Project KOALA

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

SBOM a RAMA
CISA.GOV/SBOM

Introducing TEA
- the OWASP Transparency Exchange API

oej@edvina.net

OWASP®

CycloneDX

Software transparency

Being transparent about the components in a product.

Being transparent about vulnerabilities in a product.

Sharing certifications and attestations with users.

Standard document formats and automation is the key!

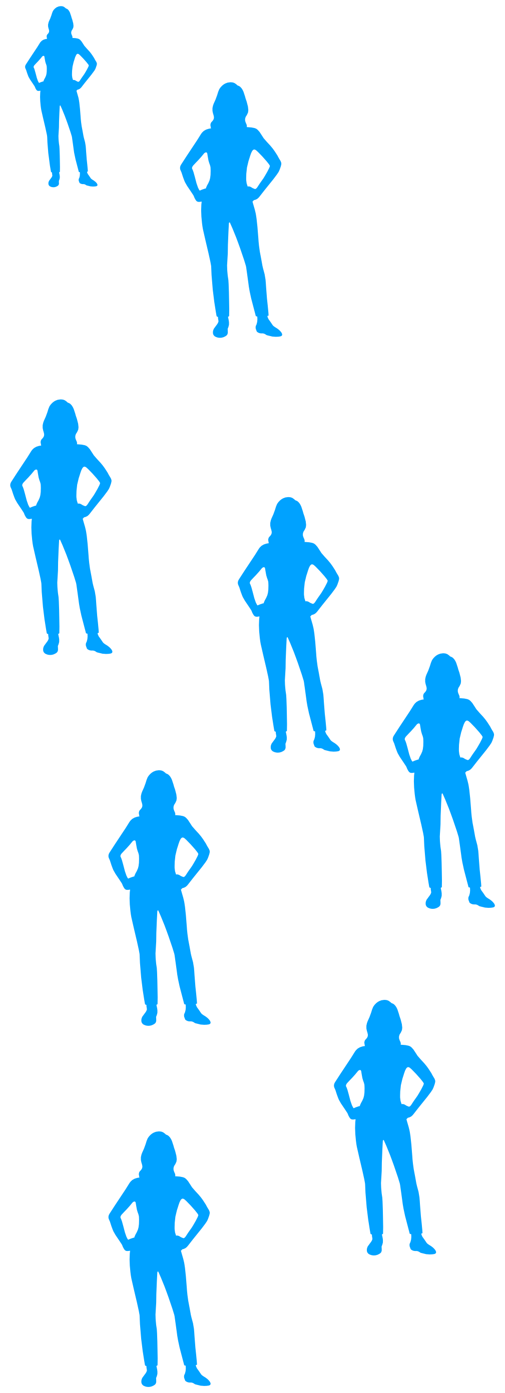
Customer

Product

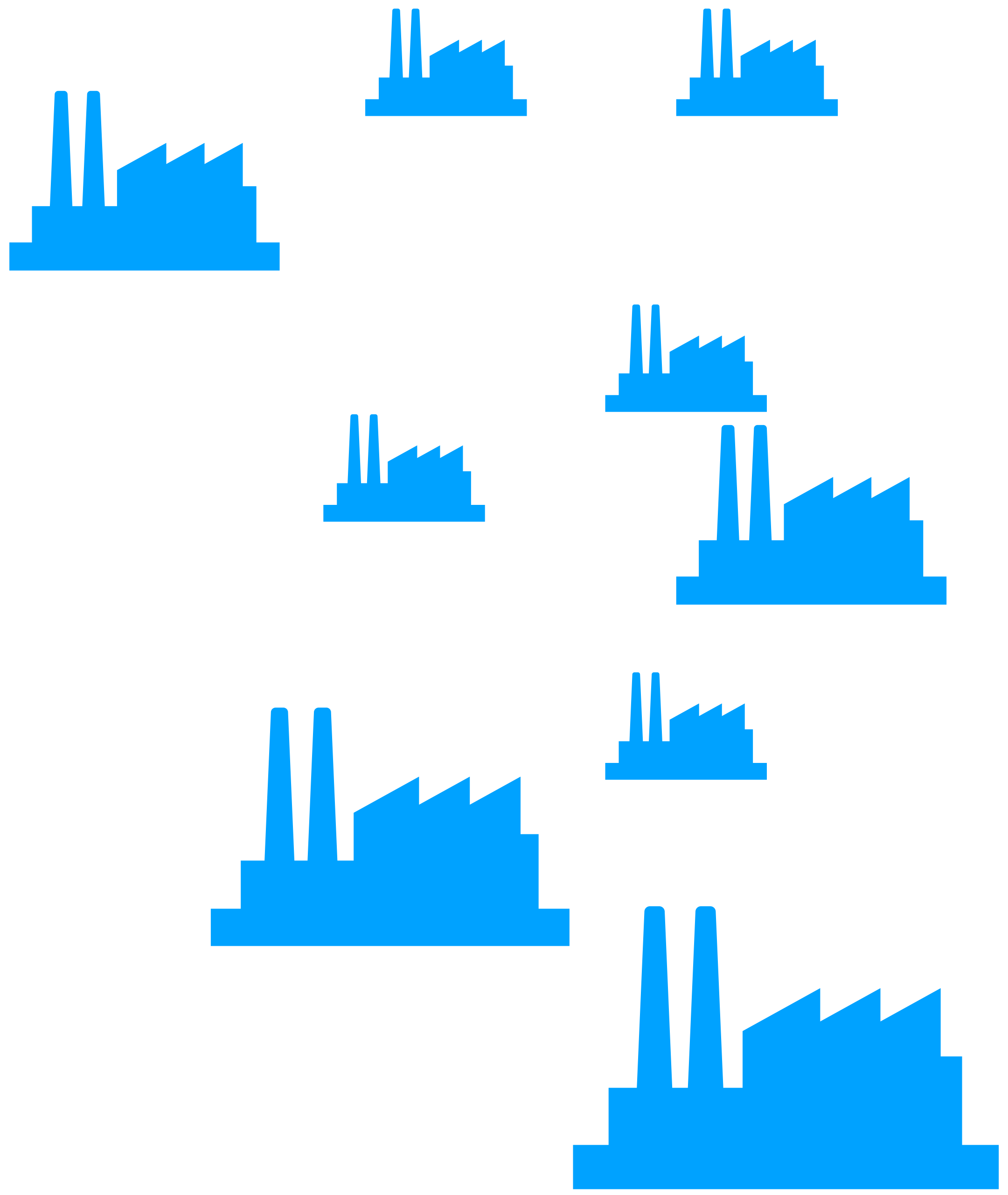
Manufacturer

CycloneDX
SPDX
In-TOTO
SCITT
...and more formats.

The problem:



Many customers have many products from many vendors and Open Source projects. Manual login, manual exchange and manual 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.

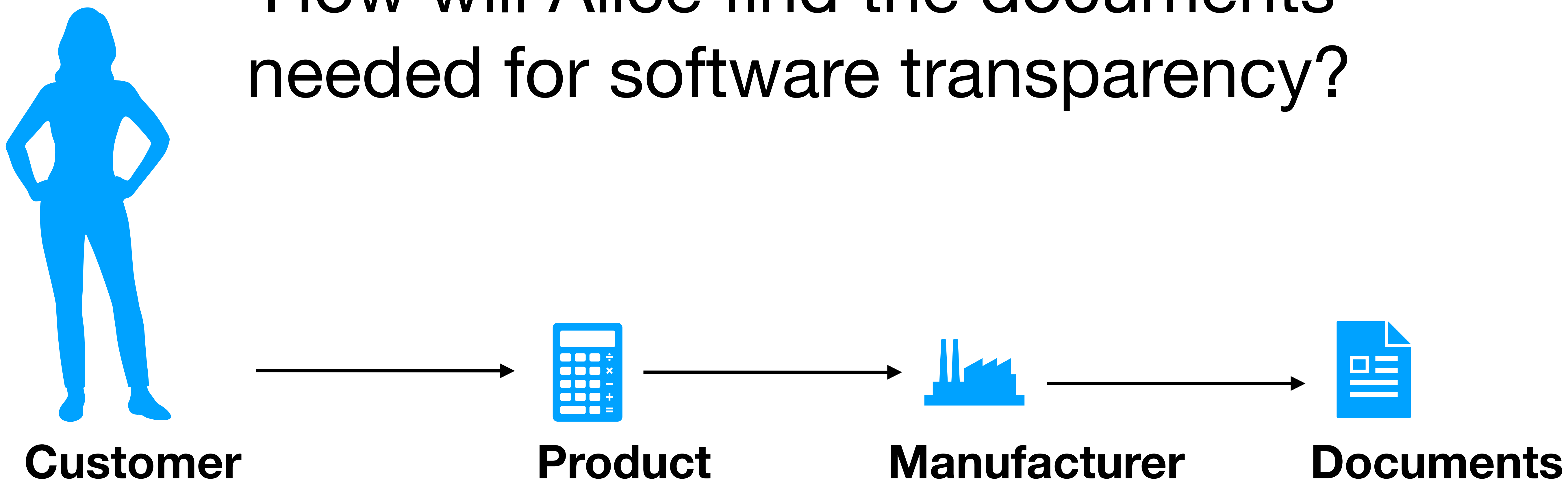
The solution has to scale globally and be standardised.

Customer **Product** **Manufacturer** **Document**

The starting point:

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

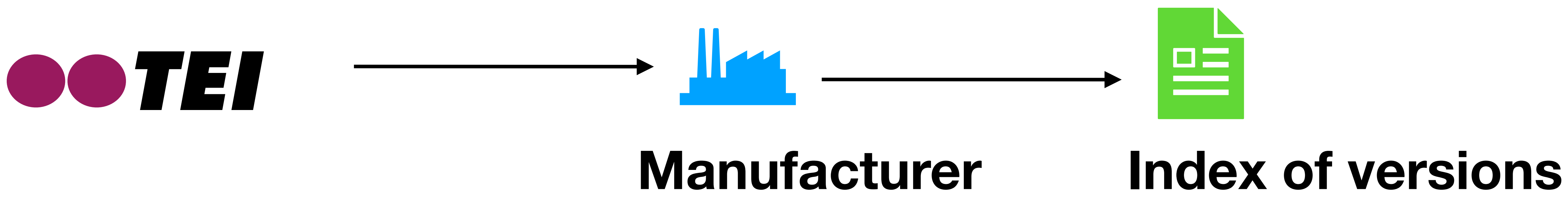
How will Alice find the documents needed for software transparency?



Introducing 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 included in a product and pointers to artefacts applicatble to each version.



Manufacturer

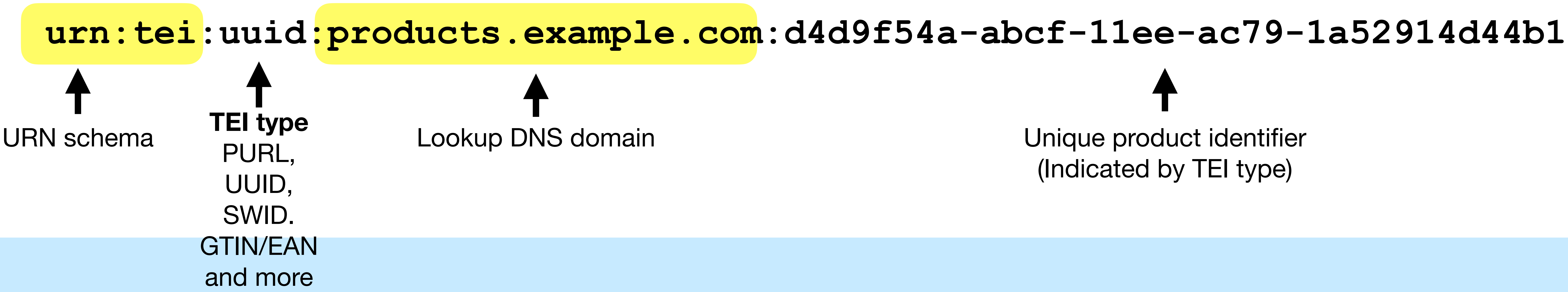
Index of versions

Discovery: The TEI URN

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 created by the manufacturer for a specific product regardless of software version.



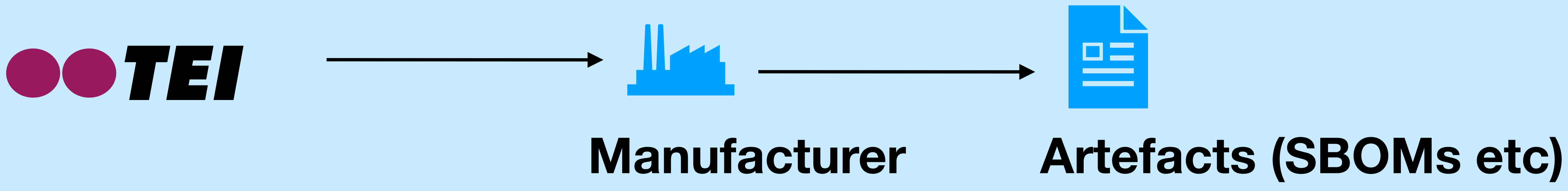
```
urn:tei:uuid:products.example.com:d4d9f54a-abcf-11ee-ac79-1a52914d44b1
```

URN schema

TEI type
PURL,
UUID,
SWID.
GTIN/EAN
and more

Lookup DNS domain

Unique product identifier
(Indicated by TEI type)



Manufacturer

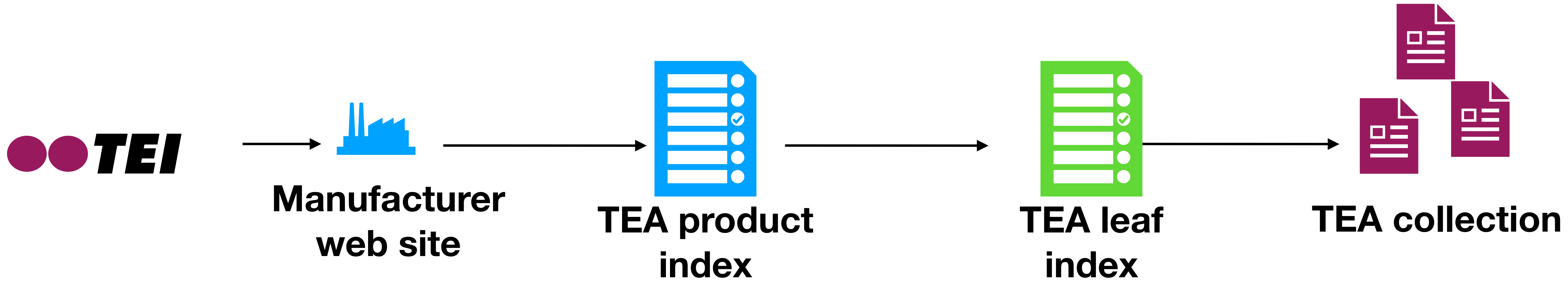
Artefacts (SBOMs etc)

The TEA objects

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.

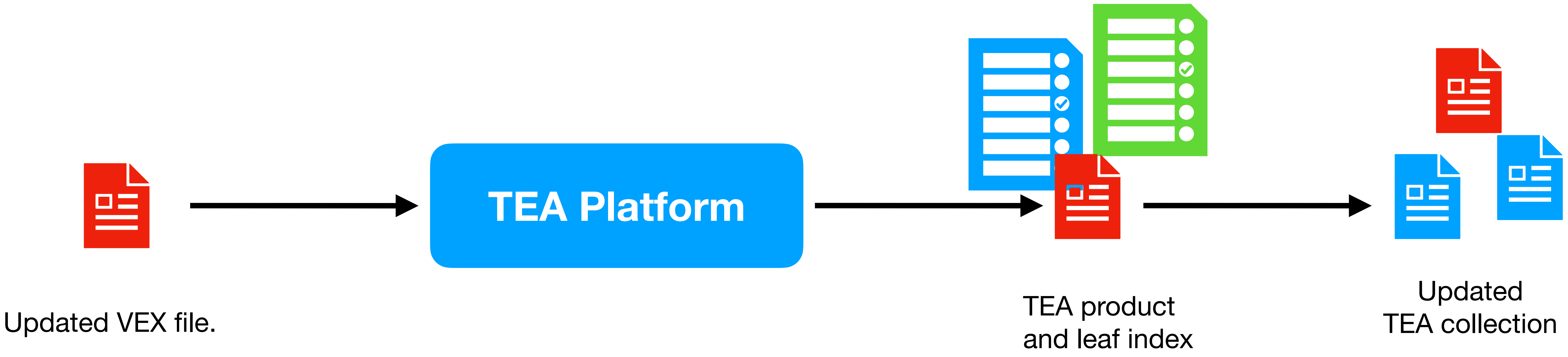
Optional Authentication and Authorization limits who can access what.



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 Publishing API.



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 ECMA TC54.

ecma INTERNATIONAL

TC 54

https://tc54.org/

CycloneDX

Got SBOM? Get TEA!

If your platform imports or exports SBOM, VEX files or
other attestations, then you want to be part of this work.

Help your customers to
automate the transparency workflow.

SPDX SBOM

CyloneDX SBOM

VEX or CSAF

SCITT Statement

IN-TOTO Attestation

Certificate of compliance

Other Attestation

Join the work!

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

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

Find all the links on our github page!

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

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

E-mail: oej@edvina.net @oej@infosec.exchange

OWASP®

CycloneDX