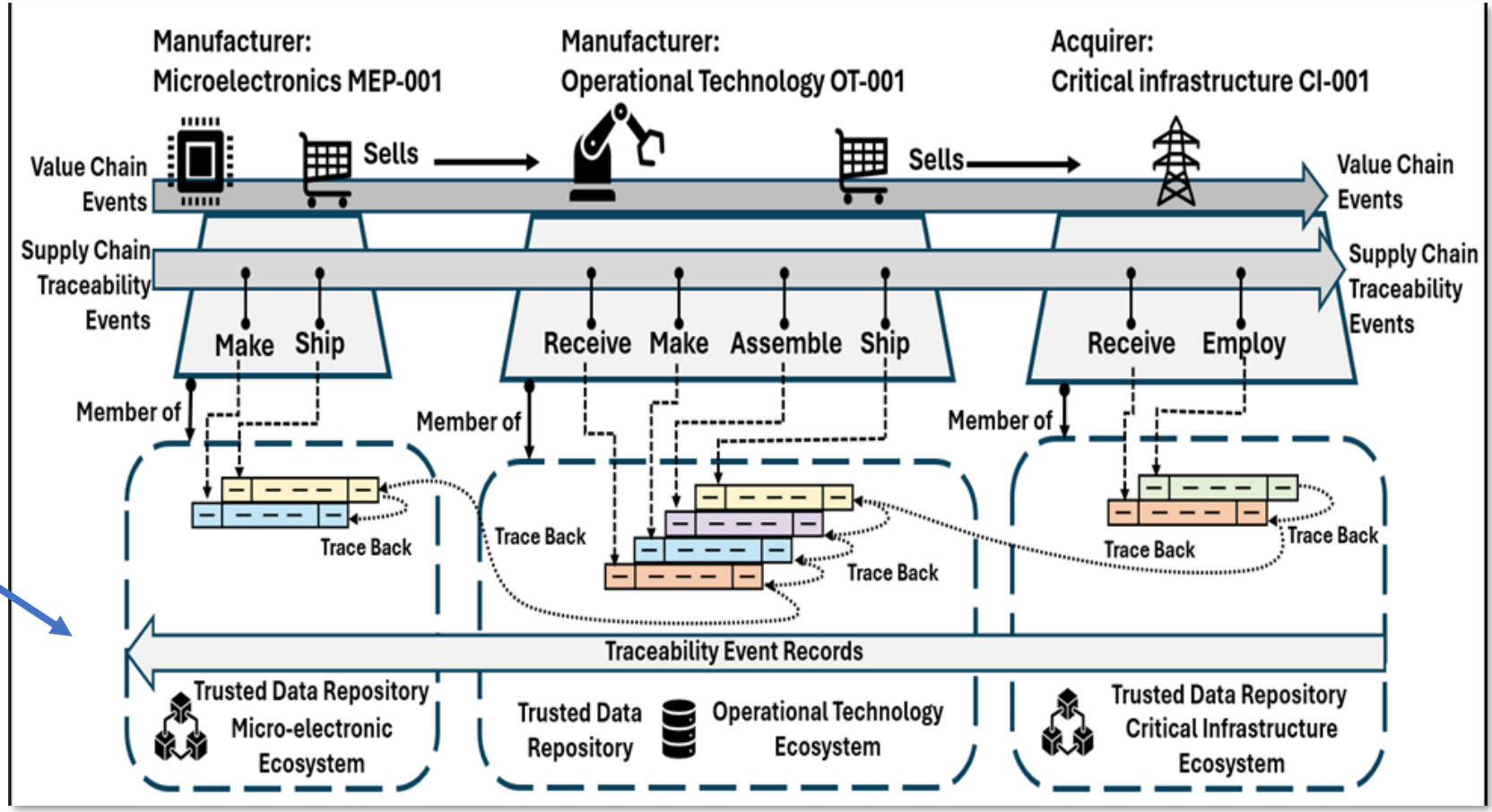


NIST IR 8536 IPD Figure 1 - Challenges to Component or Assembly Verification Across Stakeholder Tiers

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

PRINCIPAL TRACEABILITY WORKFLOW

- Workflow 1
  - Manufacturers write traceability records, incrementally creating a traceability chain
- Workflow 2
  - End customer reads the traceability chain to inform risk analysis and decide whether to employ

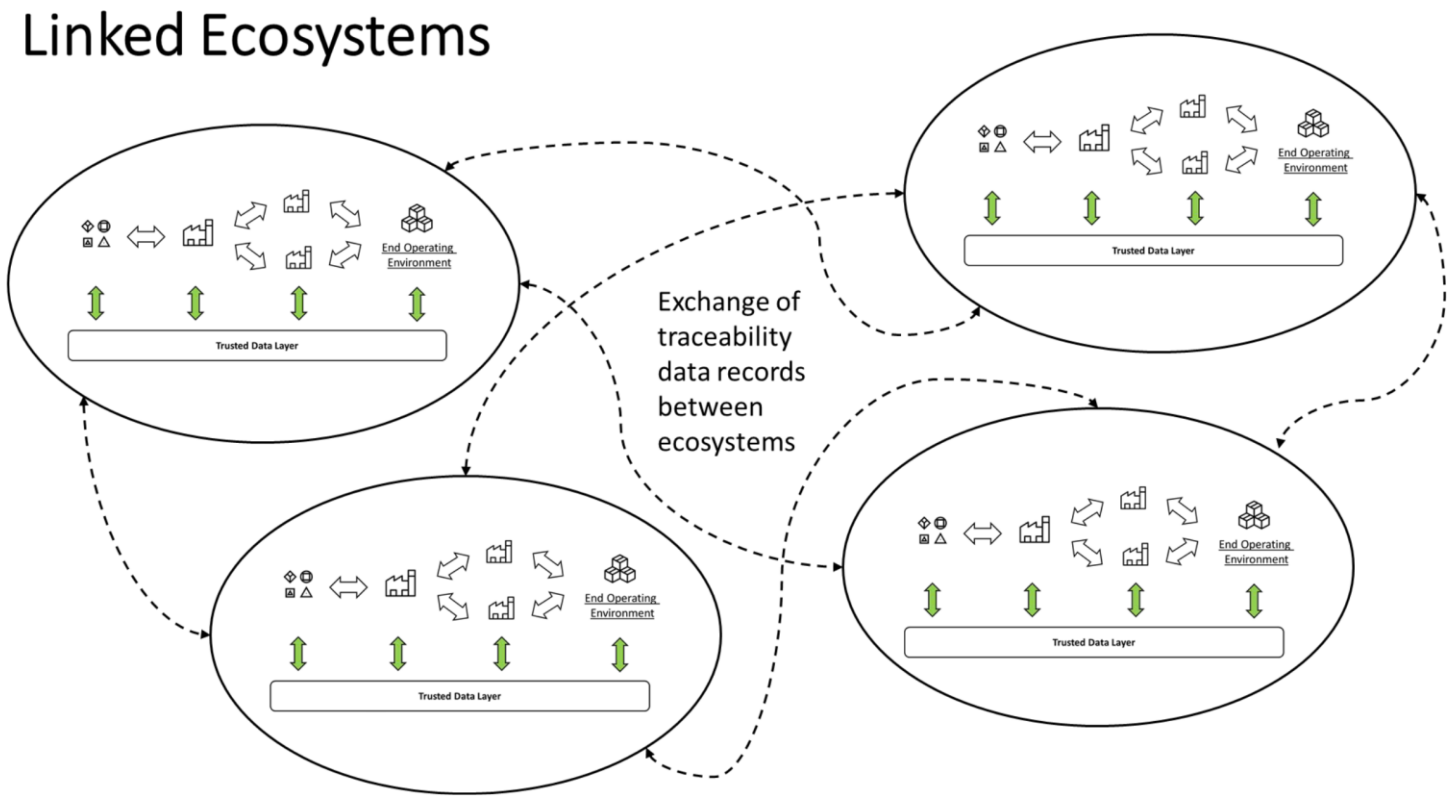


NIST IR 8536 IPD Figure 4 - Value and Supply Chain Traceability Events Across Ecosystems

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ECOSYSTEM PERSPECTIVE

- NIST IR 8419 established the supply chain ecosystem perspective
  - Holistic supply chain traceability overlaid on the NIST SP 800-53/161 “per acquirer” perspective
  - Ecosystem members trace and share product provenance and pedigree information available in a **“push” to** acquirers **vs. “pull” from** acquirers
  - Implementation is unique to each ecosystem
- Ecosystems:
  - Occur in specific markets, market sectors, economic sectors, or sub-sectors
  - Are self-governed entities
  - Scalable and ultimately interoperable among each other
- NIST IR 8536 delineates the Meta-Framework concept in supply chain traceability



NIST IR 8419 Figure 10 - Network of Traceability Ecosystems

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ECOSYSTEM CHARACTERISTICS

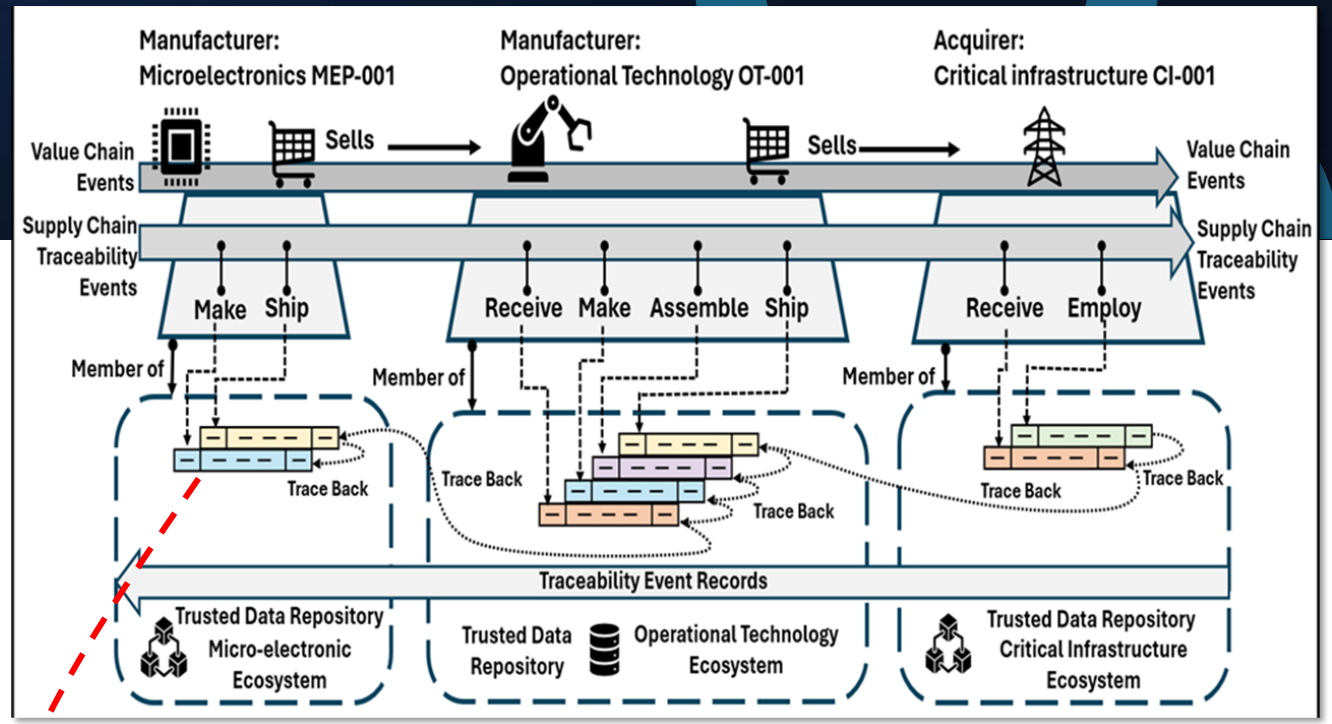
- An Ecosystem is a group of **affiliated**, **self-governing** supply chain actors with a **mutual interest or need** to share product provenance and pedigree information among each other
- Ecosystem members at all tiers of a given supply chain:
  - Agree upon data elements, conventions, and standards, and data interchange features common to their ecosystem
  - Ultimately furnish information to acquiring enterprises, as necessary to meet acquirer needs for product provenance and pedigree information
- Ecosystems improve the current state of practice by:
  - Enhancing the accessibility and visibility of supply chain information
  - Establishing a data model that supports industry and regulatory efforts to develop and establish supply chain ontologies
  - Improving data integrity with mechanisms for stakeholders to validate supply chain data from multiple sources

COMMON ELEMENTS OF AN ECOSYSTEM

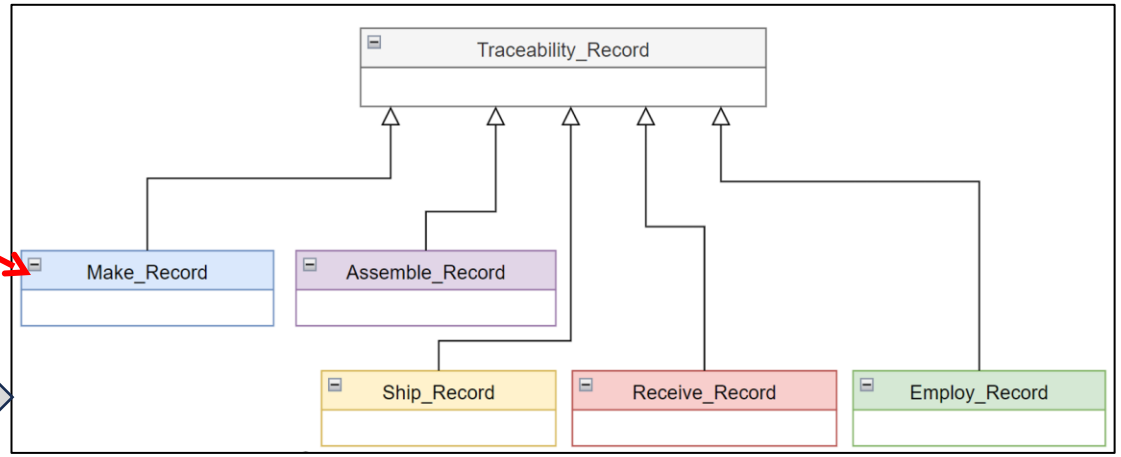
- Data Conventions & Data Standards
  - Fundamental Enabler: A common, ecosystem-wide, high-level, product provenance and pedigree **data ontology**
  - Governed ecosystem-wide set of provenance and pedigree **data references**, aligned with the ontology, that fulfill desired information sharing across the ecosystem
- Trusted Data Store
  - Shared and acknowledged by vetted ecosystem members
  - Implemented and governed per-ecosystem
  - Includes ecosystem-defined and governed cybersecurity controls on data at-rest
- Secure, Executable Data Interchange
  - Features system interfaces within and among the ecosystem members
  - Includes ecosystem-defined and governed cybersecurity controls on data in-motion

TRACEABILITY RECORDS

- Traceability Record Subclasses:
  - Subclasses represents supply chain events
  - Traceability Records capture key traceability information for each type of supply chain event, in time order
- Traceability Chain:
  - The set of linked Traceability Records form a Traceability Chain (graph)
- The Meta Framework specifies:
  - Interoperable Traceability Links used across and within ecosystems
- The Meta Framework requires:
  - Industry and regulators to define traceability data contained by Traceability Record subclasses, accessed via ecosystem interfaces



Extensible



NIST IR 8536 IPD Figure 6 - Overview Class Diagram for Traceability Record

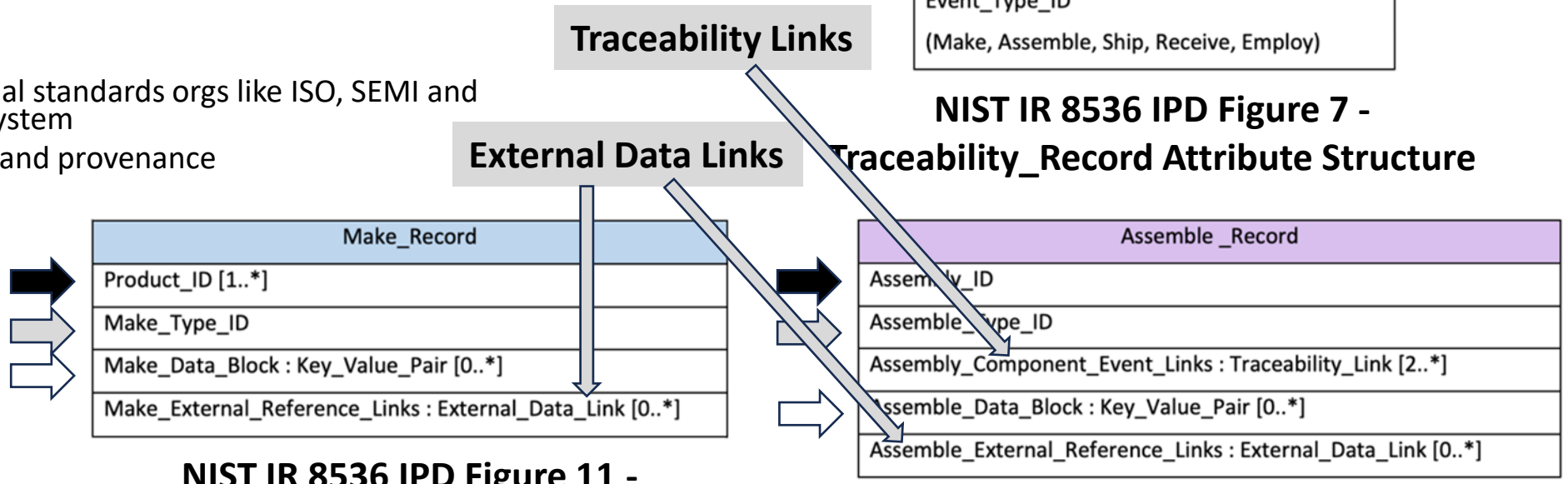
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

TRACEABILITY DATA

- Product_ID for Make and Assembly_ID for Assembly
  - Cyber-physical ID
- Make_Type_ID for Make and Assemble_Type_ID for Assembly
  - The type designator indicates the minimum content in the corresponding data block
- Make_Data_Block for Make and Assemble_Data_Block for Assemble
  - Block of Key-Value pairs
  - Data specified by external standards orgs like ISO, SEMI and is governed by the ecosystem
  - Data supports pedigree and provenance

Traceability_Record
Record_ID
Event_Occurrence_Timestamp
Event_Recorded_Timestamp
Organization_ID
Organization_Unit_ID
Event_Type_ID (Make, Assemble, Ship, Receive, Employ)

NIST IR 8536 IPD Figure 7 - Traceability_Record Attribute Structure



NIST IR 8536 IPD Figure 11 - Make_Record Attribute Structure

NIST IR 8536 IPD Figure 12 - Assemble_Record Attribute Structure

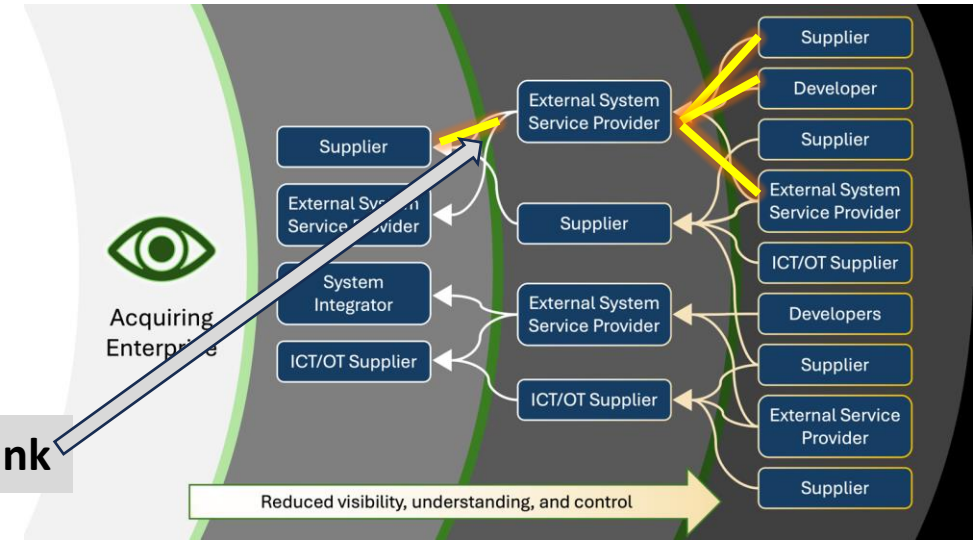
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

TRACEABILITY LINKS

- Resource_Link (IRI)
  - Resource identifier for Ecosystem interface which contains the target Traceability Record
- Parameter_Block
  - Key / Value pairs of data for query/access parameters
- Resource_Hash
  - Hash of target traceability record for subsequent data integrity validation
- Notes
  - Traceability Links form a Traceability Chain (graph) with Traceability Records (Make, Assemble, etc.) as the nodes, and Traceability Links as the arcs. E.g.:
    - Make←Assembly
    - Ship←Receive
    - Receive←Employ

Traceability_Link
Resource_Link : Internationalized_Resource_Identifier
Parameter_Block : Key_Value_Pair [0..*]
Resource_Hash

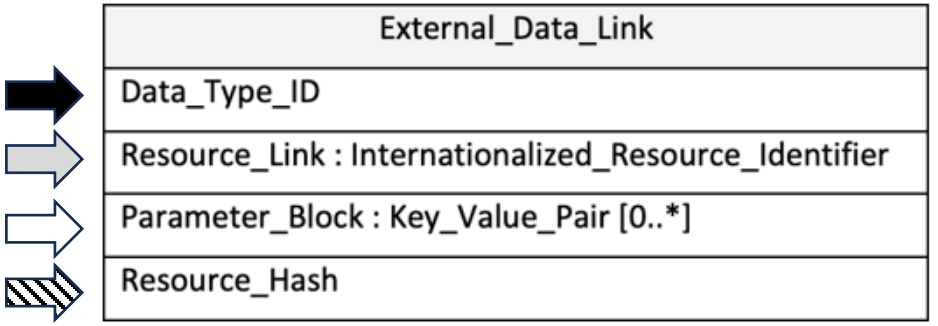
NIST IR 8536 IPD Figure 10 - Traceability_Link Attribute Structure



NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

EXTERNAL DATA LINKS

- Data_Type_ID
  - Industry defined, ecosystem governed description of target data
- Resource_Link (IRI)
  - Resource identifier for the interface which contains the target data
- Parameter_Block
  - Key / Value pairs of data for query/access parameters
- Resource_Hash
  - Hash of target data for subsequent data integrity validation
- Notes
  - External Data Link can be an attestation reference, a test reference, or similar, e.g., IETF SCITT 3rd party notary
  - Data may not be accessible by acquiring enterprise without additional steps
  - Supplemental information associated with the product or process



NIST IR 8536 IPD Figure 10 - External_Data_Link Attribute Structure

META FRAMEWORK CAPTURES USE CASES

- Perspectives of Use Cases – Enterprises that supply and acquire
  - Recording Supply Chain Event Data
  - Tracing and Retrieving Traceability Records
- Five high-level, example Sequence Diagrams provide context
  - Record Events
    - Manufacturer of Microelectronics Make Traceability Event (NIST IR 8536 IPD Figure 17)
    - Operational Technology with Receive, Make, Assemble, and Ship Events (Figure 18)
    - Critical Infrastructure Acquirer with Receive and Employ Events (Figure 19)
  - Trace and Retrieve
    - Operational Technology with Trace Back to Manufacturer of Microelectronics (Figure 20)
    - Critical Infrastructure Acquirer with Traceback to Manufacturer and Operational Technology (Figure 21)

META FRAMEWORK CONTEXT IN THUMBNAIL

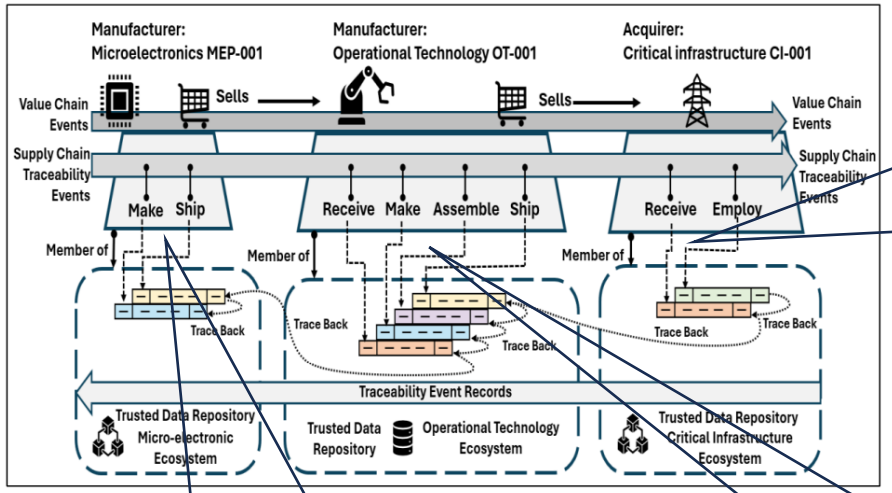
Legend for Actors and Diagrams—

Diagram A--- A
:ME-001 (Manufacturer: Microelectronics)
:ME-E IF (Micro-electronics Ecosystem Interface)

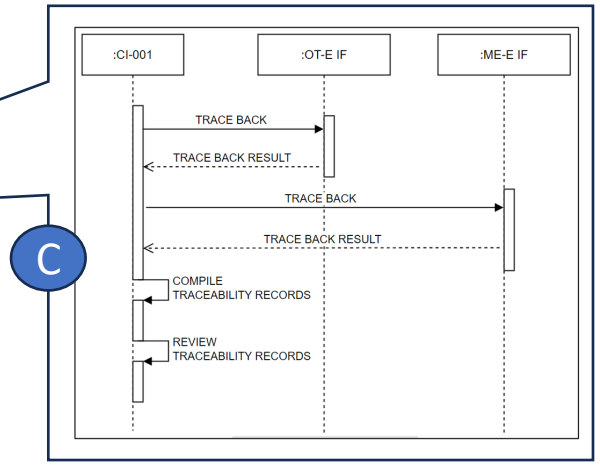
Diagram B--- B
:OT-001 (Manufacturer: Operational Technology)
:OT-E IF (Operational Technology Ecosystem Interface)

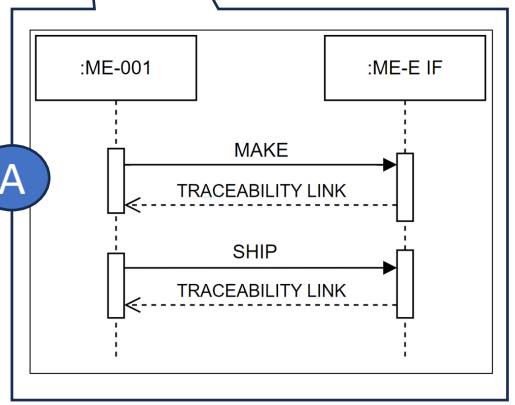
Diagram C--- C
:CI-001 (Acquirer: Critical Infrastructure)
:CI-E IF (Critical Infrastructure Ecosystem Interface

Thumbnail NIST IR 8536 IPD Figure 4

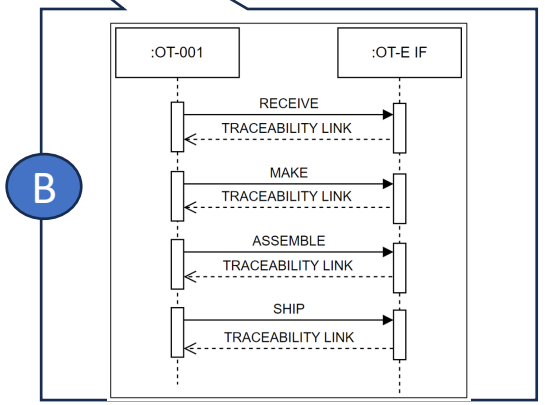


NIST IR 8536 IPD Figure 21 -Acquirer: Critical Infrastructure CI-001 Invokes Trace Back





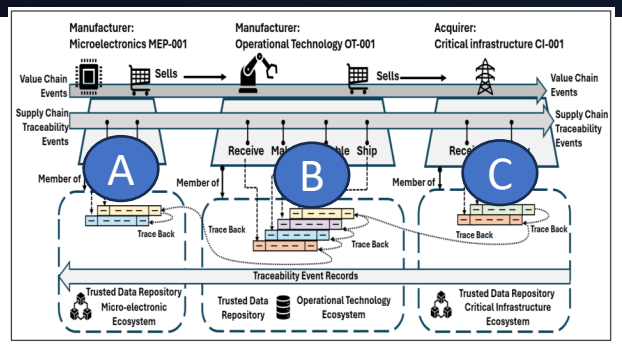
NIST IR 8536 IPD Figure 17 -Manufacturer: Microelectronics ME-001 Writes Make and Ship Event Records



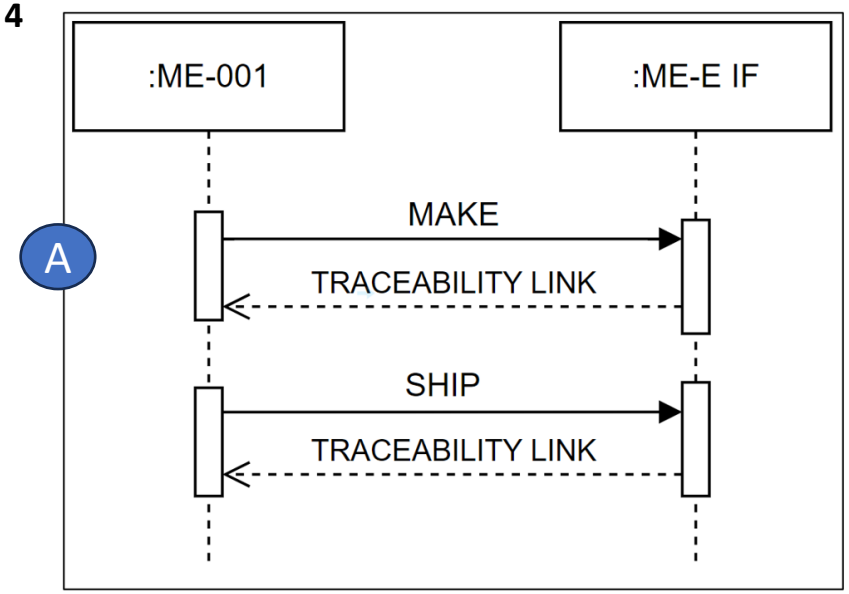
NIST IR 8536 IPD Figure 18 -Manufacturer: Operational Technology Writes Receive, Make, Assemble, and Ship Event Records

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

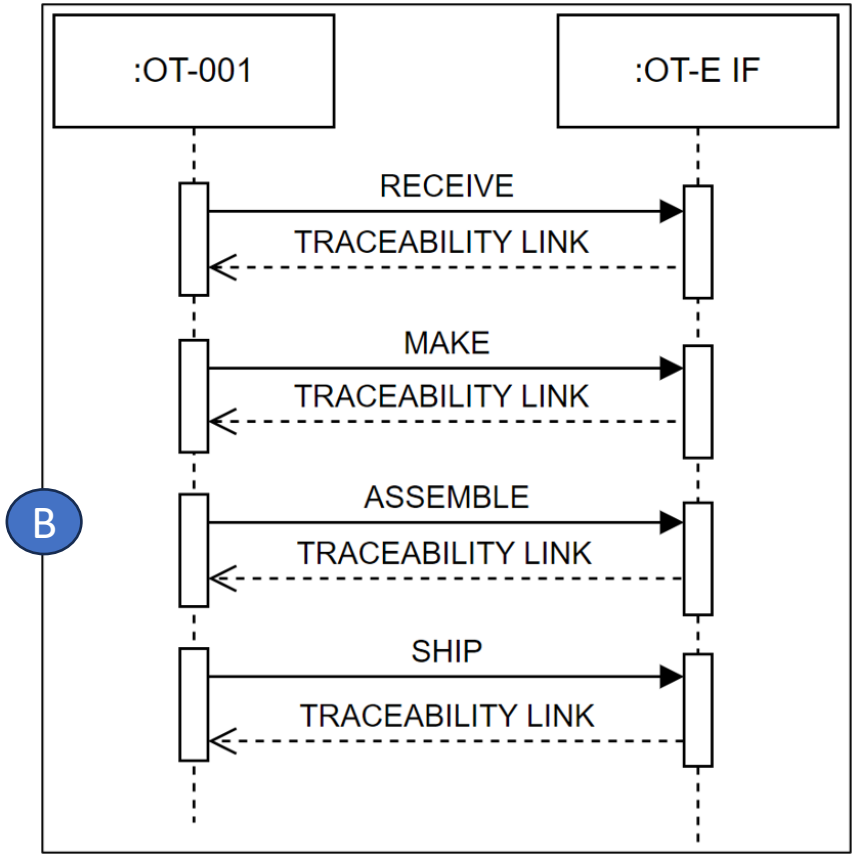
EXAMPLE RECORD TRACEABILITY USE CASES



NIST IR 8536 IPD Figure 4



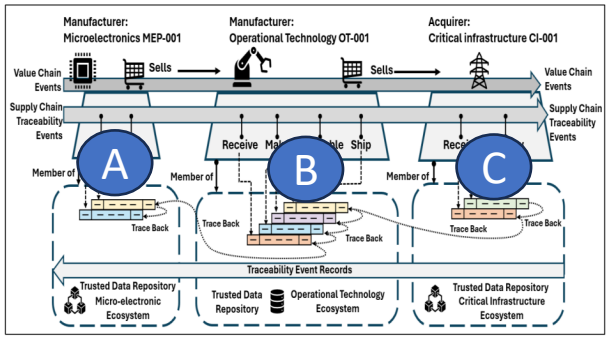
IPD NIST IR 8536 IPD Figure 17

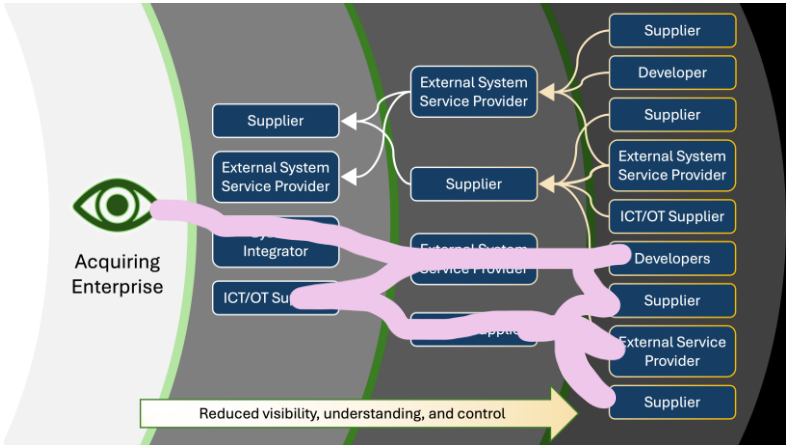


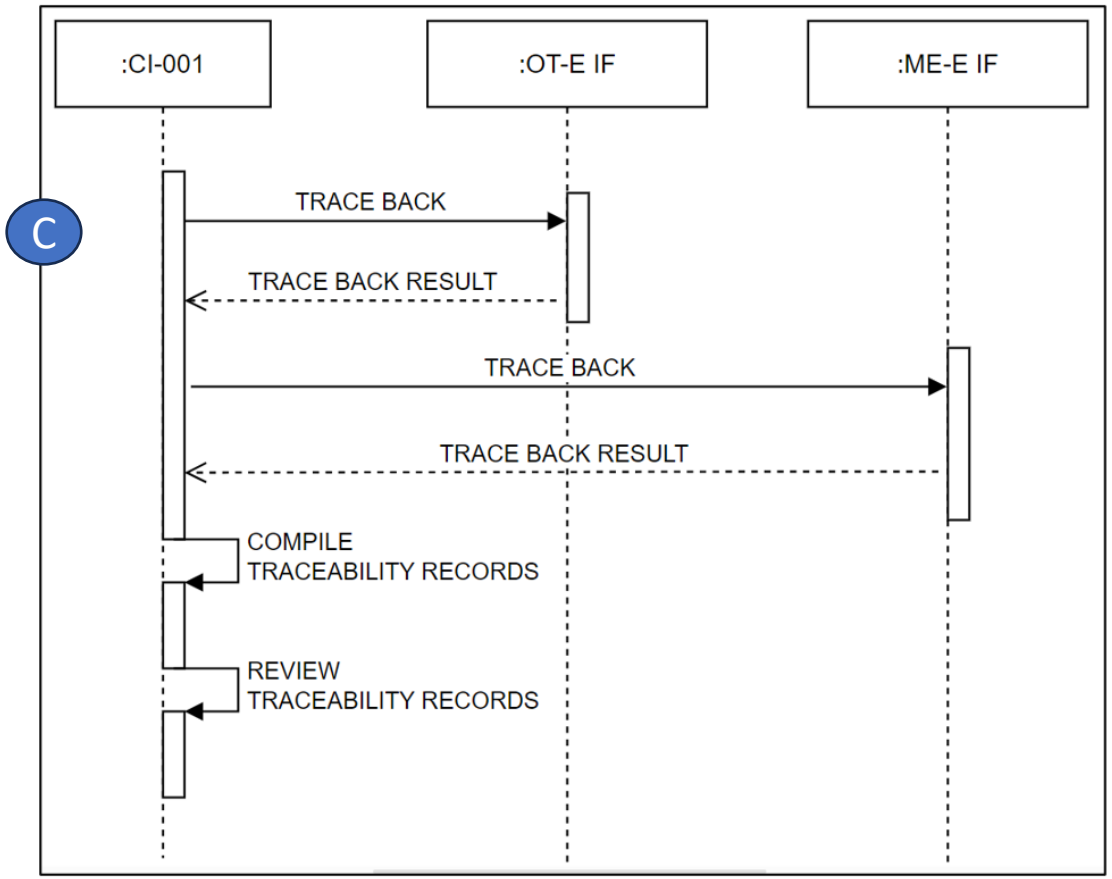
NIST IR 8536 IPD Figure 18

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

EXAMPLE RETRIEVE TRACEABILITY USE CASE







NIST IR 8536 IPD Figure 21 - Acquirer: Critical Infrastructure CI-001 Invokes Trace Back

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Panel Discussion

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

CLOSING REMARKS / NEXT STEPS

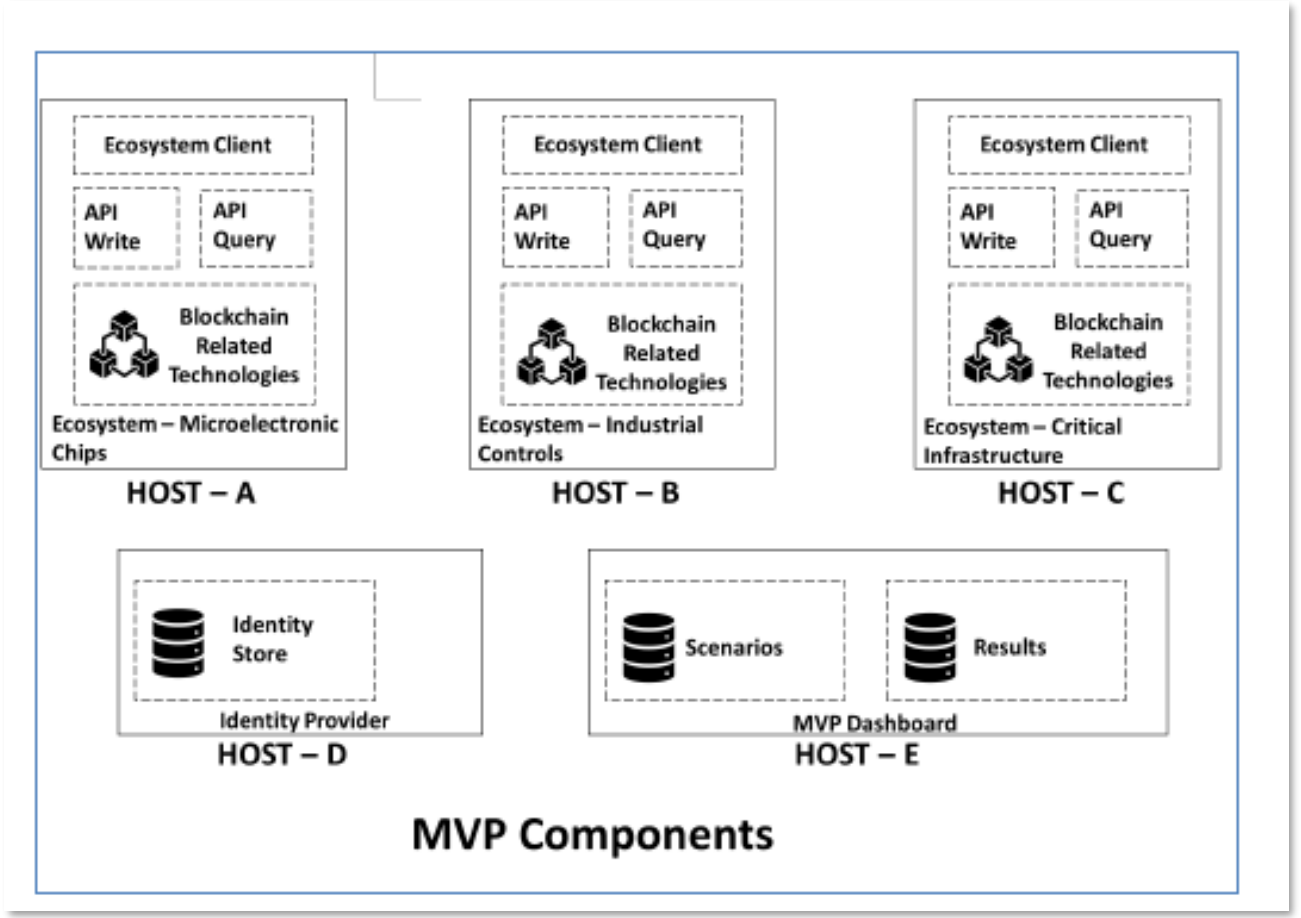
- Next Steps:
  - Adjudicate the comments and suggestions obtained for this webinar submitted through our project site.
  - **Publish NIST IR 8536**
  - Create a reference implementation (RI) / minimum viable product (MVP)
  - **Publish the RI/MVP**
  - Use the RI/MVP to support:
    - Continuing research into Supply Chain Traceability Governance, Cybersecurity, and Risk Management
    - Collaborate with industry partners and community of interest to investigate specific ecosystem and data structure implementations.

RI/MVP HIGH-LEVEL ARCHITECTURE

Goal: ***create a functional implementation that allows stakeholders to observe and test supply chain risk management practices in a controlled lab environment***.

Approach:

- **Establishing a module platform** for deploying one or more ecosystems that can support or implement different Identity Providers, APIs, and data repositories including Blockchains/Distributed Ledger Technologies, NoSQL, traditional SQL, or other data storage technologies.
- **Provide a Dashboard / Administrative Interface** to monitor/manage the ecosystems and collect KPI data.

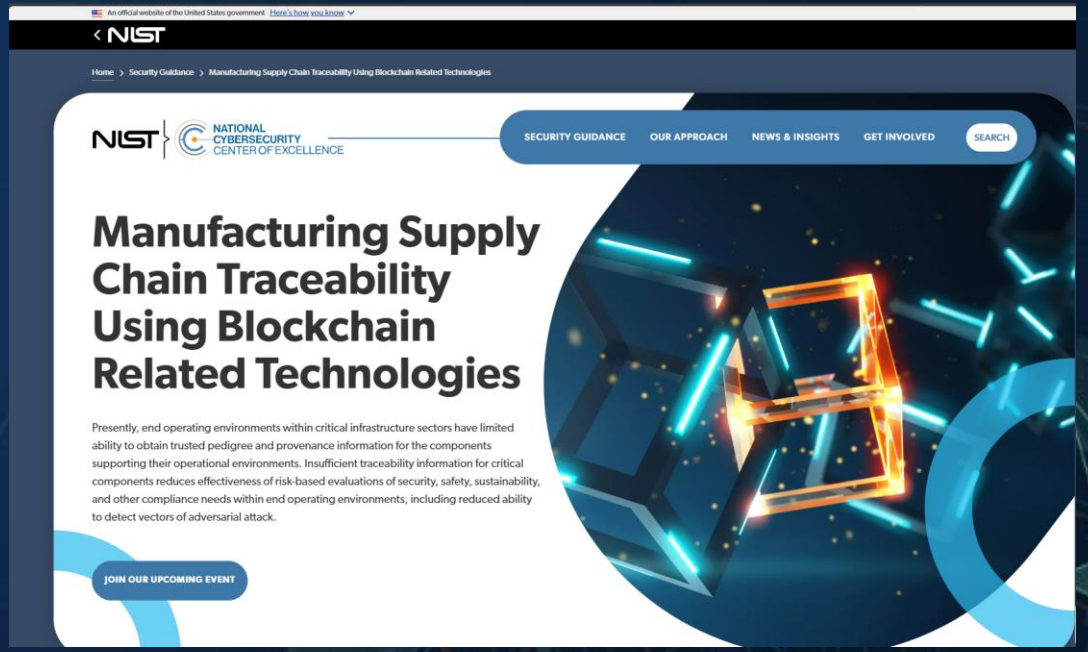


NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NCCoE "Manufacturing Supply Chain Traceability Using Blockchain Related Technologies"

https://nccoe.nist.gov/projects/manufacturing-supply-chain-traceability-using-blockchain-related-technologies

blockchain_nccoe@nist.gov



nccoe.nist.gov

@NISTcyber