SEPIA> SBOM Exchange Procedures, Interfaces and Architecture

Hans Malte Kern, Robert Bosch GmbH
Head of Bosch Center of Competence Open Source
2024-09-12

BOSCH

SEPIA – SBOM Exchange Procedures, Interfaces and Architecture
Problem 1: SBOM Formats

- OpenChain V2.0/ISO 5230 §3.1 – “A process exists for creating and managing a bill of materials that includes each Open Source component (and its Identified Licenses) from which the Supplied Software is comprised.”
  - No further definition or other requirements…
  - So “dead SBOMs” are totally valid

- 2 competing machine-processable Standards:
  - SPDX
  - CycloneDX

  - OpenChain Telco SBOM Guide Version 1.0 released April 2024 aiming to outline certain requirements
    - SPDX 2.3 + ISO/IEC 5962 (SPDX 2.2.1)
    - Defines a set of REQUIRED elements of SPDX

Draper Laboratory; restored by Adam Cuerden InfoFieldSee file page for creator info. (https://commons.wikimedia.org/wiki/File:Margaret_Hamilton_-_restoration.jpg), „Margaret Hamilton - restoration“, als gemeinfrei gekennzeichnet, Details auf Wikimedia Commons: https://commons.wikimedia.org/wiki/Template:PD-US

re/texlive/texmf-dist/fonts/type1/urw/times/utmri8a.pfb>
Output written on sbom.pdf (58544 pages, 98893885 bytes).
Transcript written on sbom.log.

SEPIA – SBOM Exchange Procedures, Interfaces and Architecture
Problem 2: External Requirements

- Customers have their own SBOM formats
  - B2B
    - Custom XLS, Word with embedded XLS
    - Upload tool that digests different formats with different outcome
    - SPDX 1.x, 2.1, CycloneDX 1.4, ...
    - ...
  - B2C
    - Published/Printed SBOM according to OSS License and target market requirements

- Authorities
  - Cyber Resilience Act – Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements
  - BIS and NSA for export controls with Open Source
  - BSI TR-3183 (Technische Richtlinie TR-03183: Cyber-Resilienz-Anforderungen an Hersteller und Produkte)
  - ...

SEPIA – SBOM Exchange Procedures, Interfaces and Architecture

Problem 3: “Standardized” SBOMs

- Apples and Bananas
  - Main focus of SPDX is license compliance
  - Main focus of CycloneDX is security and vulnerability tracking
- Problem 3.1: Too many versions with changes that are not backward compatible
  - Both formats started to also cover other focuses in their latest development
- Problem 3.2: Mapping
  - Both have unique attributes (mainly amplifying their main focus)
  - Both have common attributes with common content
  - But some common attributes are not so common There is no automatic conversion that can be used without gambling with compliance!
- Problem 3.3: SW Architecture
  - It is difficult and time-consuming to build a SBOM that reflects the SW Architecture and Dependencies
  - This information is often lost/altered when converting, merging, modifying it
- Problem 3.4: Merging SBOMs
  - How to deal with duplicated entries is a science for itself. There is no automatic conversion that can be used without gambling with compliance!

SEPIA – SBOM Exchange Procedures, Interfaces and Architecture

Our Approach: SBOM-Validation and Conversion

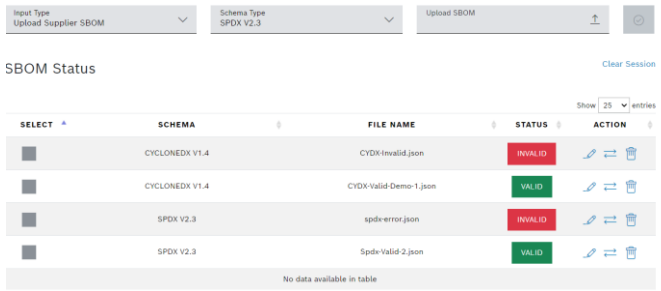
- The existing schemas were not sufficient <all assert> and allows ambiguities;
  - Syntax Checks: possible
  - Semantic Checks: impossible

1. We mapped SPDX and CycloneDX attributes to be able to define a clear semantic
2. We defined a semantic schema that reflects our requirements on a machine processable SBOM
3. We utilized existing validators to validate SBOMs against our schema
4. We implemented yet another converter that is facilitating the schema for better results

- Benefits
  - Ensure machine processable SBOM exchange with semantic relevance
  - Providing validator to suppliers would ensure SBOM quality
  - Purchase could use validator for first check of deliveries to us

SEPIA – SBOM Exchange Procedures, Interfaces and Architecture

SBOM Validator Screenshots



Edit

SBOM File Name: spdx-error.json

Schema: SPDX V2.3

```
licenseConcluded : NOASSERTION
licenseInfoFromFiles [1]
name : bcpkix-jdk15on
originator : NOASSERTION
supplier : NOASSERTION
versionInfo : 1.62
primaryPackagePurpose :
licenseDeclared : value
externalRefs [1]
0 {4}
comment : value
referenceCategory :
referenceLocator : value
referenceType : value
2 {15}
3 {14}
4 {13}
```

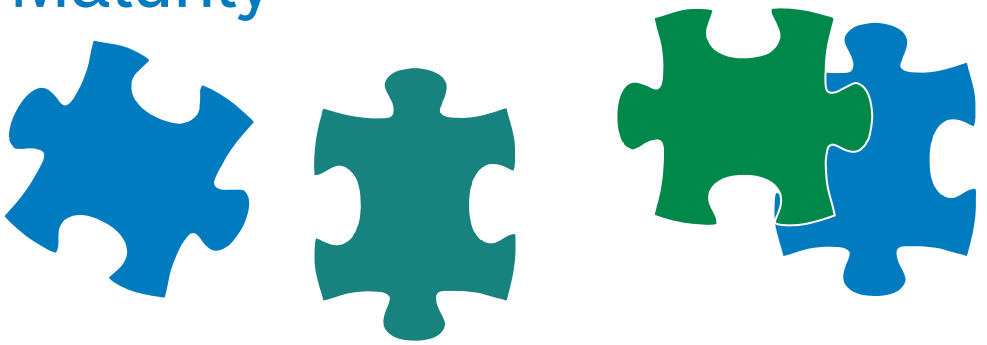
```
object {6}
$id+ : http://spdx.org/rdf/terms/2.3
title : SPDX Software Bill of Materials Standard
type : object
properties {16}
SPDXID {2}
annotations {3}
comment {1}
creationInfo {5}
dataLicense {3}
externalDocumentRefs {3}
hasExtractedLicensingInfos {3}
name {2}
revieweds {4}
spdxVersion {3}
documentNamespace {3}
documentDescribes {5}
```


BOSCH

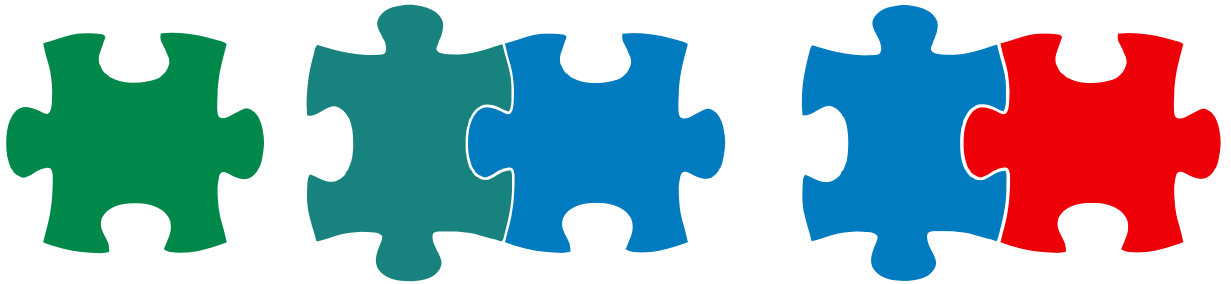
SEPIA – SBOM Exchange Procedures, Interfaces and Architecture

Supply Chain SBOM Maturity

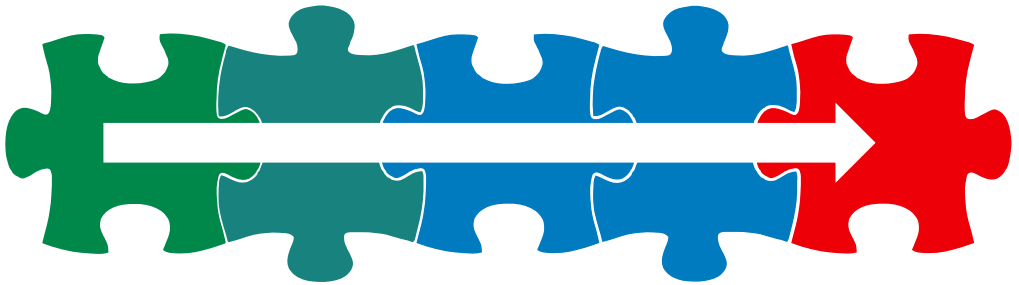
- Before OpenChain



- With OpenChain



- With OpenChain + SEPIA



BOSCH

SEPIA – SBOM Exchange Procedures, Interfaces and Architecture

Our Approach: Make it Open Source

- We started an Open Source project
  - We will provide our evaluation and mapping of SPDX and CycloneDX with semantic definition of important properties
  - We will provide our SBOM tooling and will continue its development in the Open
  - We will provide our semantic schema (currently SPDX only)
  - We will curate an Open SBOM Schema Library that can be used for automation
- We encourage you to participate in this activity
  - Providing your semantic schema to build an Open SBOM Schema Library
  - Share your insights and experience to build an SBOM ecosystem that allows an automatic processing of SBOMs independent of the tool used to generate and the format used.

https://github.com/OpenChain-Project/SBOM-sg-SEPIA

- We will use our experience and assets in the OpenChain activities to define a “common SBOM” – maybe in OpenChain’s SBOM Study Group

BOSCH

see you here: https://github.com/OpenChain-Project/SBOM-sg-SEPIA

Thank you!

Hans Malte Kern
Head of Bosch Center of Competence Open Source

BOSCH