OWASP TRANSPARENCY EXCHANGE API

OWASP Transparency Exchange API - the Data model

oej/aph wg 2024-11-19 v2.1
Olle E Johansson - oej@edvina.net

OWASP

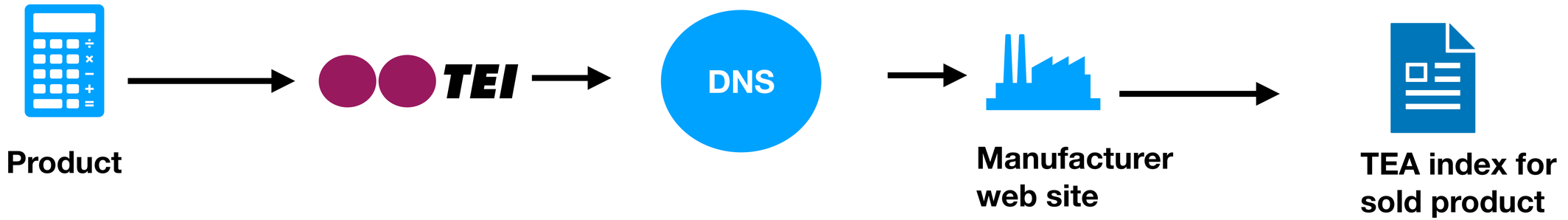
TC 54

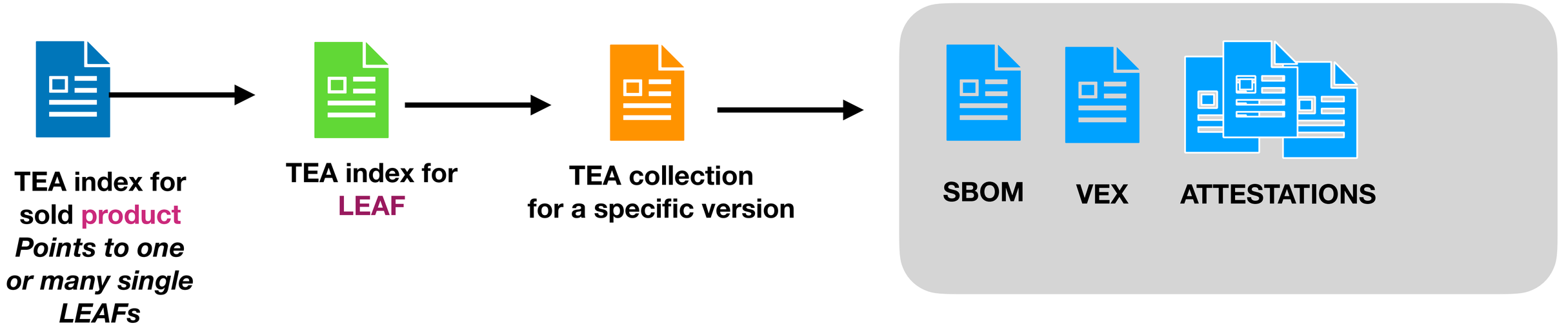
https://tc54.org/

CycloneDX

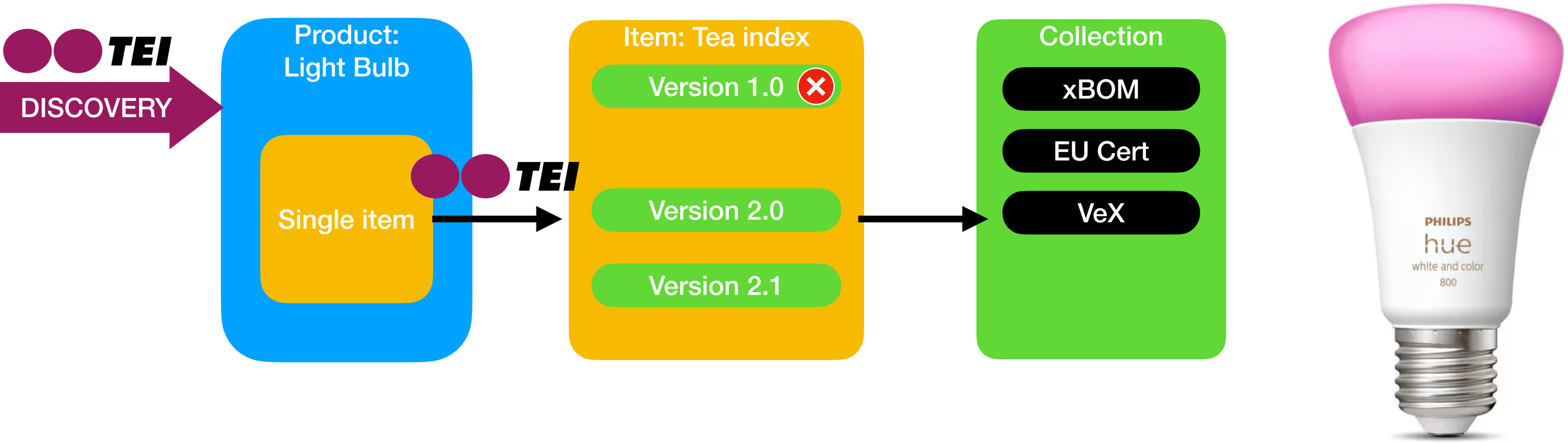
Project Koala

Discovery of transparency data

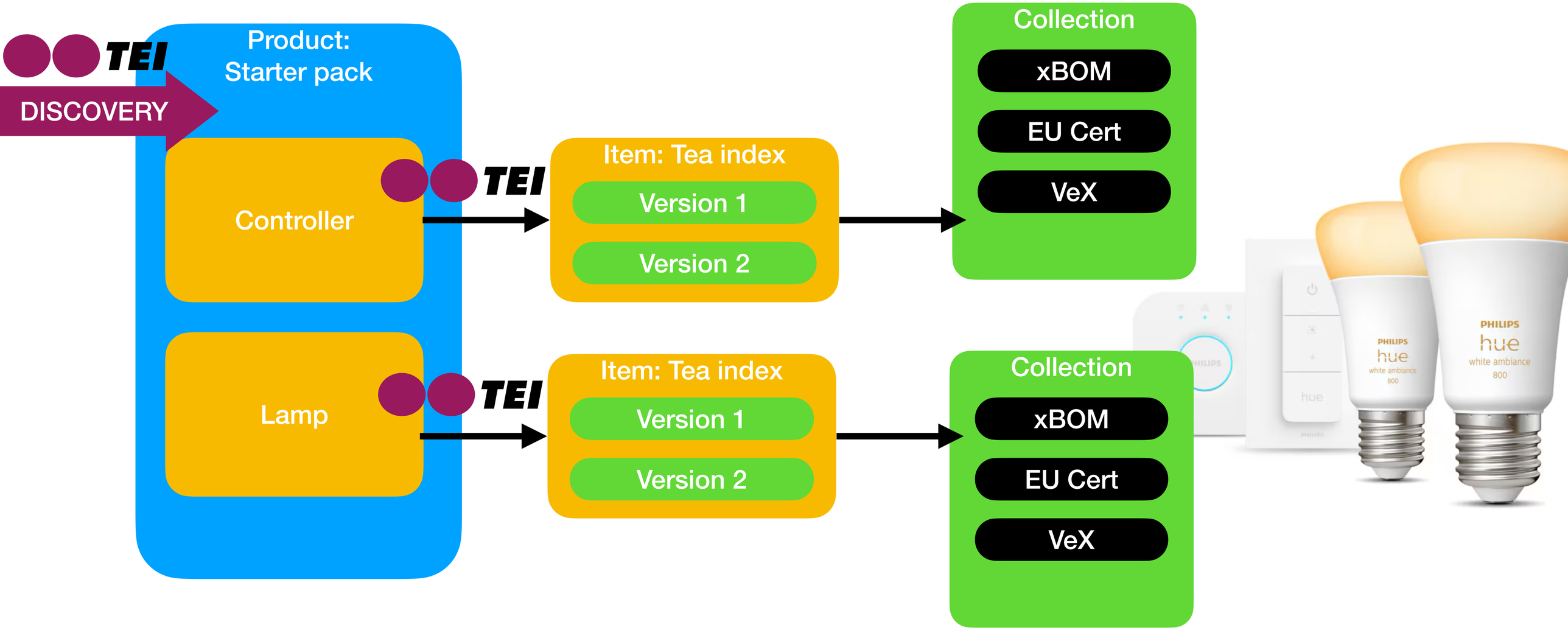




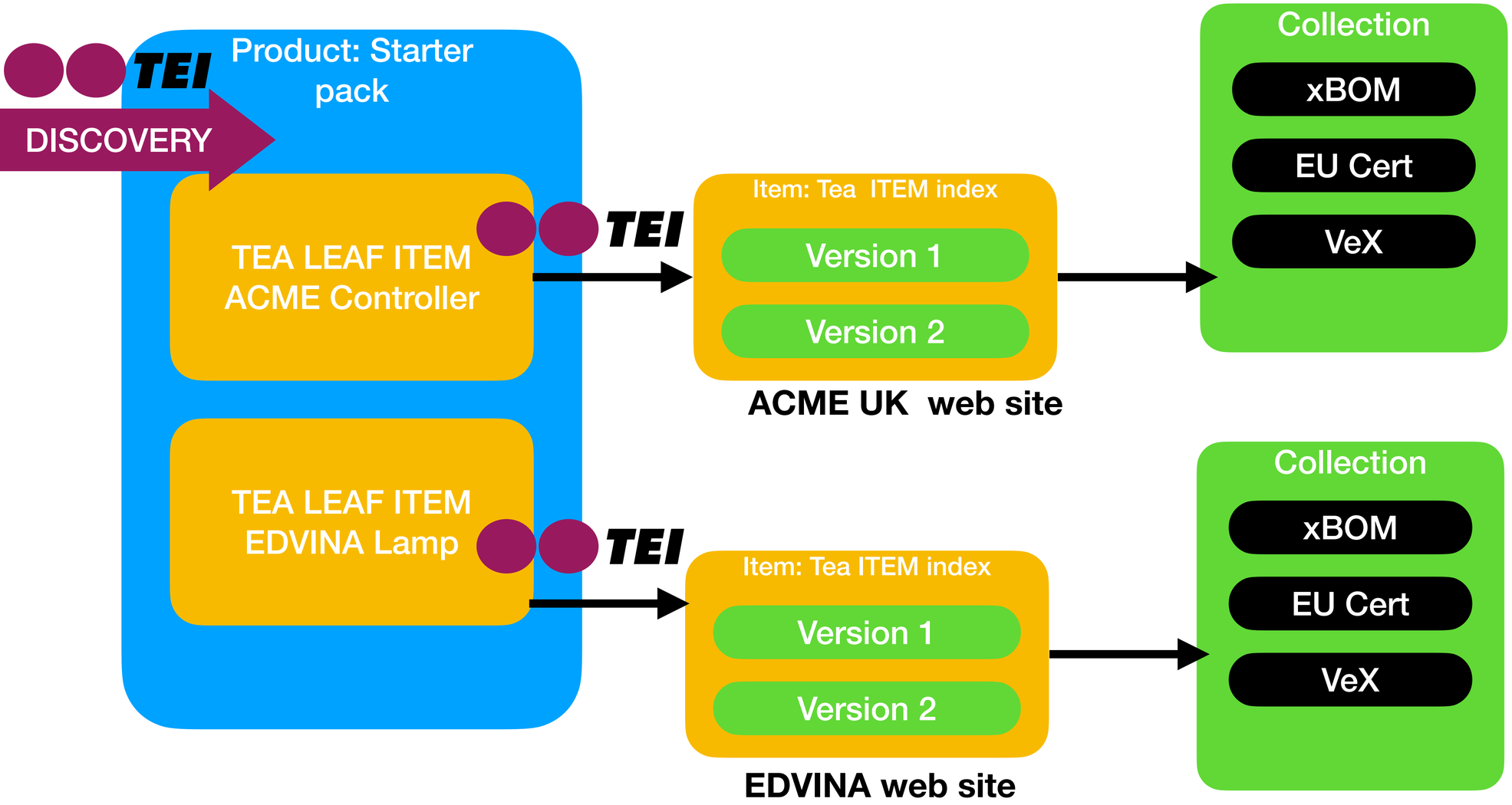
Intelligent light bulb



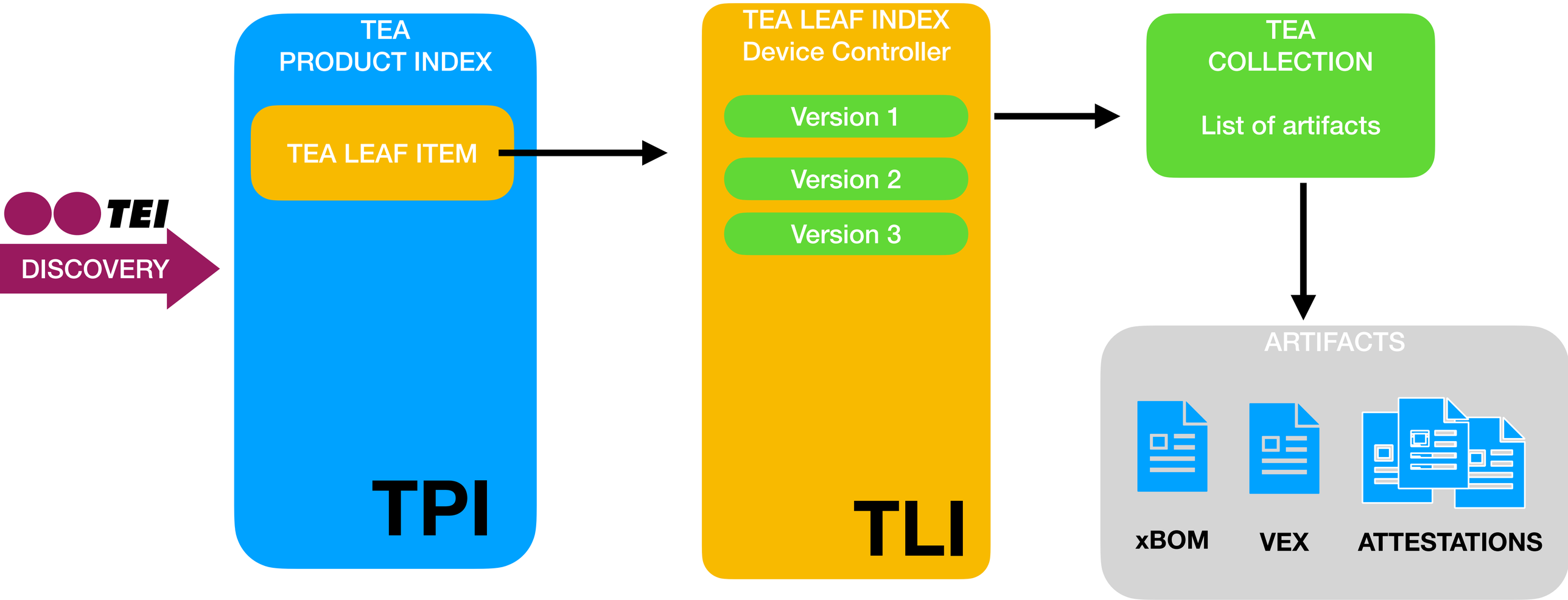
Starter pack



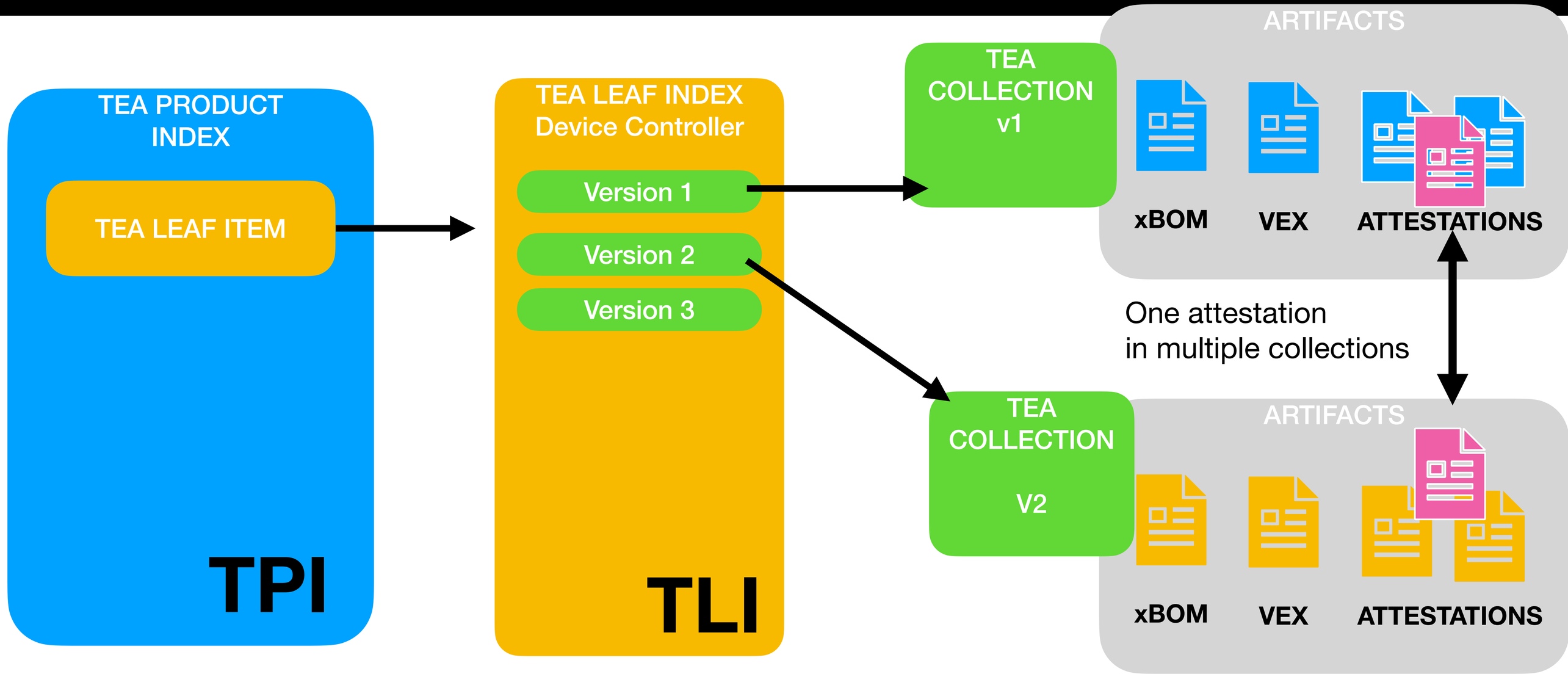
Pack from multiple vendors



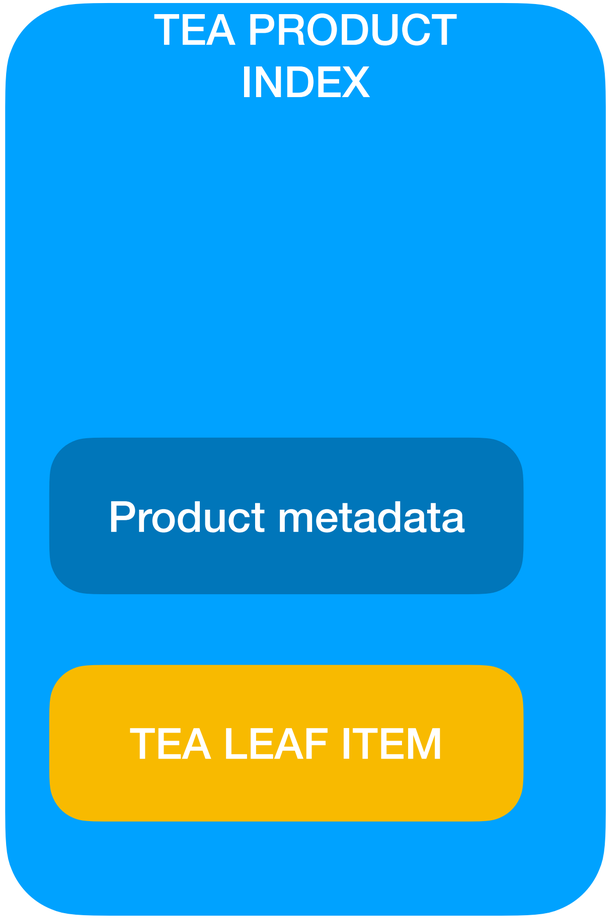
Overview TEA object model



The same attestation in multiple collections



TEA Product Index



- The first point of entry (TPI) or a product is a list of available TLI (verson indexes) for various components (one or many)
- For each product, a structured document (TLI) contains a list of UUIDs on where to find the collection for **each supported version** of the product.
- The product can be reached through one or multiple identifiers (TEI)
- The identifier (Tea Product UUID) of the structured document needs to be standardised and persistent in order to support automation.
- A document with no longer supported versions may need to exist as well.
    - *CRA mandates that documents as well as updates shall be available for all versions during the product lifetime*
- We need a redirect facility if products change ownership. (See common lifecycle enumeration - CLE - work in OWASP)

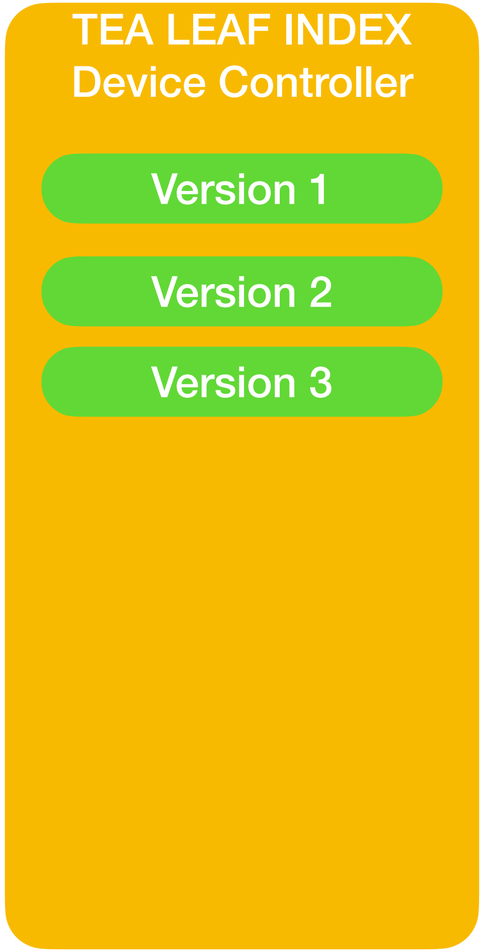
The TEA Leaf Index

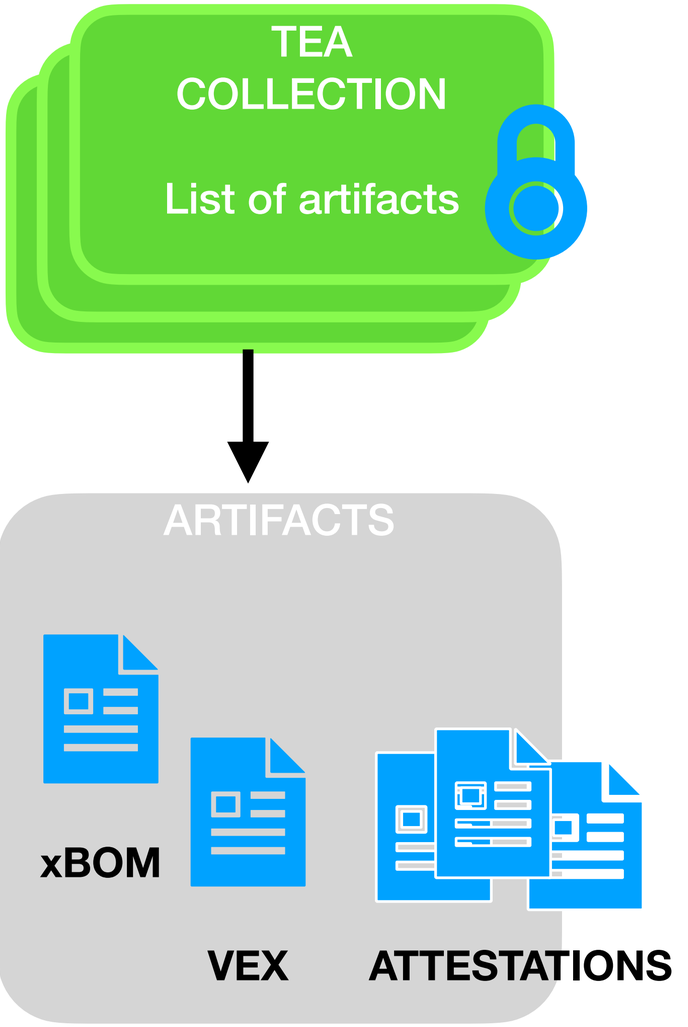
The TEA Leaf Index is a list of “versions”

The TEA Leaf object has the following parts

- UUID of TEA leaf
- Product name
- Product version (string, no syntax required)
  - Semver
  - Git HASH (sha1)
  - Random name
  - OmniBOR (sha256)
- Product Release date (timestamp)
- State: Prelease (boolean)

Notes
- Different Major versions have different TEA LEAF indexes
  - "Major version X"
  - "Major version Y"
- Lifecycle Enumeration ("states") is part of "insights" - i.e. to be documented in Vex





The TEA Leaf

The TEA Leaf is a list of “versions”

Major X “current”

Minor X

Minor Y

Major version Y

Minor Q

Minor P

TEA LEAF INDEX
Major X

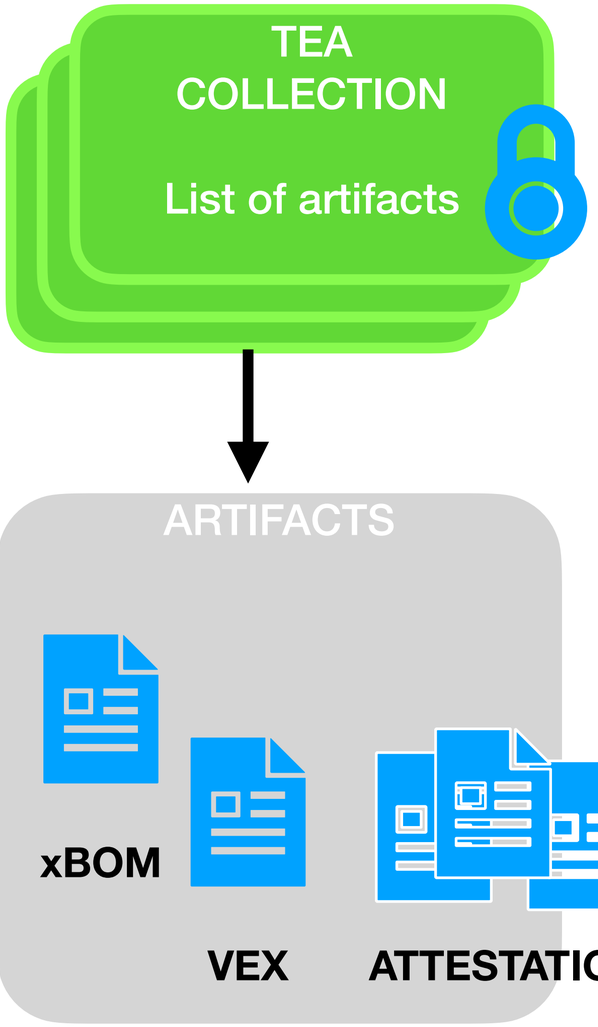
Leaf

Leaf

TEA LEAF INDEX
Major Y

Leaf

Leaf



TEA Collections

- The URL for a collection needs to be persistent to support automation
- A collection is a set of files (often signed) that applies to a specific product and version
- The collection index file indicates where to find SBOM, VEX, attestations and similar documents (like a conformance attestation for the CE marking in EU)

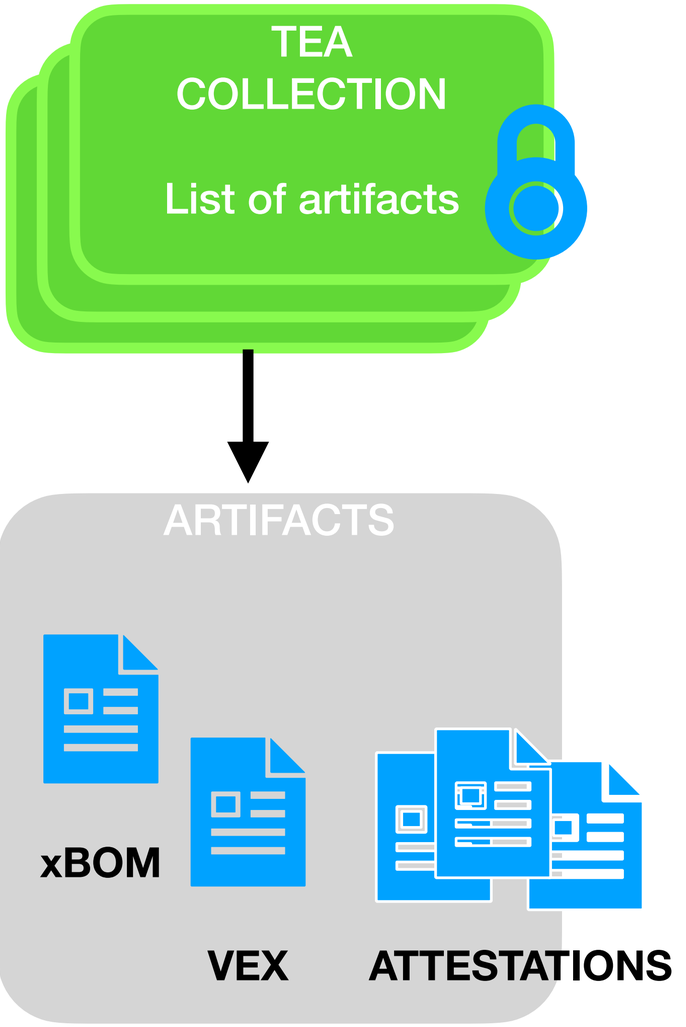
The TEA Collection

The TEA collection is a list of artifacts

- For one single version
- it contains references to artifacts

The TEA Collection object has the following parts

- Preamble
- UUID of TEA collection object
- Product name
- Product version
- Product Release date (timestamp)
- Author of TEA Collection (name, email, company)
- TEA Collection object release date (timestamp)
- TEA Collection object version (integer starting with version 1)
- Reason for update/release of TCO - clear text
  - "New product release"
  - "Corrected dependency in SBOM that was faulty"
  - "Added missing In-Toto build attestation"
- List of artifact objects (next slide)
- Optional Signature



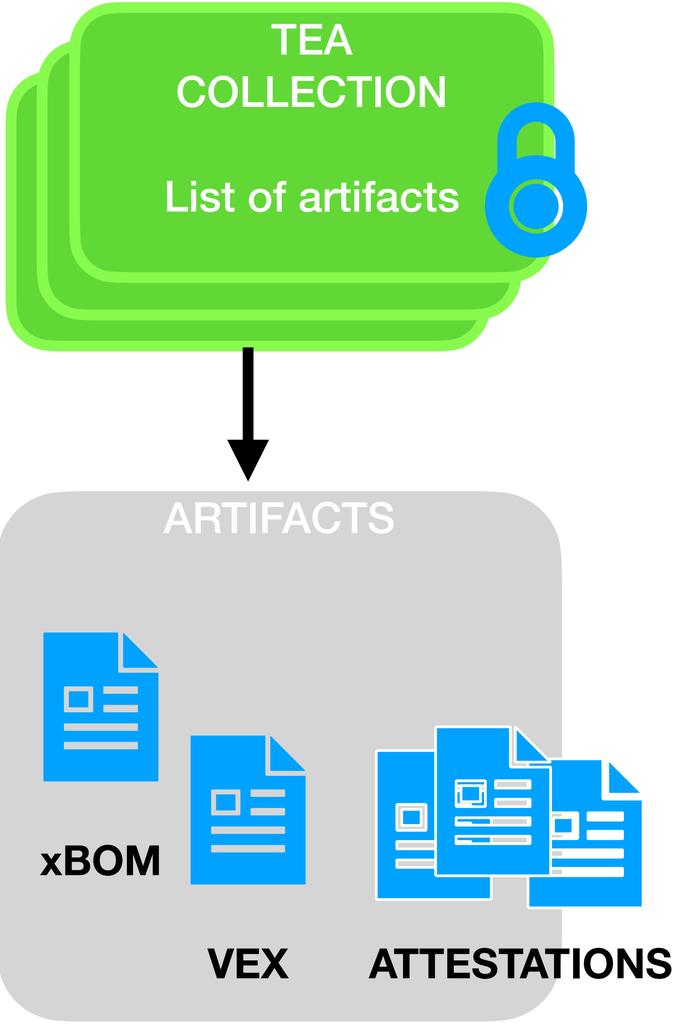
The TEA Collection artifact

The TEA artifact is a unique piece of data

- an artifact can be published for multiple collections.

The artifact object has the following parts

- Artifact UUID
- Artifact name
- Author of Artifact (name, email, company)
- List of objects - various formats of the same data. The order of the list has no significance.
  - UUID for artifact
  - Optional BOM identifier
  - SPDX or CycloneDX reference to BOM
  - MIME media type
  - Artifact category (enum)
    - https://cyclonedx.org/docs/1.6/json/#externalReferences_items_type
  - Description in clear text
  - Size in bytes
  - SHA384 checksum



Reasons for updating the collection

Updated the VEX

Updated the manual

Updated the SBOM
- found a missing dependency
or an extra non-existing dep

ENUM list needed!

VEXUPDATE

SBOMUPDATE

MISCCHANGE

The USER may want to see
what changed and audit the change.
Get notifications
from their system when it happens.

Summary

- The API is built to handle many kinds of artefacts - is agnostic to format and content
- It will be defined using OpenAPI for interoperability
- One API for consuming transparency artifacts and one for publishing
- The object definitions will evolve, but we good a good starting point

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