How do we automatically discover and exchange SBOMs and other artefacts?

Introducing TEA
- the OWASP Transparency Exchange API

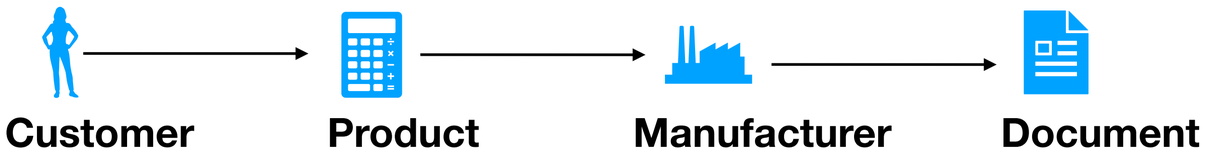
Project KOALA

The problem:

Many customers have many products from many vendors and Open Source projects. Manual login and download is not an alternative.

In order to automatically be able to retrieve standardised software 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 and be standardised.



A global standard.

We’re part of ECMA TC54.

The **TEA API** is being developed as part of the ECMA TC54 working group in order to become an ECMA standard. TC54 is the Software and System transparency working group that standardise CycloneDX, PURL and the Transparency Exchange API.

TEA will be standardised in TG1 of TC54.

ecma INTERNATIONAL

TC 54

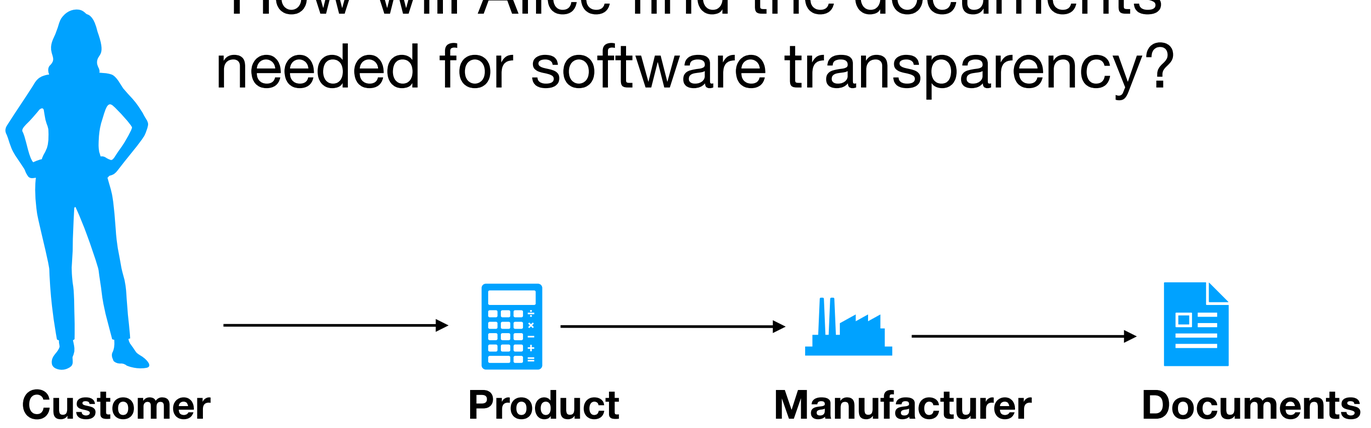
https://tc54.org/

CycloneDX

The starting point:

A user (Alice) has bought or is about to buy software or embedded systems from a vendor.

How will Alice find the documents needed for software transparency?



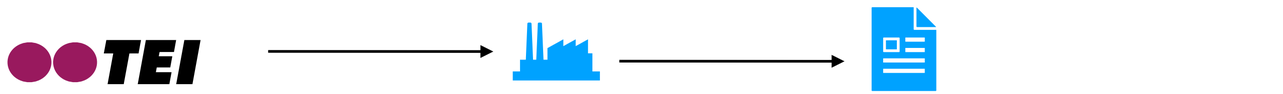
No single identifier.

There is no single identifier for software. Any solution has to support as many existing identifiers as possible.

Introducing our proposal: the TEI URN.

TEI is the **Transparency Exchange Identifier**. A unique identifier for a specific product regardless of software version.

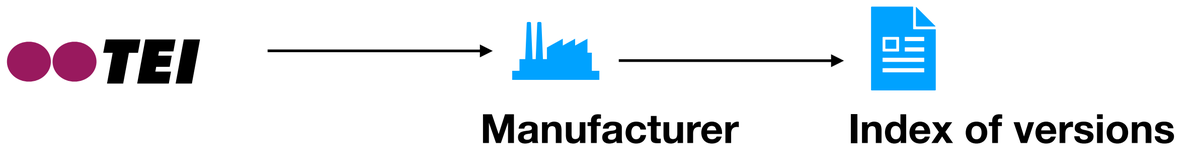
```
urn:tei:uuid:products.example.com:d4d9f54a-abcf-11ee-ac79-1a52914d44b1
```



TEI: An extensible DNS-based identifier

TEI can embed existing identifiers - product numbers, EAN bar codes, PURLs and many others. It can of course be a QR code on packaging or invoices.

TEI uses DNS for discovery. The goal is to find a **TEA index** of software versions and pointers to artefacts for each version.



Introducing TEA
- the OWASP Transparency Exchange API

The TEA product index

The TEA product index (TPI) lists all parts of a product sold using a restful HTTP based API with support for authentication and authorization.

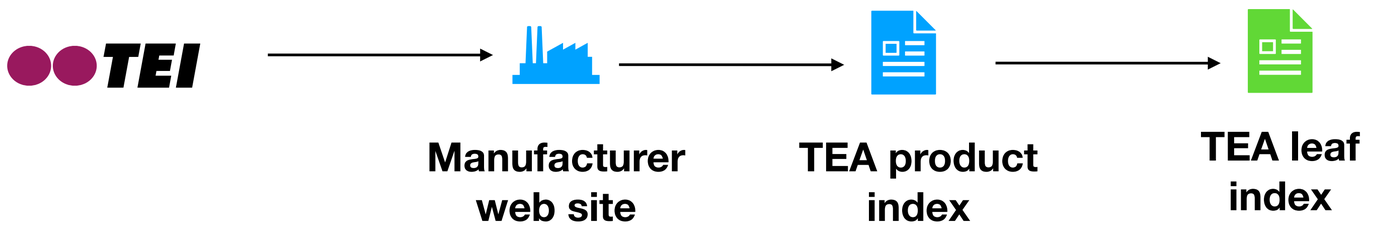
A single product may have multiple parts, called leaves, with different versions. The leaves can be created by multiple manufacturers.

The TPI may contain Common Lifecycle Enumeration objects, indicating the lifecycle status of the product.

The TEA Leaf index

The TEA leaf index lists all versions using a restful HTTP based API with support for authentication and authorization.

The **TEA leaf index** will also include the status of each version, a common lifecycle enumeration, indicating if the software is supported, past end of life or replaced by a new version because of a vulnerability.



The TEA collection

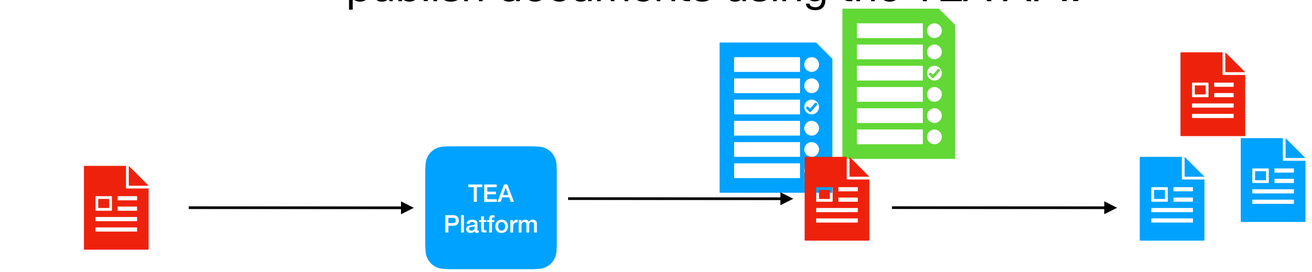
The TEA leaf index includes an identifier for a collection of artefacts for each software version.

The **TEA collection** will include a set of files in various formats, like CycloneDX or SPDX Bill of materials, VEX files, CSAF, In-Toto attestations, VDR, CDXA, SCITT Statements, EU certificate of compliance with the CRA and other documents needed for software transparency.

TEA publishing

The transparency exchange API will support publication of signed artefacts.

A vendor or an open source project will be able to publish documents using the TEA 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

CycloneDX

Project Koala