Supply Chain Integrity, Transparency, and Trust (SCITT)

Non-WG Forming BoF

16 June 2022

SCITT: Non-WG Forming BoF

- Planned Outcomes
  - Explicit interest in solving the illustrated problem statements via standardization in the IETF
  - Kick-off discussions on what to standardize in the IETF (based on the primary software supply chain security use case)
  - Bonus: High-level charter building blocks identified
- Success Factors for this meeting
  - Bringing relevant stakeholders into the room
  - Establishing a shared understanding of the problem statement
  - Define a set of standards, enabling projects and products to innovate over a common interchange formats

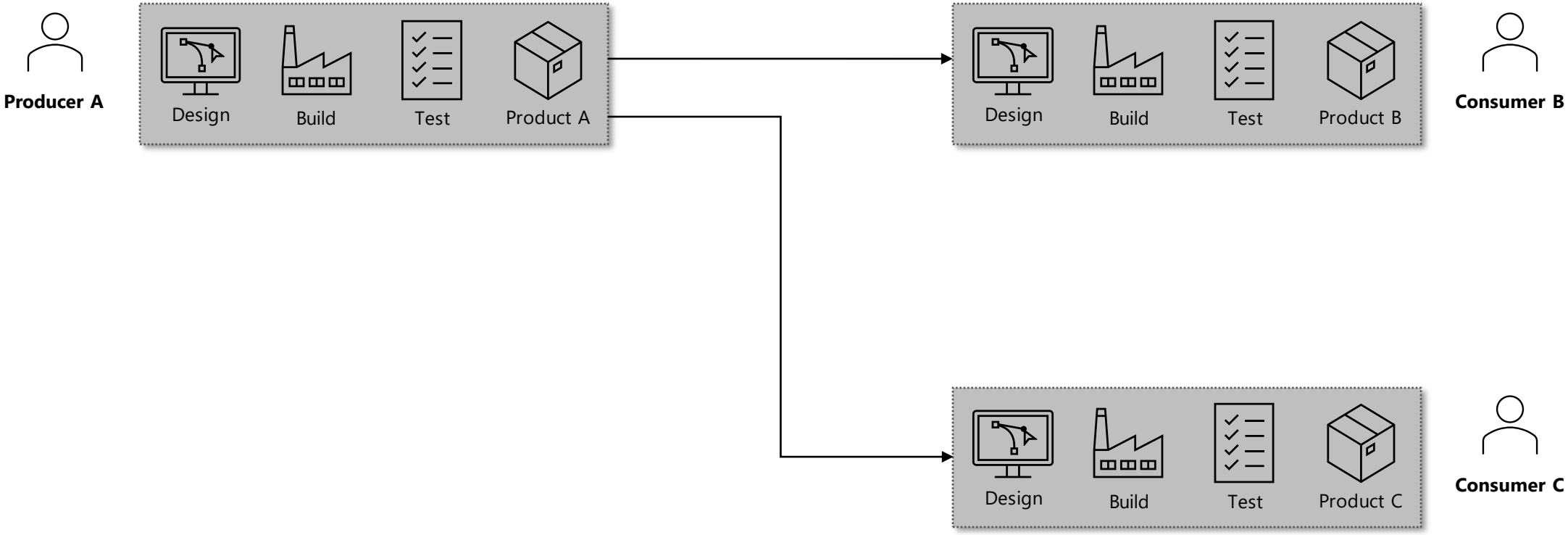
Agenda

- Problem Statement: 25 min
- Initial Use Case: 20 min
  - Software Supply Chain*
- Proposed Standardization Scope: 15 min
- Discussion: 60 min

*Bonus Goal: Selection of an additional use case in the discussion phase

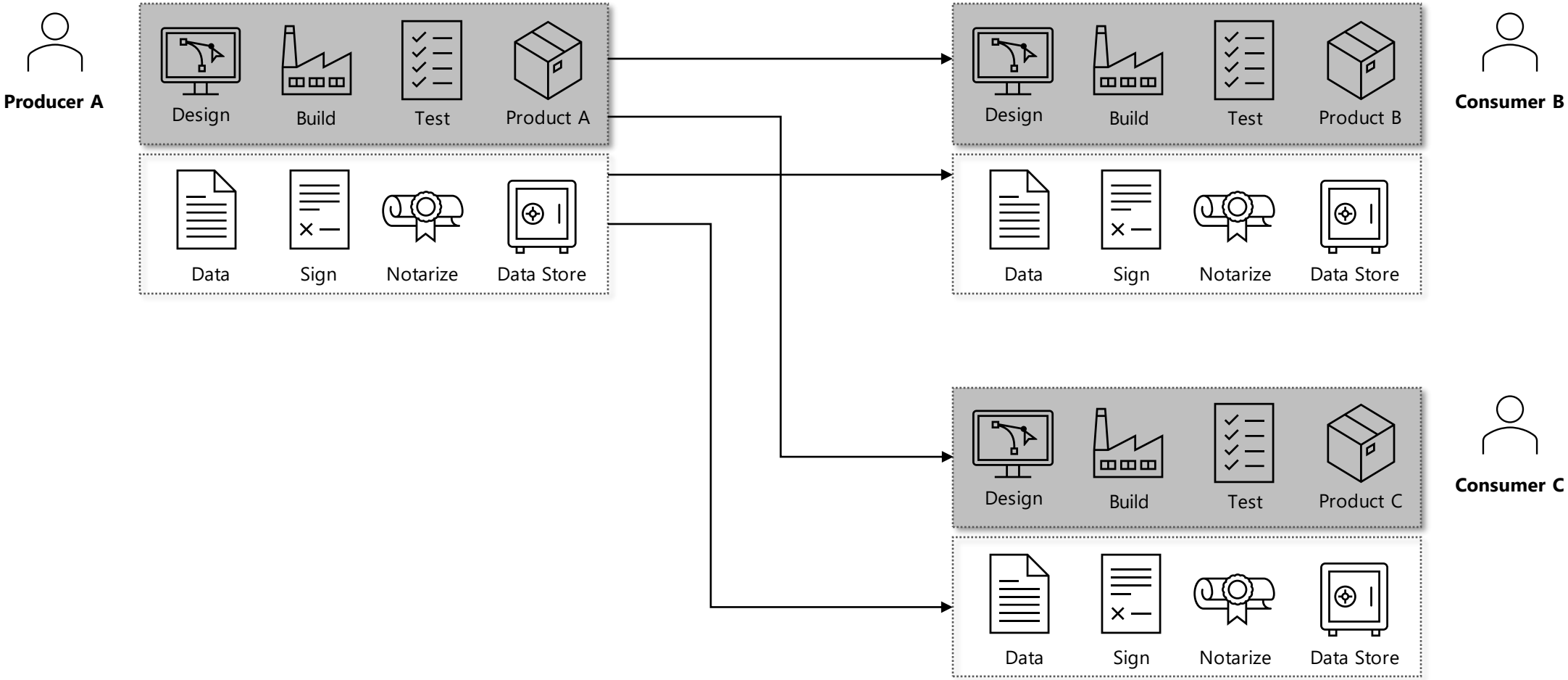
Problem Statement
(25 min)

Notional Supply Chain Workflow - Current



Current Supply Chain

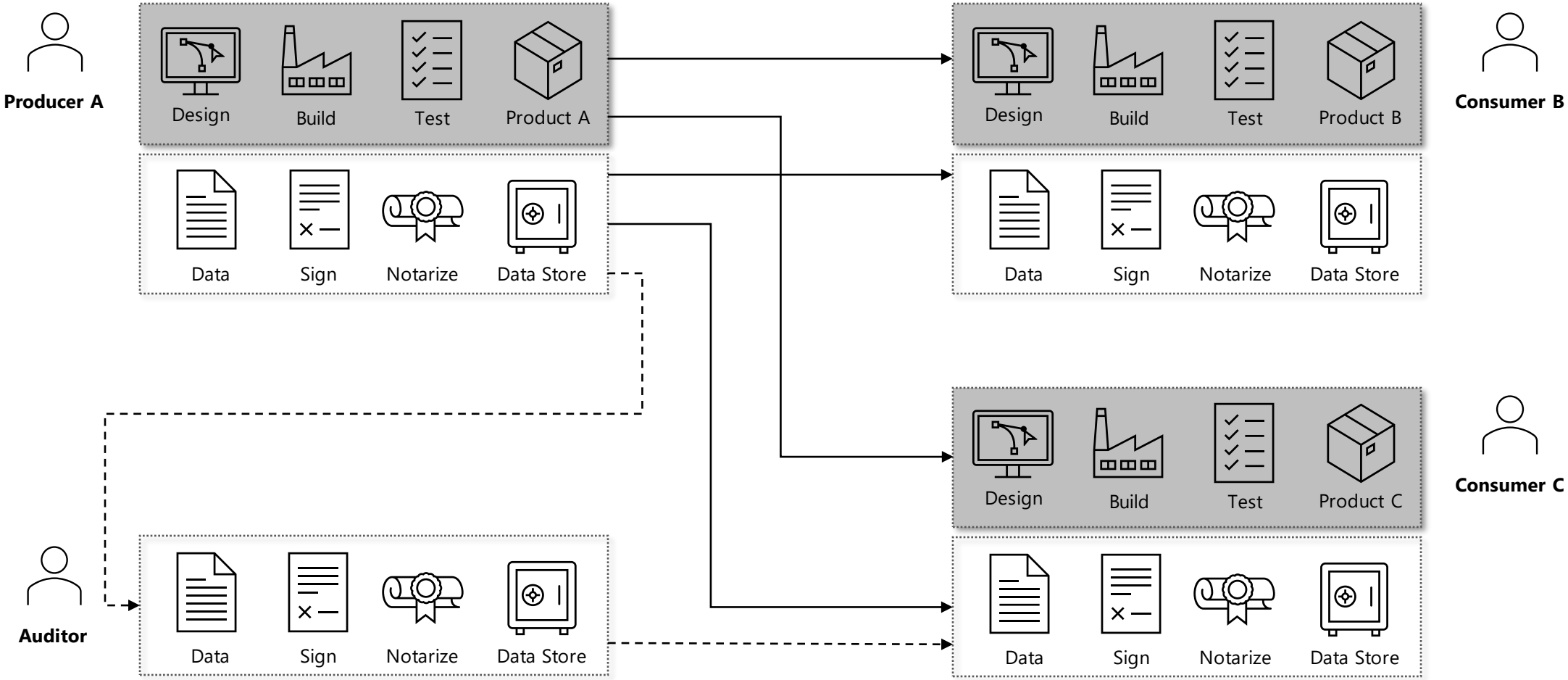
Notional Supply Chain Workflow – With SCITT



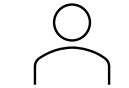
Current Supply Chain

SCITT Additions

Notional Supply Chain Workflow – With SCITT



Actor: Producer

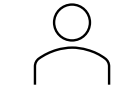


As a producer, I need to provide evidence that my products meet compliance against requirements

Problems Today

- Difficult to gather compliance evidence for what's consumed
- Difficult to share compliance evidence for what's produced
- Difficult to share claims of compliance, in a standard way across various clouds and on-prem

Actor: Consumer

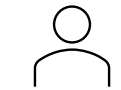


As a consumer, I need insight if my products meet compliance requirements for performance, security, quality, reliability, sustainability, safety, etc.

<u>Problems Today</u>

- There is no standard way to discover and query if a product meets “my” compliance standards
- …no standard way to promote to consumers environment
- …no standard way to attest if product meets "my" requirements
- …no standard for adding evidence

Actor: Auditor

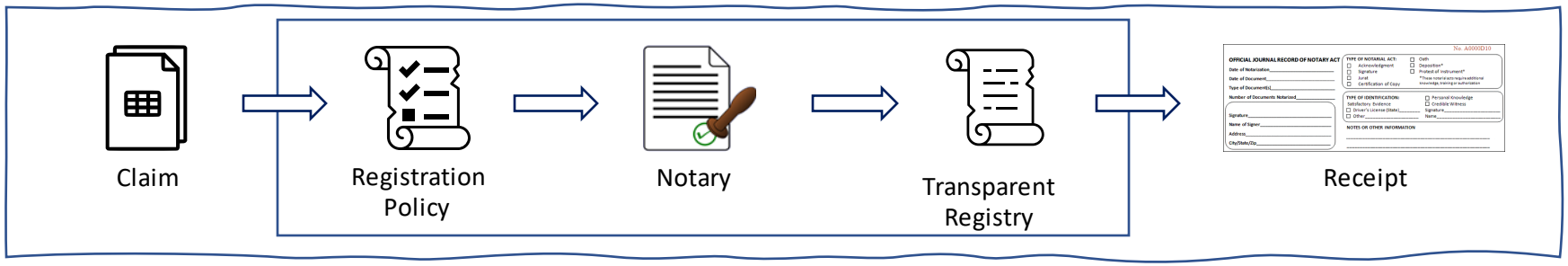


As an auditor, I need to review producer's evidence and claims to validate that products meet compliance requirements, and create new claims to support evidence of audit

Problems Today

- There is no standard way to discover and query product information across vendors, clouds, and products
- …no standard way to submit evidence and audit resultant claims

Definitions & Terms



Claim: An identifiable and non-repudiable statement about an artifact made by an Issuer

Registration Policy: Configuration for the types of identities representing issuers that may be verified, or rejected, by the notary before being placed on the registry

Notary: The act of verifying the identity of an issuer, submitting content to the system (storage + registry), based on policy, issuing a receipt for valid entry in a registry

Transparent Registry: A verifiable data structure that provides a consistent, append-only, record of all registered claims. Transparency does not *necessarily* mean public access; the notary may implement an access control policy.

Receipt: An offline, universally-verifiable proof that an entry is recorded in the registry. Receipts do not expire, but it is possible to append new entries that subsume older entries

https://ietf-scitt.github.io/draft-birkholz-scitt-architecture/draft-birkholz-scitt-architecture.html#name-definition-of-transparency

Notary Act

No. A0000D10

OFFICIAL JOURNAL RECORD OF NOTARY ACT

Date of Notarization_____

Date of Document_____

Type of Document(s) **Container Image SBOM**

Number of Documents Notarized_____

Signature_____

Name of Signer_____

Address_____

City/State/Zip_____

TYPE OF NOTARIAL ACT:

- ☐ Acknowledgment
- ☐ Signature
- ☐ Jurat
- ☐ Certification of Copy
- ☐ Oath
- ☐ Deposition*
- ☐ Protest of Instrument*

*These notarial acts require additional knowledge, training or authorization

TYPE OF IDENTIFICATION:

Satisfactory Evidence

- ☐ Driver's License (State)_____
- ☐ Other_____
- ☐ Personal Knowledge
- ☐ Credible Witness

Signature_____

Name_____

NOTES OR OTHER INFORMATION

Met ACME Security Policy – for base images

_____

_____

Transparency: Core Intuitions & Prior Work

- We cannot stop authorized supply chain actors from making false claims, but we can make them accountable by requiring their claims to be registered in a verifiable and transparent data store.
- This ensures that malicious actors who make contradictory claims to different entities (customers, auditors, regulators) can be disambiguated from valid actors.
- All consumers of claims must first verify the proof of transparency registration to ensure a claim is auditable; this proof should be compact and fast to verify offline.

Examples of transparency systems:

Certificate Transparency [RFC 9162] Adam Langley, Emilia Kasper, Ben Laurie (Google)

CONIKS: bringing key transparency to end users , M. S. Melara, A. Blankstein, J. Bonneau, E. W. Felten, and M. J. Freedman (USENIX Security'15).

Keeping authorities "honest or bust" based on large-scale decentralized witness cosigning (IEEE S&P '16)

CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds (Usenix'17, EPFL)

Contour: A practical system for binary transparency logging on bitcoin the latest authorized binary version.

M. Al-Bassam, S. Meiklejohn (Data Privacy Management, Cryptocurrencies and Blockchain Technology, 2018).

Challenges and Pain Points

Pain: Identity, attribution, and data confidentiality and integrity are unspecified, unverifiable, or inconsistently implemented, resulting in uncertain results in auditing, accountability, and assurance

Example: The current market is a mix of closed/proprietary solutions and open-source tamper-evident or tamper-proof data stores

Pain: Identity and data attribution are suspect without countersigning/notarization of the identity and content from suppliers, consumers, and auditors; Data persistence is critical to lifecycle management

Examples: Supply/value chain resiliency requires quantitative risk assessment based on notarized evidence; Servicing products requires data persistence over the entire lifecycle of the product even in the case of a defunct supplier; Used automobile scenario

Pain: Multiple data-sharing platforms, different protocols and ontologies for artifacts and claims

Example: In response to supply chain attacks, governments and companies have initiated compliance mandates, developed novel point solutions, or are still actively pursuing emergent technologies to reduce supply chain risk

Draft Problem Statement

The increasing scale, size, and complexity of supply chain digitalization challenges traditional pre- and post-audit methodologies exposing gaps in essential primitives. A minimal, simple, and concise set of building blocks could guarantee long-time accountability and interoperability for software components and their metadata through their life-cycles across architecturally diverse systems.

What are the root causes?

- Lack of legally meaningful and persistent supply/value chain data needed to automate the system
- Insufficient standards for tamper proof and independently verifiable data stores
- Absence of decentralized globally interoperable transparency services

Initial Use Case: Software Supply Chain

(20 min)

Software Supply Chain: Opportunity

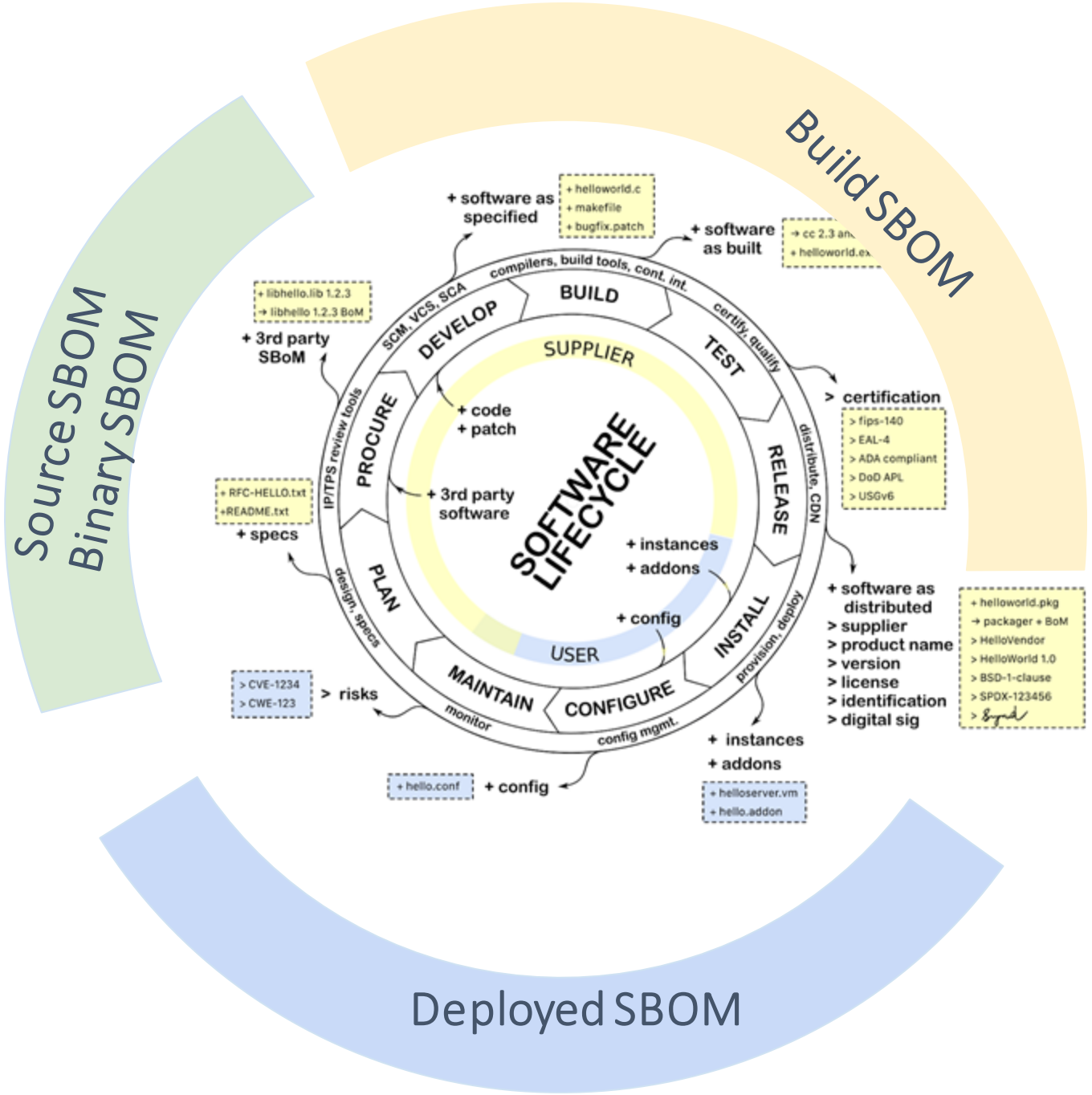
- The software supply chain is complex, dynamic, and often obscure
- The speed and number of automated releases are no longer manageable by manual processes. Humans must feed the machine
- The lack of transparency into the contributors, composition, and functionality of software-enabled systems and the trusted computing base (TCB) make automation impractical
  - Contributes substantially to cybersecurity risks
  - Increases lifecycle costs of development, procurement, and maintenance
- Third-party components are a known systemic risk
  - Transparency can drive tools and behavior to document risk, support mitigations, and drive better software development practices
- Standards enable interchange of information, as artifacts and incremental information is promoted across environments

Software Supply Chain: Market Analysis

- Emergent Software Bill of Materials (SBOM) compliance mandates from governments and industries
- SBOM is a key building block in software security and software supply chain risk management
- An SBOM by itself may not contain the necessary proofs to determine who generated it, its authenticity, and if it is verifiable
- Applications (e.g., repo and package manager health, CVE analyzers, compliance actions: endorsement/revocation/suspension) must have globally interoperable transparency services to:
  - Assure the authenticity of software suppliers, evidence, policy, and artifacts
  - Guarantee the actions of suppliers to be authorized, non-repudiable, immutable, and auditable

Software Supply Chain: Requirements

- Statements made by the producers must be identifiable, authentic, non-repudiable, and verifiable by consumers
- Allow an independent audit of provenance (i.e., chain of custody) and pedigree (i.e., history)
- Visibility and proof of issuer claim registrations
- Operationalize and automate the supply chain to scale over time



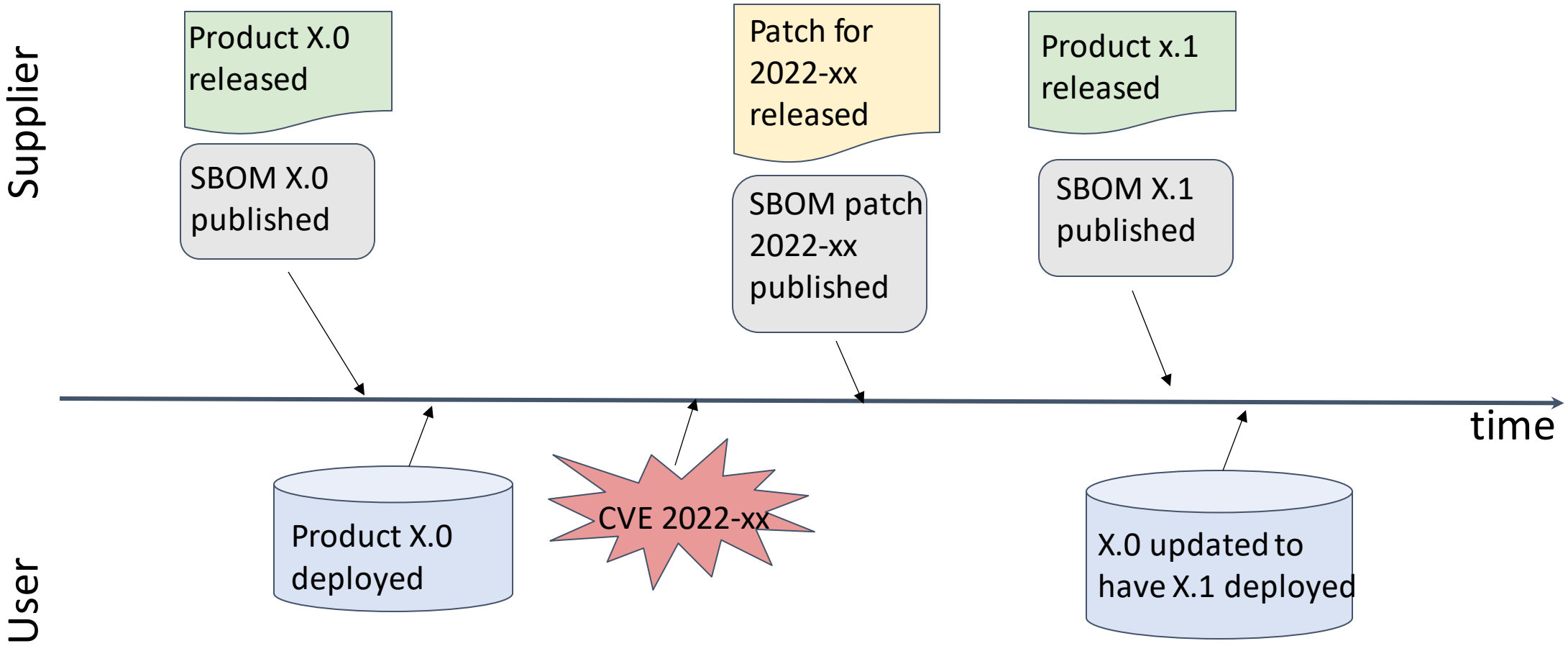
Source SBOM - software sources imported used to build binary executable image.

Build SBOM - List of components and relationships between dependent components assembled to create a product released from Supplier.

Binary Analysis SBOM - executable image to be integrated into deliverable. Created from 3rd party heuristics.

Deployed SBOM - Tracking configuration options on how a product has been deployed by User.

Understanding State through Time



Draft Problem Statement

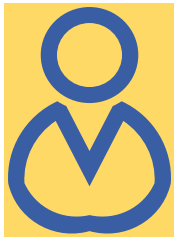
The increasing scale, size, and complexity of supply chain digitalization challenges traditional pre- and post-audit methodologies exposing gaps in essential primitives. A minimal, simple, and concise set of building blocks could guarantee long-time accountability and interoperability for software components and their metadata through their life-cycles across architecturally diverse systems.

What are the root causes?

- Lack of legally meaningful and persistent supply/value chain data needed to automate the system
- Insufficient standards for tamper proof and independently verifiable data stores
- Absence of decentralized globally interoperable transparency services

Proposed Standardization Scope
(15 min)

Proposed Standardization Scope

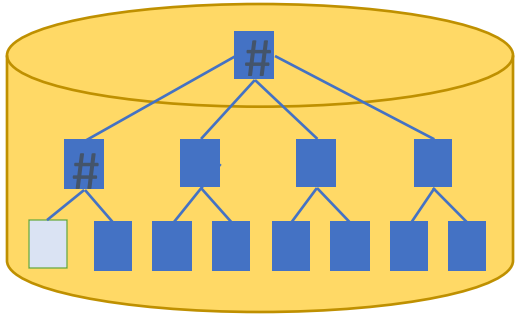


Supply Chain Issuer

Identity of SCITT Issuer, i.e., define common Identity methods that are Verifiable and Non-Repudiable for an indefinite period.

Homogeneous data format:

- in support of authenticity
- allows for multi organization and cross region interoperability
- enables ease of technology adaption



Supply Chain Claim Storage

Standardize the Store Requirements to generate homogeneity across multiple Supply Chain Systems.

Example storage requirements:

Operation types, append only, long-term integrity, immutable evidence about "statements made" & "statements read"

Proposed Standardization Scope

Define one standard format for receipts (authenticity data returned from store, like proofs, etc.) about issuer claims. Intended to enable independent verification of claims about Supply Chain Artifacts.

Supply Chain Auditor

Define a standard workflow of auditing the claims stored within the Supply Chain Claim Storage.

Standardize the processes and procedures performed by a Notary in a Supply Chain Eco-System

Out of Scope (of standardization)

1. System components that specify exact Storage, Query, or Retrieval of statements
2. Policy Language as lingo-franco in support of expressing basic requirements
3. Technology already defined in the IETF (few examples below)
   a. Use of COSE as a top-level envelope for Claims and Receipts
   b. Principles and Concepts reused from Certificate Transparency
   c. Remote Attestation to establish trust in Transparency Service's operational state
4. A Replication model across regional nodes of an instance to additionally increase trust in Transparency Services
5. Various "Bill of Material" formats and metadata header

Discussion
(60 min)

Is the IETF the right place to do this work?

Which organizations need to be involved/collaborated with?

What are the expected technical challenges?

Is there interest in implementing such specifications?

Is the technology likely to get deployed?

Is there enough interest in helping with the work (spec editing, reviewing, implementing, deploying)?

Problem Statement

It is challenging to manage the ongoing compliance of products/services against requirements across global end-to-end supply/value chains.

What are the root causes?

- Insufficient standards for tamper proof and independently verifiable data stores
- Lack of legally meaningful and persistent supply/value chain data
- Absence of decentralized globally interoperable transparency services and trusted service discovery

Next Steps

- Draft Charter
- Propose WG forming BoF during IETF#114
- Continued participation on mailing list and in community meetings
  - Mailing List
  - Community Meetings
- Review related IETF drafts
  - Countersigning COSE Envelopes in Transparency Services
  - An Architecture for Trustworthy and Transparent Digital Supply Chains

Appendix

Actor: Policy Manager (consumer)

As a policy manager, I need to ensure all products in my organization meet compliance policies

Problems Today

- It is difficult and time consuming to gather and assess compliance information (many organizations to work with, different data formats)
- Limited ability to enforce policy across end-to-end supply chain (specifically for components of products)
- Requirements change over time, requiring automated tools to keep up to rapidly updating components and products

Actor: Security Responder (consumer)

As a security responder, I need to identify all products with a given security issue, and ensure they are updated, replaced or removed

Problems Today

- It is difficult to identify which products have the identified issue
- …difficult to identify where those products are used