SBOM and SPDXv3 Update

November 2023

Alexios Zavras



Generate SBOMS when the data is known



Managing set of relevant items with SBOMs

Q	Design SBOM	Functional Safety Management (Plans) and Safety Concept
	Source SBOM	Requirements, Design, Safety Analysis, Source Code, Test Cases
	Build SBOM	Build Framework, Build configuration and environment data, Test Framework, Executable, Test Reports
6	Deploy SBOM	Deployed configuration and environment data, Hardware architecture specific information and data, deployment tests and reports
	Runtime SBOM	Runtime relevant data (configuration data), training data, error logging data



The road to SPDX 3.0



StandardizedComplianceSingleUse Cases:PackageAdditionalInformation:Project andMachine andLicensehuman readableInformationformatsState

PackageSecuritRelationships:cases:30+ additionalExternaluse casesreferendsupported forvulneralcomplexand propackaging andidentifieddistributionscenarios

Security use ISO Standard cases: External references for vulnerabilities and product identification

Format Interoperability

Profiles: Support several new areas of use cases without increasing the complexity (e.g. Build, Defects, AI, Data)



Why SPDX 3.0?

- Interest in SPDX for additional scenarios and use cases
 - Supporting security and safety critical application compliance requirements
 - AI/ML and datasets increasing need for transparency
 - Software Build provenance
- Simplify
 - Profiles
 - Remove confusing names
 - Reorganize and enable general SBOM use cases with minimum overhead
- Flexibility
 - Designed for online access
 - Can communicate a single element
 - Support optional inclusion properties for specific profiles
 - Enhanced relationship structure



SPDX 3.0 Specification Infrastructure

• Specification is being transformed into markdown describing

- Classes, Properties, Enumerations
- Metadata (type and cardinality) and description for each element
- Automatically generate schema from this version (for JSON, RDF, XML, etc.) as well as web and print editions
- Profiles can add their own Classes and Properties and may also restrict other profiles (e.g. values, cardinalities, etc)
- See <u>https://github.com/spdx/spdx-3-model</u>



External Document Reference Changes

SPDX 2.3



SPDX 3.0





SPDX Profiles



Introducing SPDX Profiles

Profile Conformance

Is the SPDX creator asserting the data is there for my use case?

Profile Name Space

Where's the spec I'm interested in?

Profile Workgroup

How can I contribute?

















Core Profile Overview



• Defines foundational concepts which are the basis for all SPDX 3.0 profiles





Software Profile Overview

SPDX



- Defines concepts related to software artifacts
- Introduces and supports CISA SBOM Types
 - Design/Source/Build/Deployed/Runtime/Analyzed



https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf

Licensing Profile Overview



• Split into two separate profiles with different ways to represent license expressions:

- SimpleLicensing: via SPDX License Expression syntax strings
- ExpandedLicensing: via object model corresponding to each license component
- License model
 - includes those previously defined in SPDX 2.3, as well as SPDX License List fields
 - represents Licenses, License Exceptions, and the data model for license combinations (AND, OR, WITH, +)
 - now with License Additions (custom text for right side of WITH expressions)
- Relationships for Licensing-related metadata
 - conceptually similar to SPDX 2.3
 - o now structured as SPDX Relationships rather than properties
 - enables one SPDX data creator to define the software artifacts, and others to later specify their conclusions as to licenses by reference to the same artifacts



Security Profile Overview



Captures security-related metadata specific to a piece of software

- Security profile v3.0 properties and relationships support vulnerability management.
 - discovery & disclosure: Communicate the vulnerabilities found by person (auditor/researcher), tool, or organization in a particular piece of software, e.g. CVE
 - severity: Communicate severity and rank vulnerabilities in a specific piece of software using industry standardized methods, e.g. CVSS
 - risk: Communicate how a vulnerability affects a specific piece of software, e.g., EPSS, VEX
 - remediation: Communicate how a vulnerability may be addressed or has already been addressed for a particular piece of software
- Security assurances for software integrity and other secure SDL activities are also supported in SPDX 3.0



AI & Data Profile Overview

A profile that adds on top of the Core and Software profiles to describe AI-specific elements that will enable transparency and traceability of both components and processes.

A profile that adds on top of the Core and Software profiles to describe the datasets that are used to train or test an AI software. Similar to AI profile, it captures both components and processes – also provenance and lineage.







Profiles Beyond SPDX 3.0

More to come...

• Software as a Service

- Profile team has been active for about 3 months
- Tracking the CISA workgroup
- Safety
 - We're realizing that we already have in 3.0 most of what we need

• Hardware

- Safety Standards expect to know "system" that software is running on
- Potential participants include RISC-V & ARM core adopters, Chips Alliance Members and Board Manufacturers



Participate!

- Teams
 - Technical
 - Legal
 - Outreach
- Profile groups
- Mailing lists
- Meetings
- GitHub



Thank you!

Questions?

