Project KOALA

TEA Collections and transparency

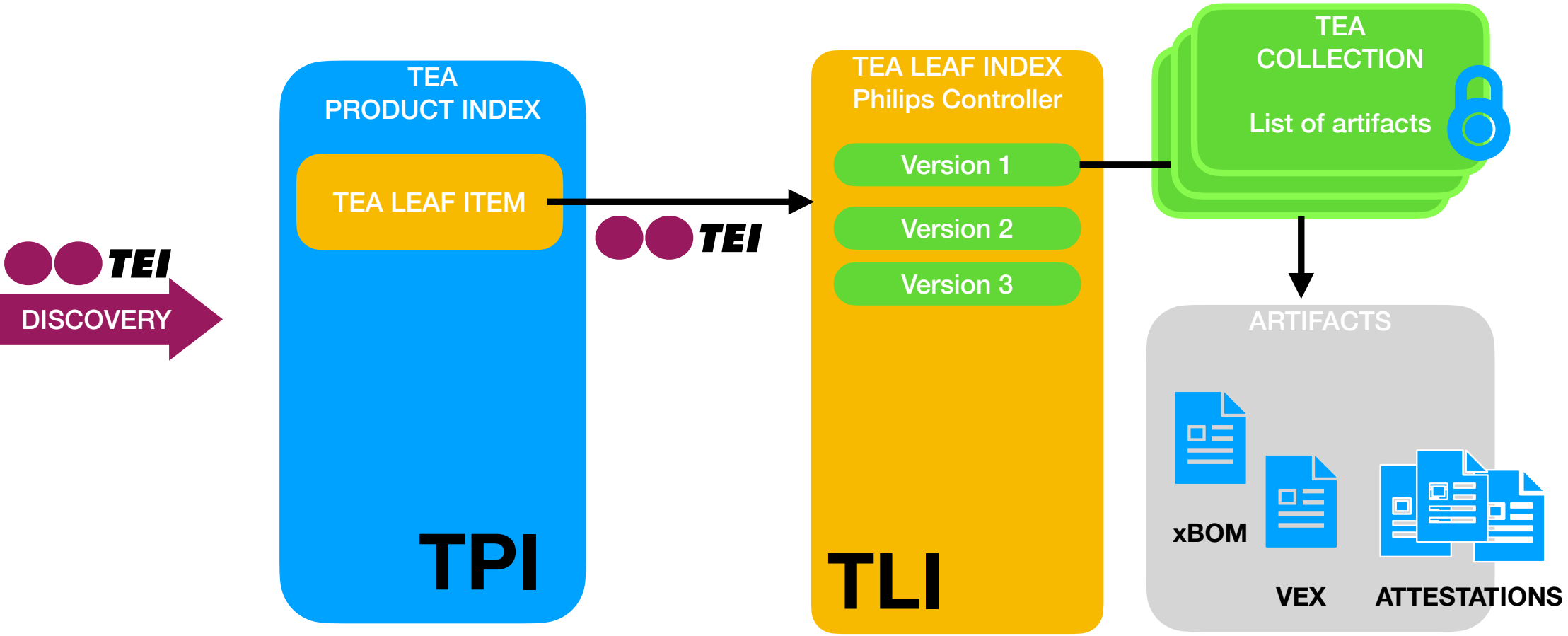
oej@edvina.net

2024-08-26

OWASP®

CycloneDX

TEA object model



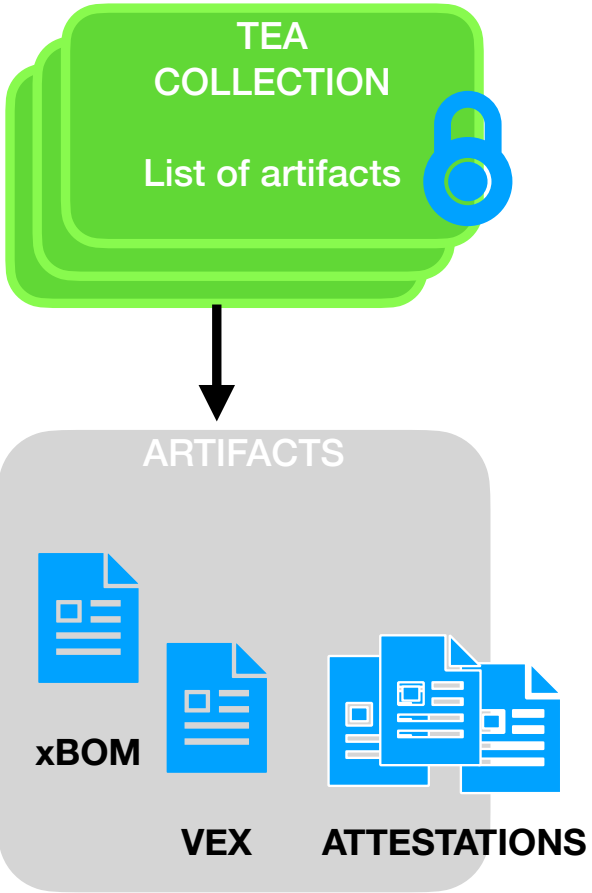
The TEA Collection

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 (changes for every update)
- Product name
- Product version
- Product Release date (timestamp)
- 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

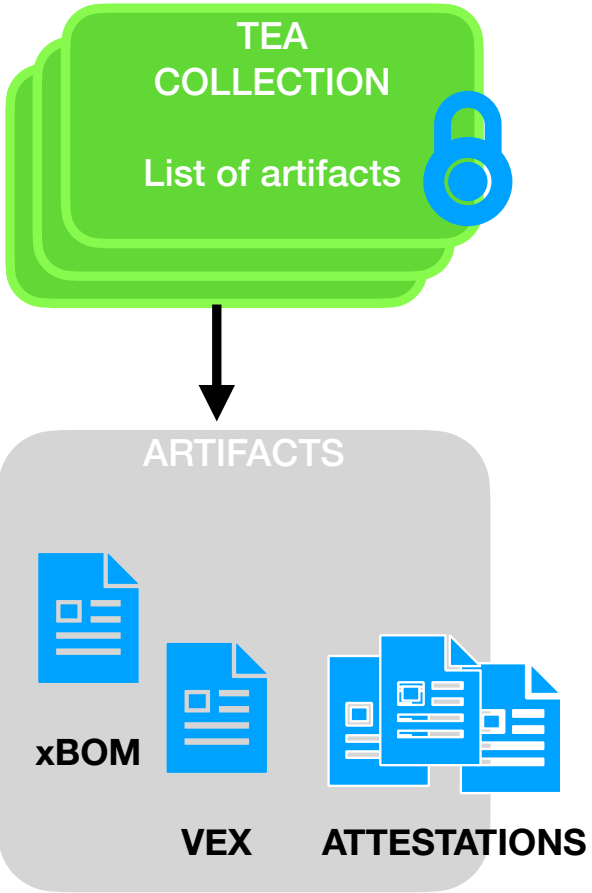


The TEA Collection artifact

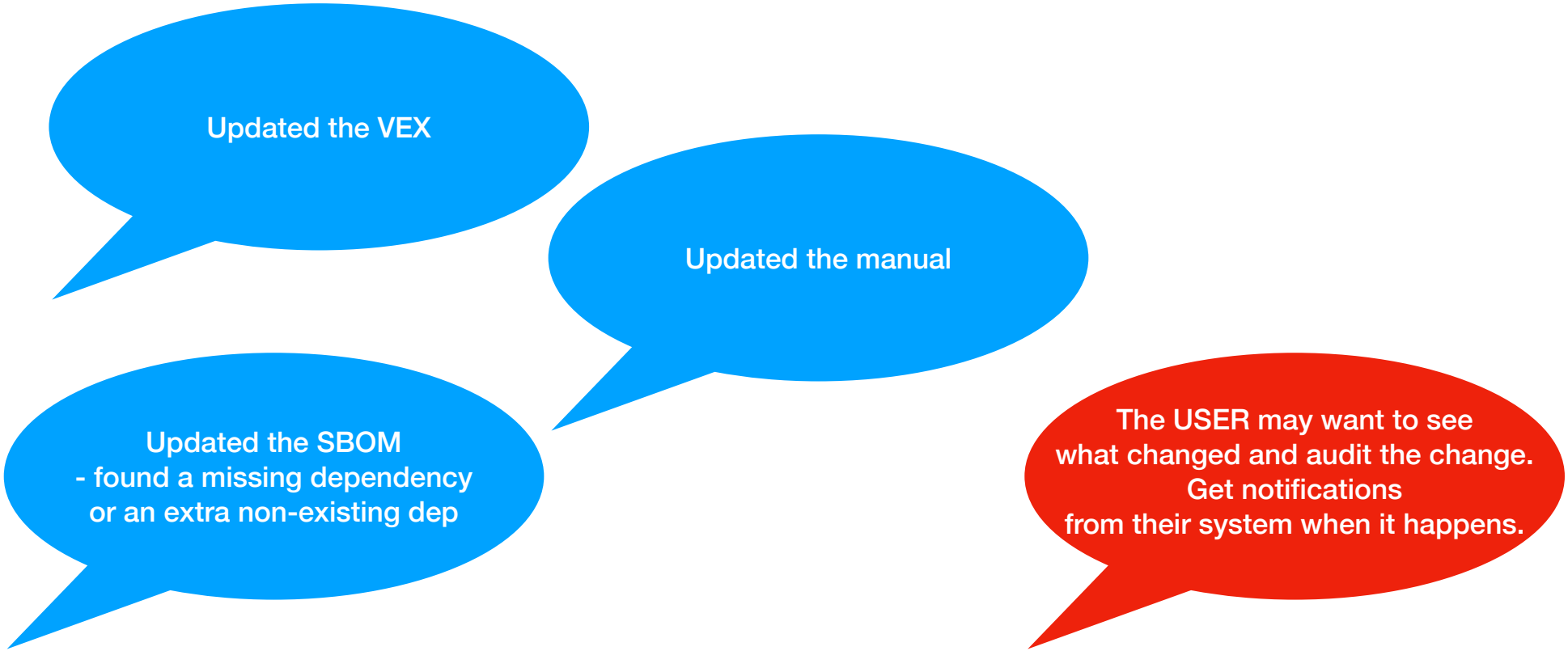
The TEA artifact is a unique piece of data

- an artifact can be published for multiple collections.

The artifact object has the following parts
- Artifact UUID
- Artifact name
- 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

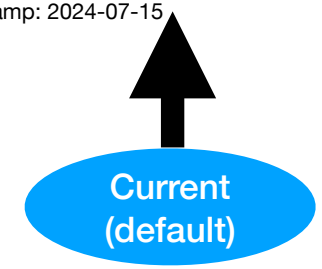


The audit trail

UUID: a3058dfa-637a-11ef-aa63-1a52914d44b3
Version: 1
Timestamp: 2024-02-04

UUID: 0039d6ca-637b-11ef-847f-c323ce57878d
Version: 2
Timestamp: 2024-03-13

UUID: 0039e994-637b-11ef-8480-279465849cc5
Version: 3
Timestamp: 2024-07-15



The optional signature (with timestamp) provides integrity as well as identity.

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

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.
Find all the links on our github page!

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

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

OWASP

OWASP®

Project Koala

CycloneDX