The System Package Data Exchange (SPDX) specification defines an open standard for communicating bill of material (BOM) information for different topic areas.

SPDX defines an underlying data model as well as multiple serialization formats to encode that data model.

SPDX metadata includes details about creation and distribution, including the following:

• software composition, for collections of software (Packages), individual Files, and portions of files (Snippets)
• software build information
• artificial intelligence (AI) models
• datasets
• creator, supplier and distributor identity information
• provenance and integrity
• licenses and copyrights, including a curated list of licenses and exceptions
• security vulnerabilities, defects, and other quality data
• relationships between system elements
• software usage and lifecycle
• mechanisms to enable annotating SPDX elements and linking between multiple SPDX Documents

System Package Data Exchange (SPDX), v3.0 – beta 1

1   Scope

This Software Package Data Exchange® (SPDX®) specification defines a standard data format for communicating the component and metadata information associated with software packages. An SPDX document can be associated with a set of software packages, files or snippets and contains information about the software in the SPDX format described in this specification.

1.1   General

Companies and organizations (collectively "Organizations") are widely using and reusing open source and other software packages. Accurate identification of software is key for many supply chain processes. Vulnerability remediation starts with knowing the details of which version of software is in use on a system. Compliance with the associated licenses requires a set of analysis activities and due diligence that each Organization performs independently, which may include a manual and/or automated scan of software and identification of associated licenses followed by manual verification. Software development teams across the globe use the same open source packages, but little infrastructure exists to facilitate collaboration on the analysis or share the results of these analysis activities. As a result, many groups are performing the same work leading to duplicated efforts and redundant information. With this document, the SPDX workgroup, a combined effort of the Linux Foundation SPDX group and the OMG/CISQ Tool to Tool effort, has created a data exchange format so that information about software packages and related content may be collected and shared in a common format with the goal of saving time and improving data accuracy.

The merged activities of the two group slid together the beginning weeks of 2021 with activities generally moving forward but occasionally stalling while the larger group worked through issues that one or the other hadn't discussed or had a different opinion about. Eventually, after releasing SPDX 2.3 in August of 2022 with updates that brought some of the concepts and capabilities slated for SPDX 3.0 to the community in preparation of the shift that SPDX 3.0 represents, the first release candidate of SPDX 3.0 was released in May of 2023. Within the SPDX community, which is both a standards creation organization as well as a community of open source developers, a release candidate offers an opportunity for implementors of SPDX, both new and old, to review the work and determine whether there were parts that were unclear or that would be extremely burdensome to implement.

Based on the comments and change requests from the initial candidate release several areas of the model were revised and reworked, resulting in a release candidate 2 of SPDX in February of 2024. This release candidate will give tool creators and those who maintain the support libraries for working with SPDX time to start revising their projects in advance of the final version of the specification. For those not following the inner workings, debates, and discussion of the combined 3T-SBOM and SPDX 3.0 working group for the last 3 years there will be a dramatic change in the SPDX model as it goes from SPDX 2.3 to SPDX 3.0, shifting the SPDX name from Software Package Data eXchange to System Package Data eXchange and the scope of items it can convey in a Bill of Materials from software to many additional aspects like data sets, AI models, security, licencing, and build informaton.