Ecma TC54 Brief

Software and System Transparency

OWASP FOUNDATION

®

Agenda

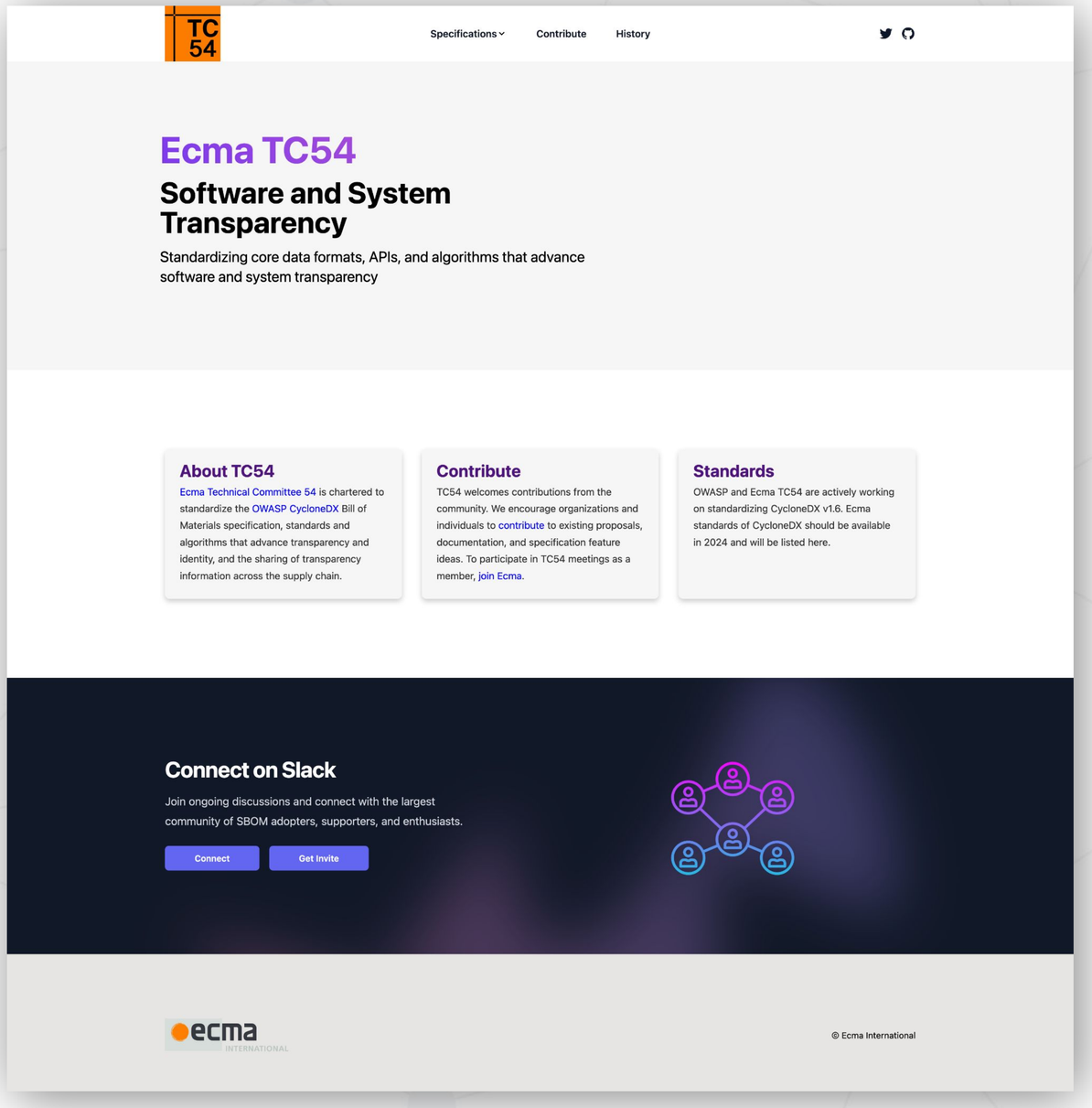
- Introduce Ecma Technical Committee 54
- Review CycloneDX Working Groups and TC54 Working Model
- Overview of TC54 scope and deliverables
- Path to standardization
- CycloneDX updates and CBOM overview
- Transparency Exchange API (aka Project Koala)
- Package URL updates

Ecma TC54 Overview

Programme of work:

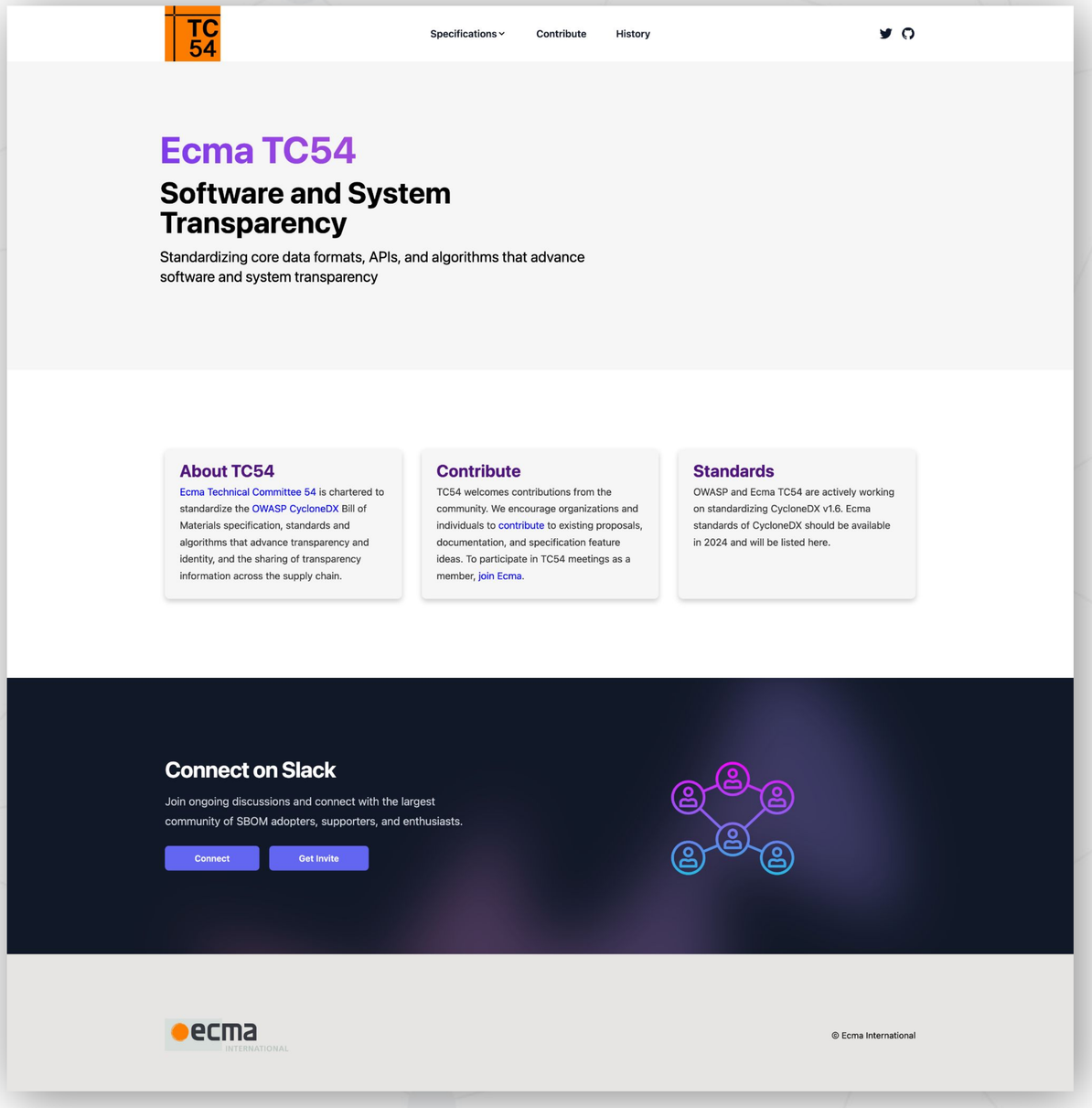
- To develop a standard for the CycloneDX software transparency and Bill of Materials specification.
- To develop a standard for the Transparency Exchange API (Project Koala) for discovering and sharing of software transparency information.
- To develop a standard and guidance for multiple BOM merging algorithms.
- To investigate the further direction of standards in the software transparency space.
- To evaluate and consider proposals for complementary or additional technology.

https://tc54.org/



Ecma TC54 Overview

TC54 uses a [Royalty-Free Patent Policy]



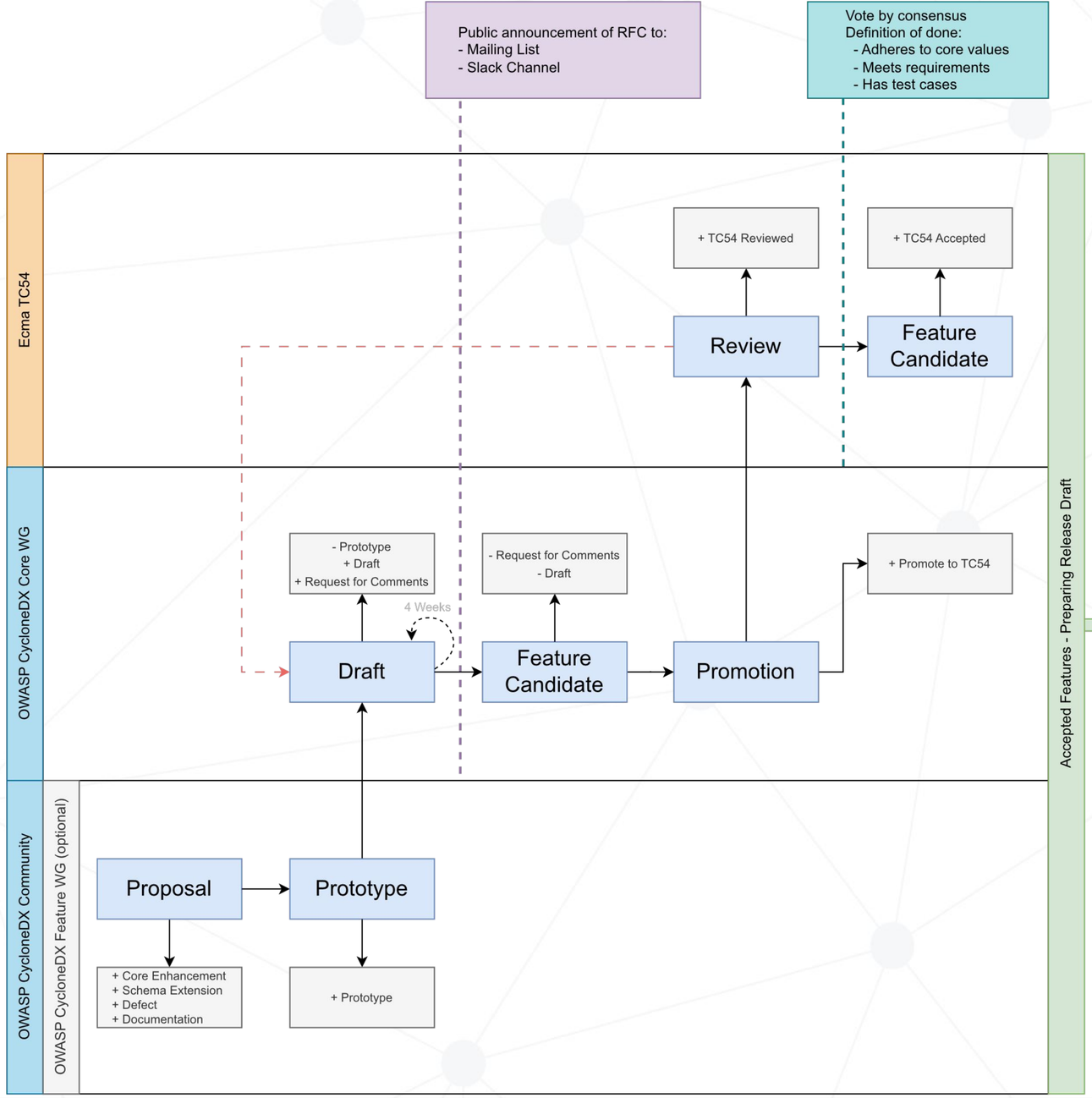
https://ecma-international.org/policies/by-ipr/royalty-free-patent-policy-extension-option/

CycloneDX Working Groups

	WORKGROUP	DESCRIPTION
ECMA	**Ecma TC54**	Technical committee of Ecma International responsible for final technical reviews of CycloneDX features and specification versions. Ecma members are encouraged to participate in the work of OWASP and vice versa.
OWASP	**Core (CWG)**	The Core Working Group are OWASP members that are responsible for the entirety of the CycloneDX project, including the specification, all tools and libraries, onboarding and offboarding maintainers, and community outreach. The Core Working Group ensures that CycloneDX maintains project continuity. OWASP classifies these individuals as “Leaders” and are documented at https://owasp.org/cyclonedx.
	Industry (IWG)	This is an invite only working group of vendors that use the specification in some way, typically through implementation in one or more products. The IWG is similar to an “on-site customer” in the extreme programming methodology. They provide insight into real-world usage, challenges, and opportunities.
	Feature (FWG)	For large features, Feature Working Groups are initiated and tasked with developing the core functionality of that specific feature. Once complete, the feature proceeds through the normal standardization process. Meetings are recorded and publicly accessible on YouTube.
	Community	OWASP projects are vendor neutral, allowing any organization or individual to contribute and have an equal seat at the table. The community may consist of OWASP members and non-members, adopters, and SBOM enthusiasts.

Working Model

- Developed jointly by OWASP and Ecma
- Provides outcomes achieved by TC39 in a repeatable working model
- Combines community collaboration with formal requirements, structure, and governance
- Facilitates rapid innovation and standards development
- Provides a blueprint for future Technical Committees
- Results in the OWASP community and TC54 being “design partners” in the advancement of supply chain standards



TC 54	Standardize core data formats, APIs, and algorithms that advance software and system transparency. TC54 standardizes OWASP CycloneDX along with proposals developed by the individual Technical Groups.	CycloneDX
TG1	Develop and maintain a standardized, format-agnostic API that enables the efficient discovery and exchange of Bills of Materials (BOMs) and other related artifacts and intelligence between systems.	Transparency Exchange API Project Koala 
TG2	Develop and maintain the Package URL specification. TG2 also standardizes the VERS specification for uniform version ranges and establishes an ongoing review process and governance for new PURL types.	Package URL PURL, VERS, PURL Types

ecma INTERNATIONAL

OWASP

TC 54	Standardize core data formats, APIs, and algorithms that advance software and system transparency. TC54 standardizes OWASP CycloneDX along with proposals developed by the individual Technical Groups.	CycloneDX
TG1	Develop and maintain a standardized, format-agnostic API that enables the efficient discovery and exchange of Bills of Materials (BOMs) and other related artifacts and intelligence between systems.	Transparency Exchange API Project Koala 
TG2	Develop and maintain the Package URL specification. TG2 also standardizes the VERS specification for uniform version ranges and establishes an ongoing review process and governance for new PURL types.	Package URL PURL, VERS, PURL Types
TGx	Future task groups are being considered	

Standardization Path

CycloneDX Updates

CycloneDX v1.6

- Released by OWASP in April 2024
- Added support for CBOM and Attestations (CDXA) to capabilities
- Will become Ecma standard in 2024
- Pursuing ISO standardization

CycloneDX v1.7

- Work underway. Three FWGs established
- Will add support for Blueprints (ABOM + BOB), TM-BOM, and OSS Sustainability
- Will become an Ecma standard (likely in 2025)
- Will pursue ISO standardization

CURRENT CAPABILITIES

SBOM
SaaSBOM
HBOM
OBOM
BOV
VDR
VEX
AI/MLBOM
MBOM
CDXA
CBOM

ecma INTERNATIONAL

OWASP

Cryptography Bill of Materials (CBOM)

An Introduction to CBOM for Post-Quantium Readiness

®

CBOM Use Cases

- Cryptography Asset Management
- Identifying Weak Cryptographic Algorithms
- Post-Quantum Cryptography (PQC) Readiness
- Assess Cryptographic Policies and Advisories
- Identify Expiring and Long-Term Cryptographic Material
- Ensure Cryptographic Certifications

Cryptography Asset Management

- Comprehensive inventory of cryptographic assets, encompassing keys, certificates, tokens, and more.
- Requirement of OMB M-23-02

> *… software or hardware implementation of one or more cryptographic algorithms that provide one or more of the following services: (1) creation and exchange of encryption keys; (2) encrypted connections; or (3) creation and validation of digital signatures.*

Identifying Weak Algorithms

- Discover weak algorithms or flawed implementations
- Helps to prioritize remediation efforts

Post-Quantum Cryptography Readiness

- Structured approach to inventorying cryptographic assets and evaluating their resilience against quantum threats
- NIST SP 1800-38B (draft) defines CBOM as a PQC requirement, mapping to NIST SSDF.

> *It is critical to begin planning for replacement of hardware, software, and services that use public-key algorithms now so that the information is protected from future attacks.*

Source: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

Assess Cryptographic Policies & Advisories

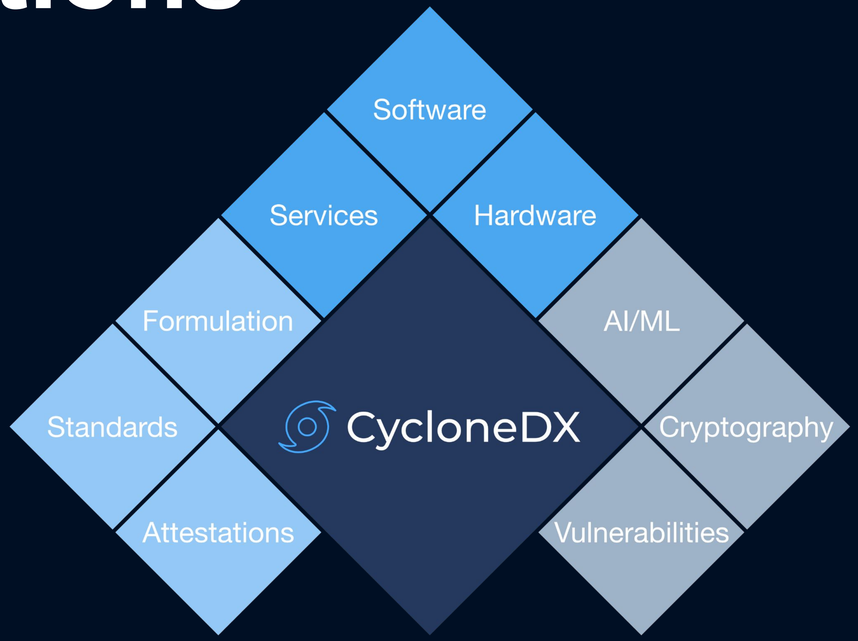
- Automate the compliance to internal or public policies and advisories, such as CNSA 2.0.

  CNSA 2.0 states that National Security Systems for firmware and software signing needs to support and prefer CNSA 2.0 algorithms by 2025 and exclusively use them by 2030.

Identify Expiring & Long-Term Crypto Material

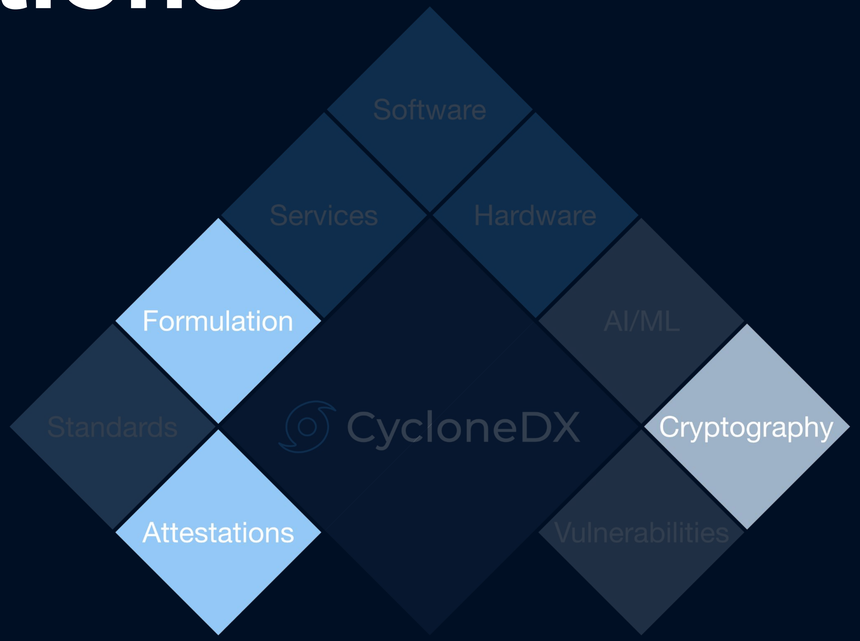
- Identify cryptographic assets, such as certificates, that expire soon
  - Reduce the likelihood of service downtime due to expired certs
- Identify cryptographic assets that have long-term validity, not expiring for several years (or decades)

Ensure Cryptographic Certifications



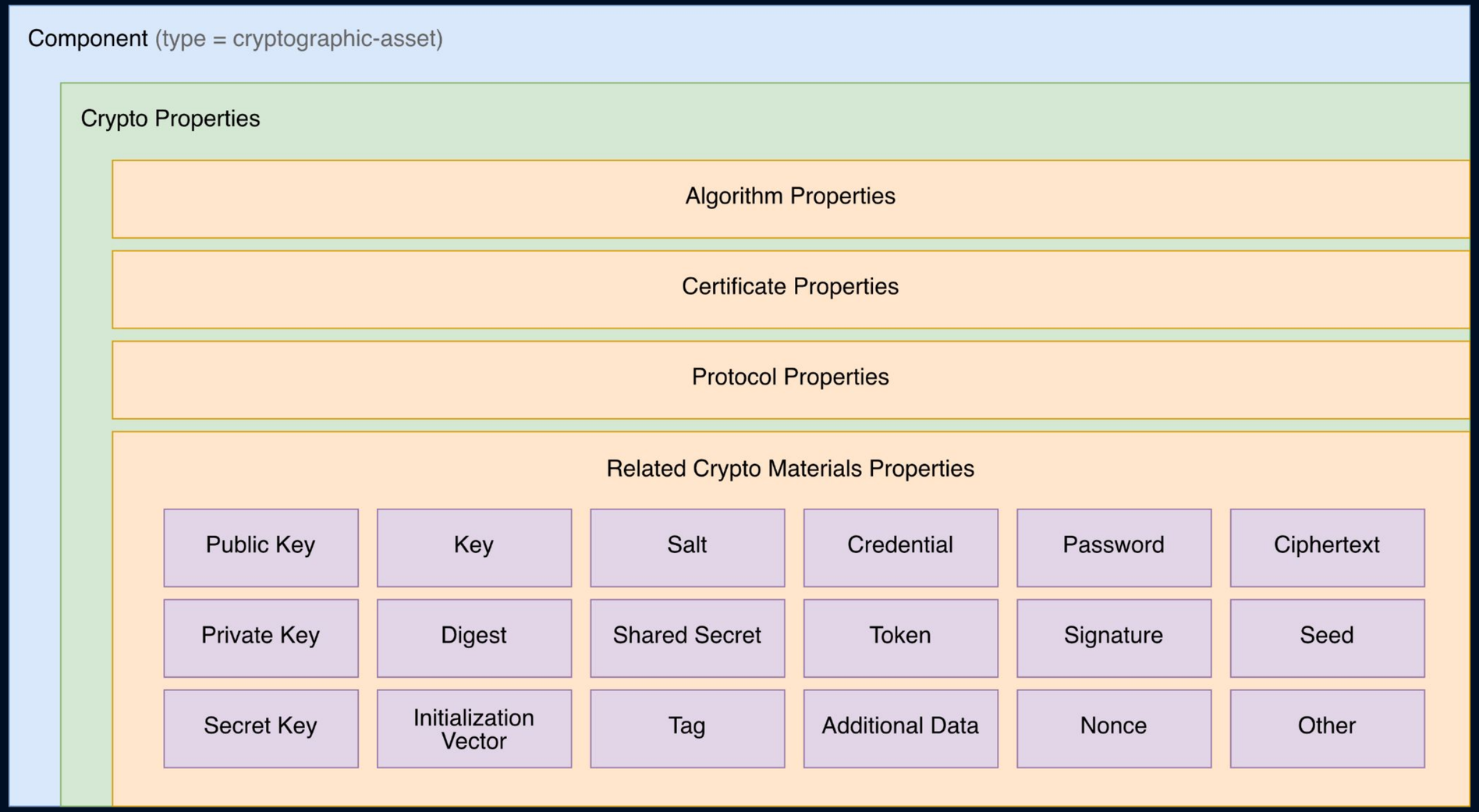
- Capture certification levels of crypto assets
- Supports:
  - FIPS 140-3 (levels 1 - 4)
  - Common Criteria EAL 1 - 7
- Optionally use CycloneDX Attestations to attest to any certification
- Optionally use CycloneDX Formulation to describe precise steps for how certification can be independently verified

Ensure Cryptographic Certifications



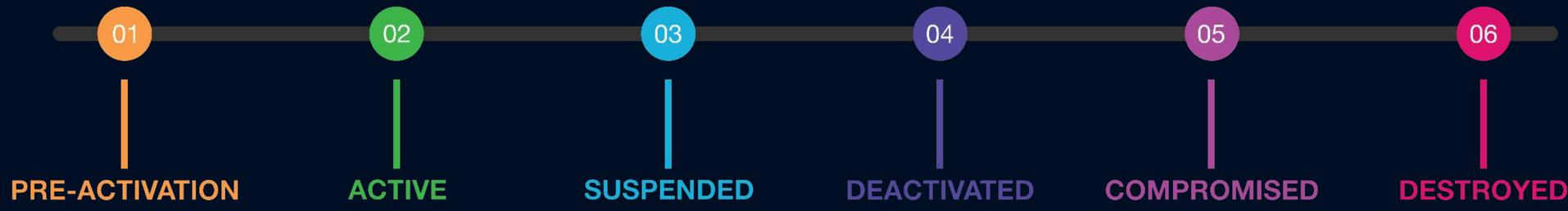
- Capture certification levels of crypto assets
- Supports:
  - FIPS 140-3 (levels 1 - 4)
  - Common Criteria EAL 1 - 7
- Optionally use CycloneDX Attestations to attest to any certification
- Optionally use CycloneDX Formulation to describe precise steps for how certification can be independently verified

Anatomy of a CBOM



Key Management Lifecycles

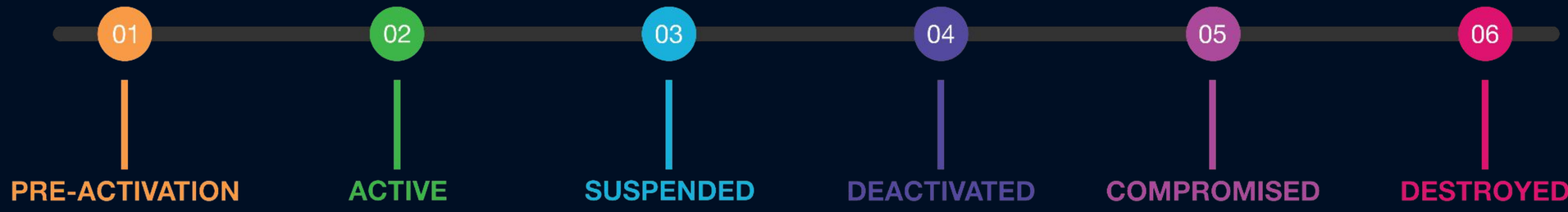
CycloneDX supports key management states defined in [NIST SP 800-57]



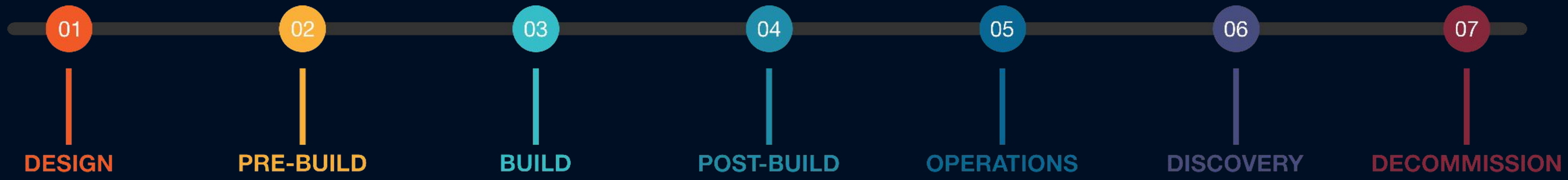
- Manage keys from inception
- Useful for anomaly detection
- Prevention of compromised keys during build or deployment

Key Management Lifecycles

CycloneDX supports key management states defined in NIST SP 800-57



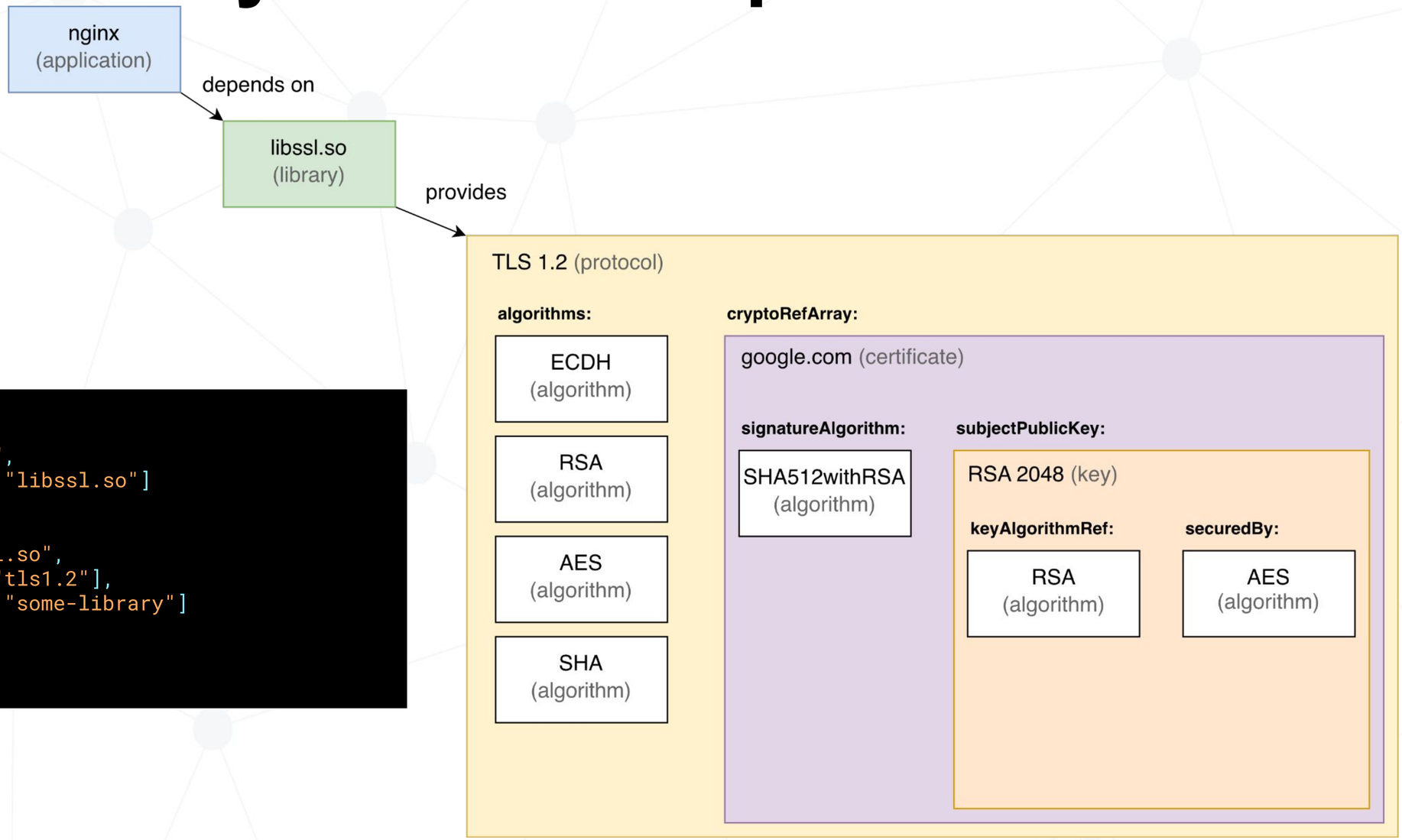
Can be combined with CycloneDX lifecycles for any asset



ecma INTERNATIONAL

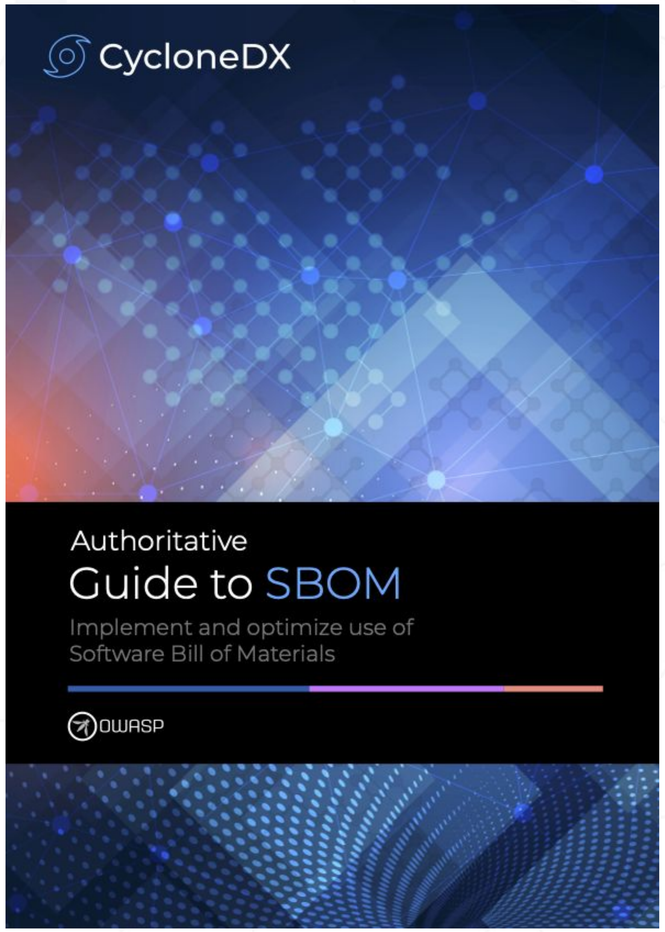
OWASP

Dependency Relationships




```
"dependencies": [
  {
    "ref": "nginx",
    "dependsOn": ["libssl.so"]
  },
  {
    "ref": "libssl.so",
    "provides": ["tls1.2"],
    "dependsOn": ["some-library"]
  }
  …
]
```

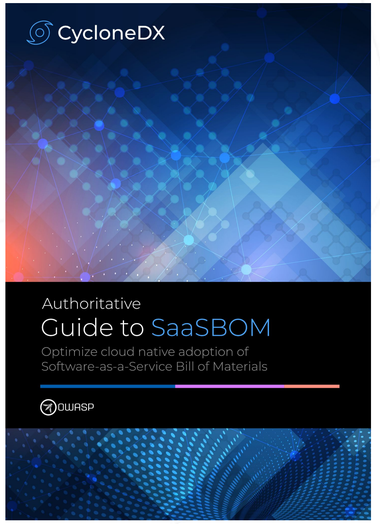
Authoritative Guides

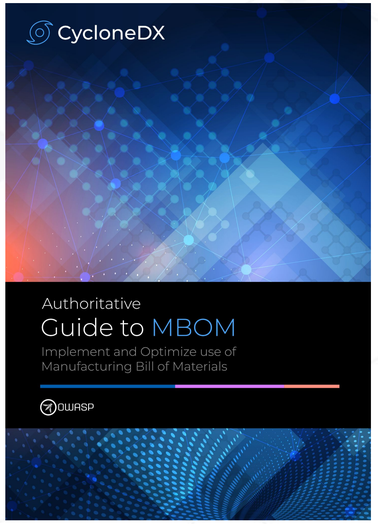


Second Edition of SBOM Guide now available

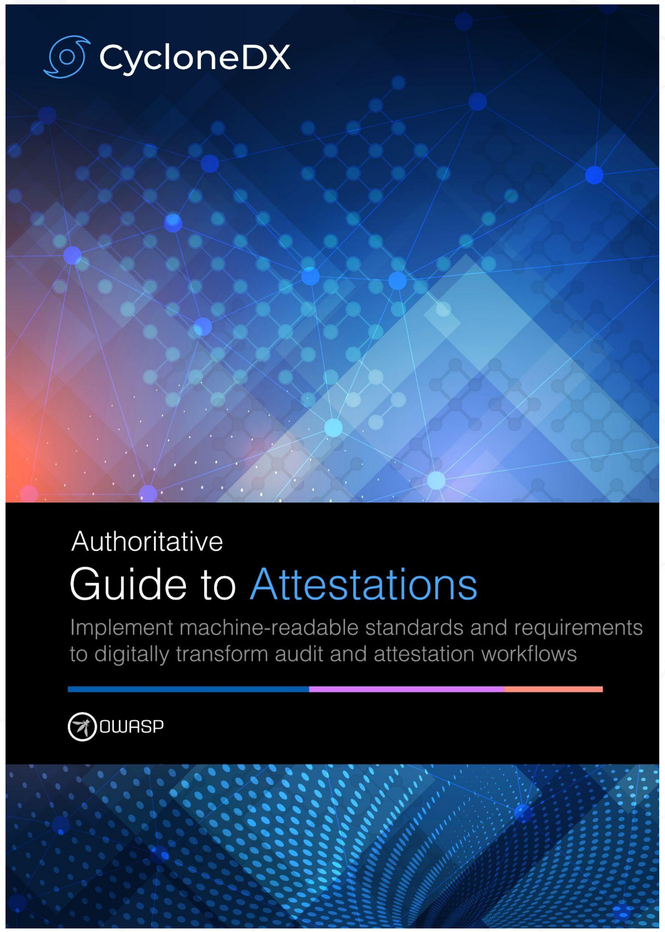
Future guides include:

https://cyclonedx.org/guides



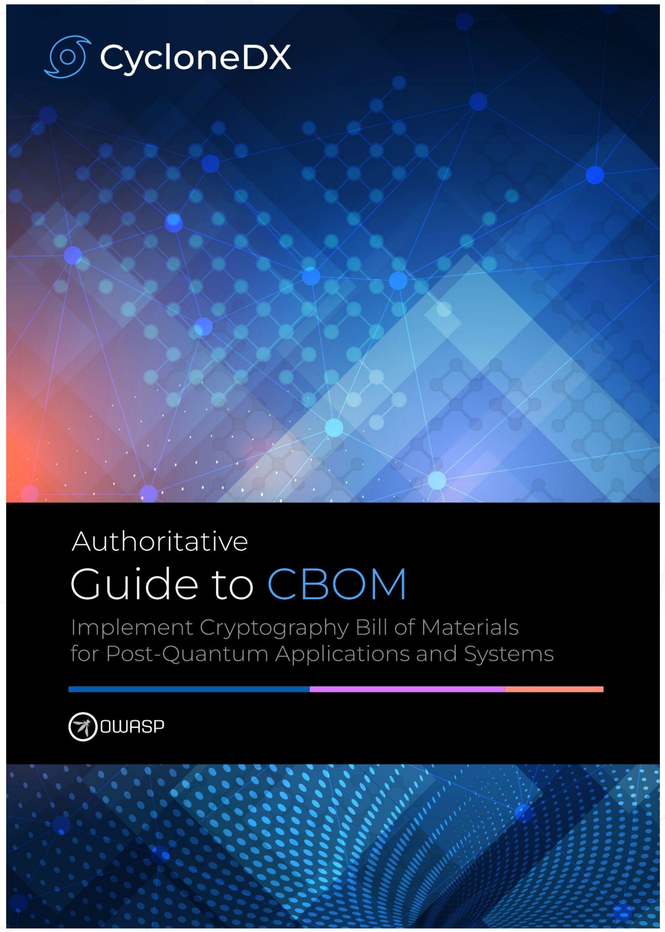


Authoritative Guides



Now Available

https://cyclonedx.org/guides

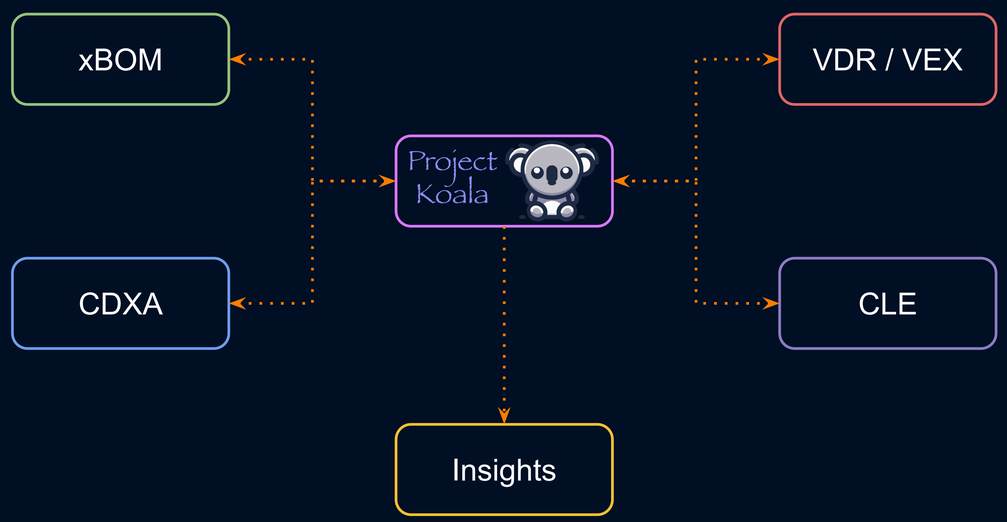


Transparency Exchange API

Discover and exchange supply chain artifacts and intelligence

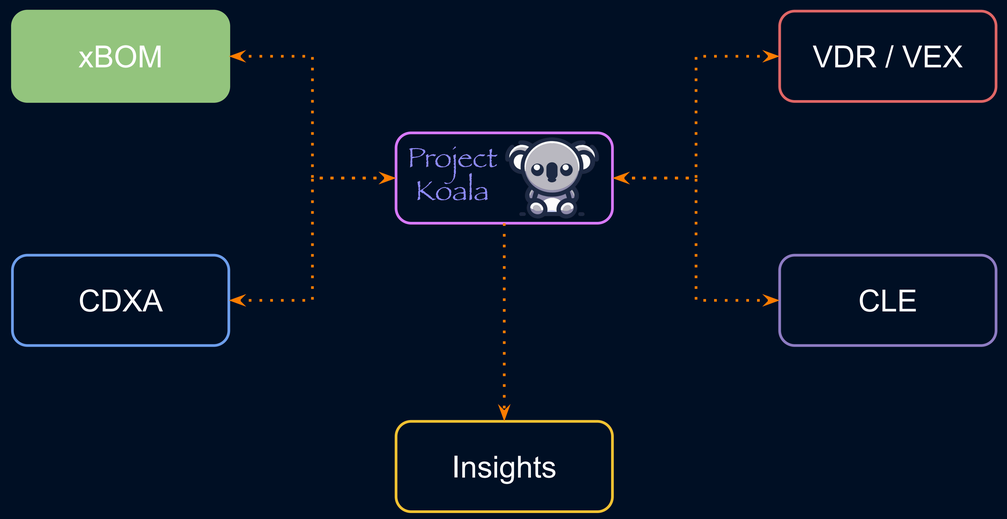
®

Transparency Exchange API (TEA)



… defines a standard, format agnostic, API for the discovery and exchange of BOMs and supporting material between systems. The core problem here is to discover a set of artifacts based on a product and version identifier for a given product. The API also provides functionality for publishing artifacts with or without signatures.

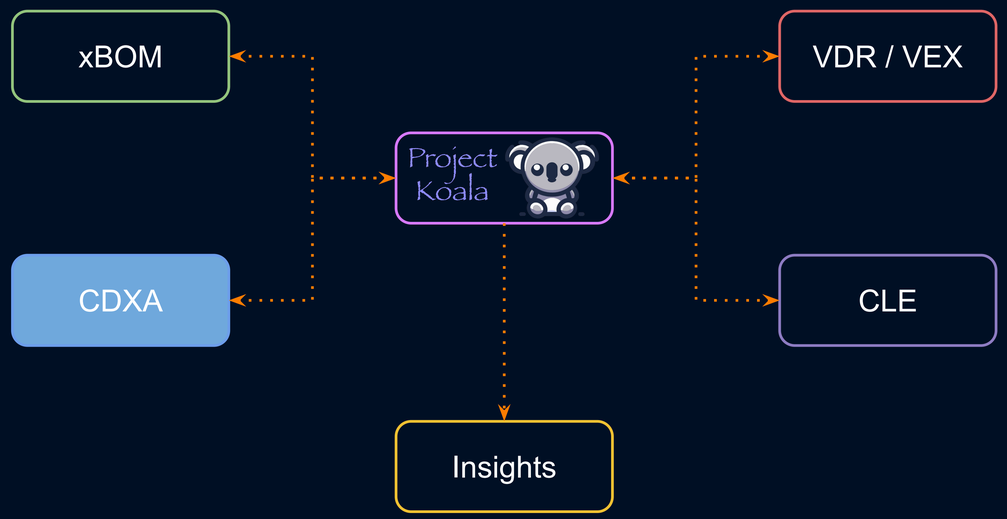
Transparency Exchange API (TEA)



xBOM

Bill of materials for any type of component and service are supported. This includes, but is not limited to, SBOM, HBOM, AI/ML-BOM, SaaSBOM, and CBOM. The API provides a BOM format agnostic way of publishing, searching, and retrieval of xBOM artifacts.

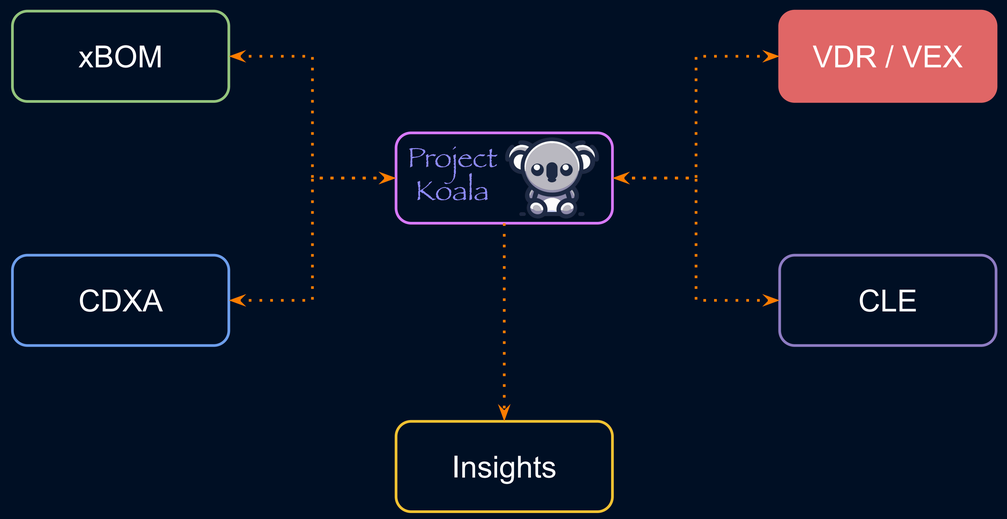
Transparency Exchange API (TEA)



CDXA

Standards and requirements along with attestations to those standards and requirements are captured and supported by CycloneDX Attestations (CDXA). Much like xBOM, these are supply chain artifacts that are captured allowing for consistent publishing, searching, and retrieval.

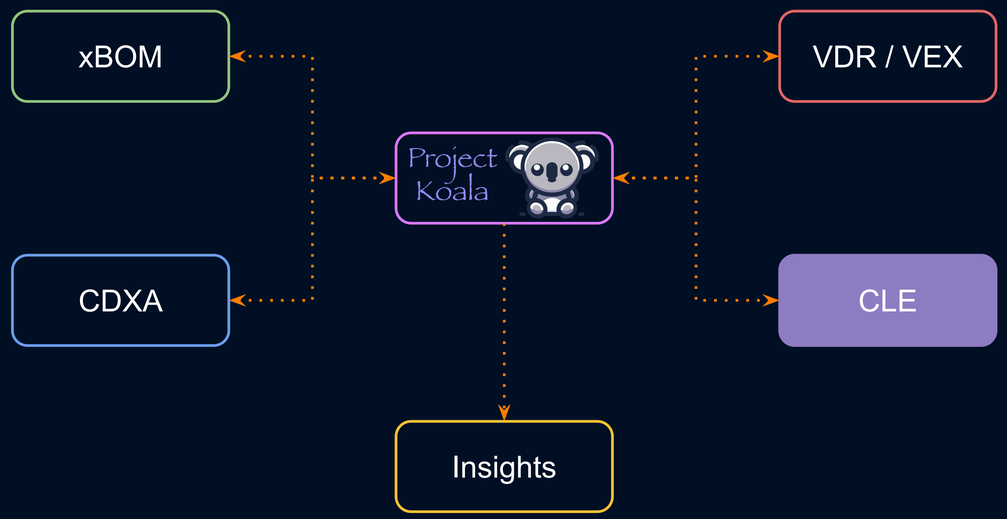
Transparency Exchange API (TEA)



VDR / VEX

Vulnerability Disclosure Reports (VDR) and Vulnerability Exploitability eXchange (VEX) are supported artifact types. Like the xBOM element, the VDR/VEX support is format agnostic. However, CSAF has its own distribution requirements that may not be compatible with APIs. Therefore, the initial focus will be on CycloneDX (VDR/VEX) and OpenVEX.

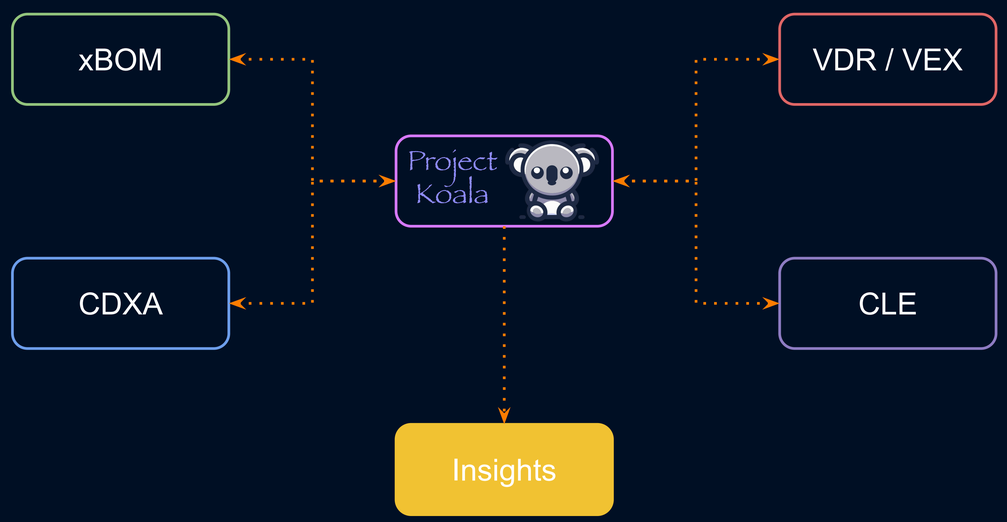
Transparency Exchange API (TEA)



CLE

Product lifecycle events that are captured and communicated through the Common Lifecycle Enumeration will be supported. This includes product rebranding, repackaging, mergers and acquisitions, and product milestone events such as end-of-life and end-of-support.

Transparency Exchange API (TEA)



Insights

Much of the focus on Software Transparency centers around the concept of “full transparency”. Consumers often need to ingest, process, and analyze SBOMs or VEXs just to be able to answer simple questions such as:

- Do any of my licensed products from Vendor A use Apache Struts?
- Are any of my licensed products from Vendor A vulnerable to log4shell and is there any action I need to take?

Insights allows for “limited transparency” that can be asked and answered using an expression language that can be tightly scoped or outcome-driven. Insights also removes the complexities of BOM format conversion away from the consumers.

Package URL

Unified approach to identify and locate software packages

Package URL

- TC54-TG2 will convene in June or July
- Led by Philippe Ombredanne
- Will standardize PURL
- Will complete and standardize VERS
- Will establish an ongoing review process and governance for new PURL types

Participation

- Participation in the OWASP community open to everyone
- Participation in Ecma TC54 or any of the TGs requires:
  - Ecma membership
    - https://ecma-international.org/about-ecma/join-ecma/
  - Invited expert
  - Observer

Resources

- Ecma International TC54
  - https://ecma-international.org/technical-committees/tc54/
  - https://ecma-international.org/task-groups/tc54-tg1/
  - https://ecma-international.org/task-groups/tc54-tg2/
- TC54 Website
  - https://tc54.org/
  - Includes participation and Slack information

Q&A


OWASP
TM