TEA

OWASP TRANSPARENCY EXCHANGE API

OWASP Transparency Exchange API UPDATE

oej CISA SBOM 2025-05-12 v1.1
Olle E Johansson - oej@edvina.net

OWASP®

TC 54
https://tc54.org/

CycloneDX

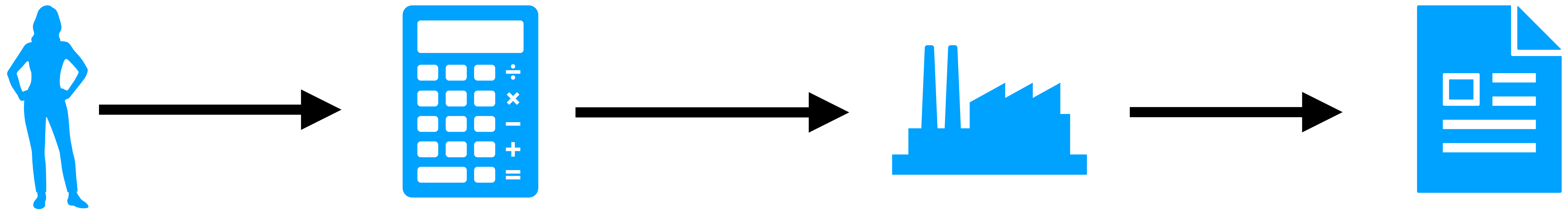
Project Koala

The problem

Many customers have many products from many vendors.

In order to **automatically** or manually be able to retrieve standardised transparency attestations (SBOM, VEX and others) we need to also standardise **discovery**, **identification**, **authentication** and retrieval of these documents.

The solution has to scale globally.



Customer

Product

Manufacturer

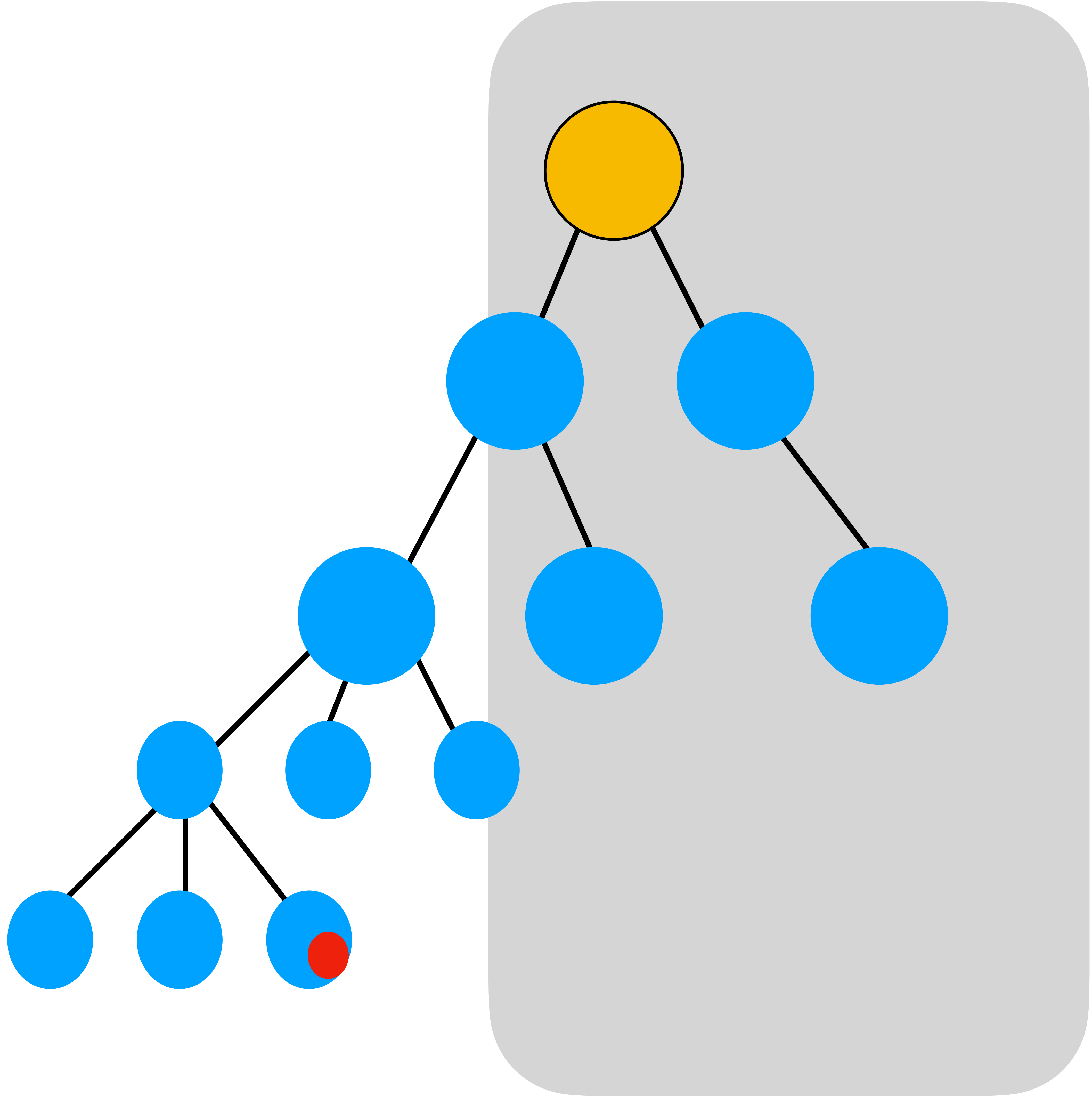
Document

The supply chain

- **As a customer**, I need to get attestations from all my suppliers - both commercial and open source

- **As a manufacturer,** I need to get attestation from upstream suppliers, both commercial and open source

- As an **Open Source project**, we need to make sure that our software with dependencies can always be built without vulnerabilities



It’s not only about the SBOM

SPDX SBOM

CycloneDX SBOM

VEX

SCITT Statement

IN-TOTO Attestation

CBOM

HBOM

Certificate of compliance

Other Attestation

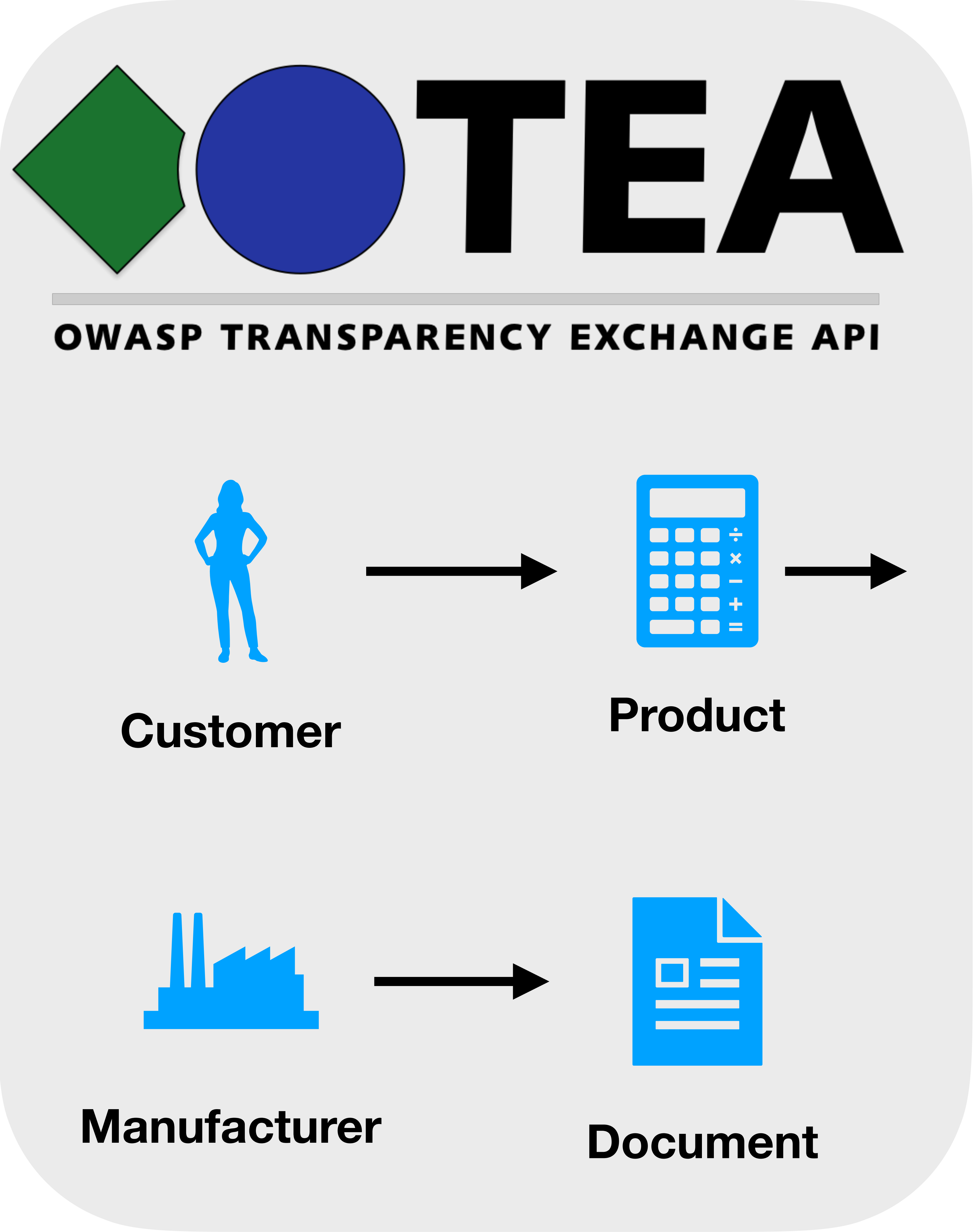
Many different attestations depending on sector, regulation and type of product.

TEA will be a standardised API

- The **Transparency Exchange API** will standardise publication and retrieval of transparency data for software and hardware.
- The API is based on a **discovery scheme** with a URN called Transparency Exchange Identifier
- The URN uniqueness is based on DNS names and existing product identifiers, from EAN barcodes to Package URLs and random UUIDs. The manufacturer defines the TEI.
- While TEA is standardised as part of the OWASP CycloneDX project, it's not specific to the CycloneDX format.
- TEA includes authentication and authorization, controlling who can access what information and who can publish what.

TC 54

ECMA
https://tc54.org/



TEA Components

Product

A product is something sold with software - an app, a server, embedded system, toy, IoT sensor etc

TEX Product index

TPI is a list of parts in a product, called TEA leaves. For each part there is a pointer (TEI or URL) for the TLI for each leaf.

TEX Component index

TLI is an index of all software versions for a product with indications of the state of the software version and reference to where a collection can be found.

TEI

TEI is a Transparency Exchange Identifier. A unique identifier for a specific product regardless of software version.
TEI is based on existing identities for a product, not replacing them.

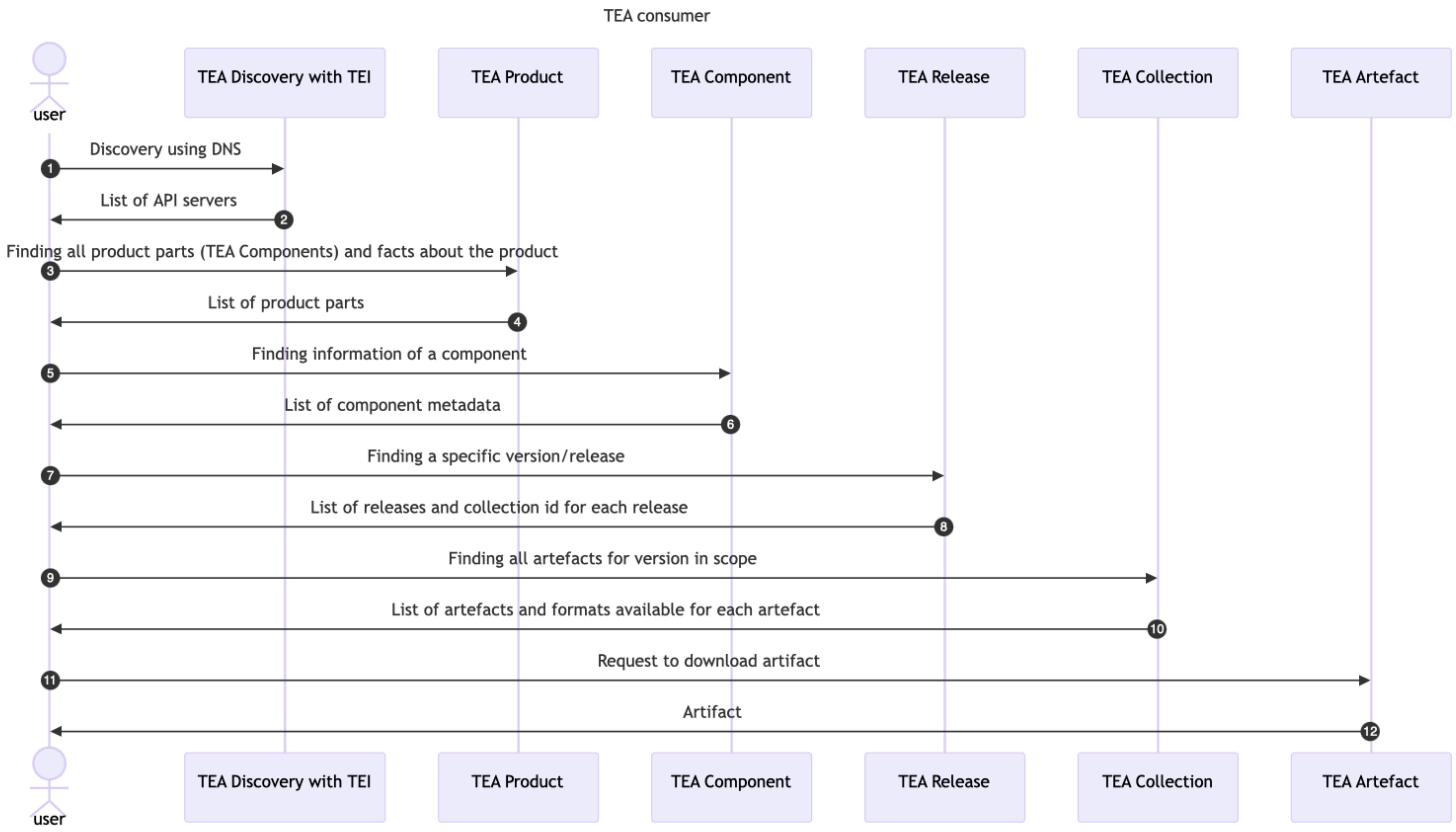
TEA Collection

The TEA collection is the repository of current artifacts for a specific version of software in a given product.
The collection includes SBOM, VEX, SLSA attestations and more.

TEA
OWASP TRANSPARENCY EXCHANGE API

The API flow

https://github.com/CycloneDX/transparency-exchange-api/blob/main/api-flow/consumer.md

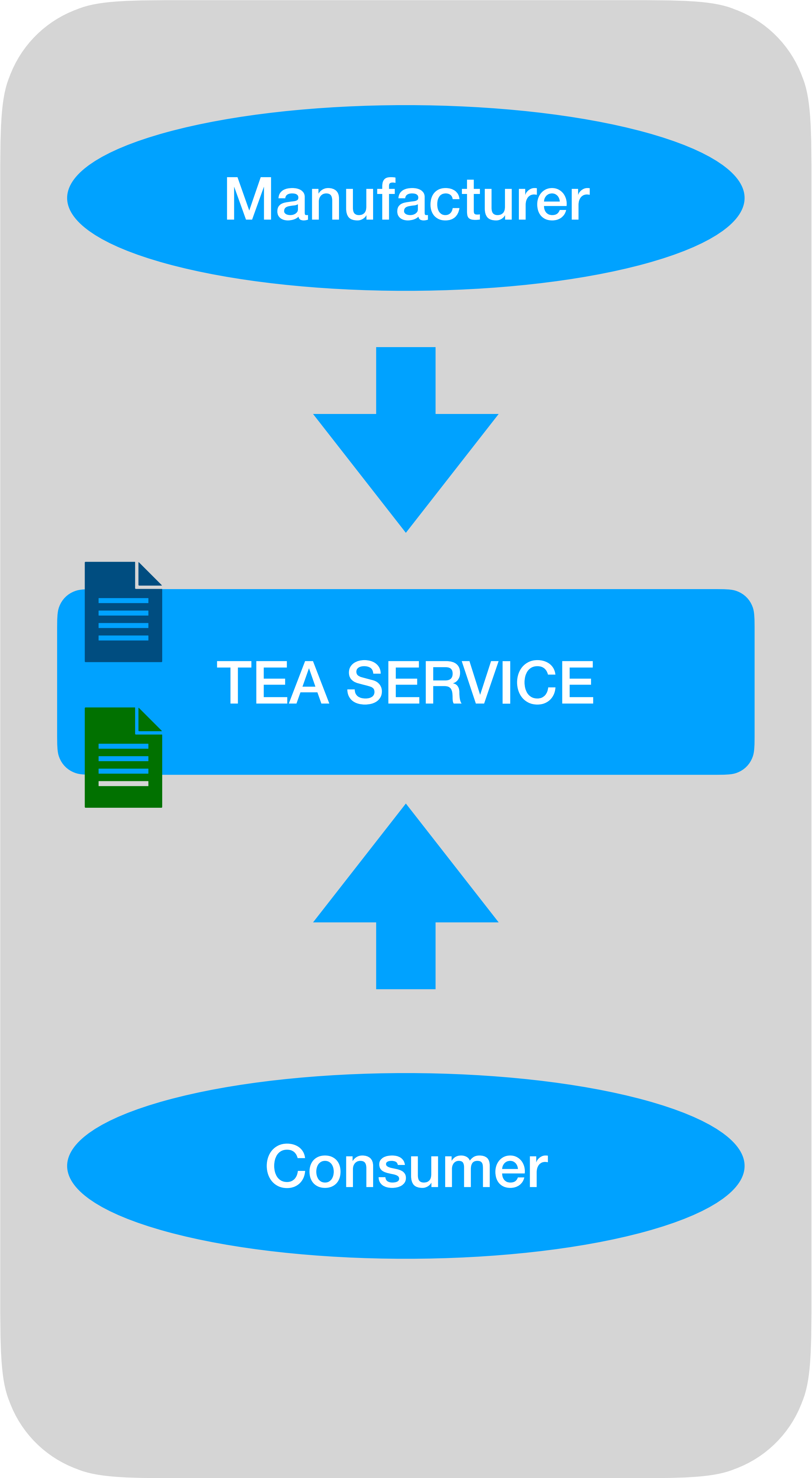


TEA consumer

1. Discovery using DNS
2. List of API servers
3. Finding all product parts (TEA Components) and facts about the product
4. List of product parts
5. Finding information of a component
6. List of component metadata
7. Finding a specific version/release
8. List of releases and collection id for each release
9. Finding all artefacts for version in scope
10. List of artefacts and formats available for each artefact
11. Request to download artifact
12. Artifact

Step 1: Artifact retrieval

- The first focus is to get the basic API done for distribution of various kinds of artifacts
- Publication API for manufacturers
- Consumer API for customers
- Discovery mechanism to find the API servers on the net
- Getting information about new versions and life cycle events (CLE)
- Support for hosted solutions (multi-tenant)



Step 2: Insights

- In a coming release we'll add insights
- Insights allows for a "limited transparency" that can be handled within the API using an expression language that can be tightly scoped or outcome-driven.
- Insights allow customers to query like:
    - Do any of my licensed produces from use Apache Struts?
    - Are any products vulnerable for log4shell - is there any action I need to take?

TEA
INSIGHTS

Status update

Generic modules	Consumer	Publisher
Discovery: Stable	Open API spec: BETA	Workflow: Started
Object model: Stable	Security arch: BETA	Open API spec: Alfa
Use cases: Done	Authentication, authoritization BETA	Security arch: Not yet
	Implementation: Not yet	Implementation: Not yet

Time to start coding!

TEA Clients

TEA client libraries

TEA Servers

TEA addon layers to existing platforms

TEA Automated tests

HACK{A}THON

{WED_MAY_28_2025}

OWASP 2025 GLOBAL AppSec | BARCELONA MAY 26-30

CycloneDX

ecma INTERNATIONAL

Summary

- TEA BETA 1 is now live!

- Hackathon May 28th 2025 to test implementations and feed back to standardisatoin

- Starting standardisation process in ECMA TC54 Summer 25

- **Meet us at OWASP Global AppSec Eu in Barcelona!**

TEA

OWASP TRANSPARENCY EXCHANGE API

Join the work!

We are working on writing specifications for the API and the various formats.

Join the OWASP CycloneDX Transparency Exchange API working group today to participate. We have a channel in the CycloneDX slack space to communicate.

`https://github.com/CycloneDX/transparency-exchange-api`

`https://cyclonedx.org/about/participate/`

OWASP

TEA

OWASP TRANSPARENCY EXCHANGE API

TC 54

https://tc54.org/

CycloneDX

Project Koala