Software that conforms to the SPDX specification at the extension profile compliance point shall be able to import and export serialized documents that conform with one of the SPDX serialization formats defined SPDX serialization formats, including the abstract Extension class serving as the base for all defined extension subclasses.

Conformance to the extension profile compliance point does not entail support for the Licencing, Security, Data Set, AI,

Build, or profiles of the SPDX but is expected to be used in combination with the other profiles to extend them.

This compliance point facilitates interchange of extended information that goes beyond the standard SPDX produced by tools supporting SPDX and is used between cooperating parties that understand the form of the extension and can produce and consume its non-standard content.

2 ~~3~~ References

2 ~~3~~.1 Normative References

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Apache Maven, Apache Software Foundation, https://maven.apache.org/

Bower API, https://bower.io/docs/api/#install

Common Platform Enumeration (CPE) – Specification, The MITRE Corporation, https://cpe.mitre.org/files/cpe-specification_2.2.pdf

NISTIR 7695, Common Platform Enumeration: Naming Specification Version 2.3, NIST, https://csrc.nist.gov/publications/detail/nistir/7695/final

npm-package.json, npm Inc., https://docs.npmjs.com/files/package.json

NuGet documentation, Microsoft, https://docs.microsoft.com/en-us/nuget/

POSIX.1-2017 The Open Group Base Specifications Issue 7, 2018 edition, IEEE/Open Group, https://pubs.opengroup.org/onlinepubs/9699919799/

purl (package URL), https://github.com/package-url/purl-spec

Resource Description Framework (RDF), 2014-02-25, W3C, http://www.w3.org/standards/techs/rdf

RFC-1321, The MD5 Message-Digest Algorithm, The Internet Society Network Working Group, https://tools.ietf.org/html/rfc1321

RFC-3174, US Secure Hash Algorithm 1 (SHA1), The Internet Society Network Working Group, https://tools.ietf.org/html/rfc3174

RFC-3986, Uniform Resource Identifier (URI): Generic Syntax, The Internet Society Network Working Group, https://tools.ietf.org/html/rfc3986

RFC-5234, Augmented BNF for Syntax Specifications: ABNF, The Internet Society Network Working Group, https://tools.ietf.org/html/rfc5234

RFC-6234, US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF), The Internet Society Network Working Group, https://tools.ietf.org/html/rfc6234

SoftWare Heritage persistent IDentifiers (SWHIDs), https://docs.softwareheritage.org/devel/swh-model/persistent-identifiers.html

SPDX and RDF Ontology, http://spdx.org/rdf/ontology/spdx-2-3

SPDX License list, Linux Foundation, https://spdx.org/licenses/

SPDX License Exceptions list, Linux Foundation, https://spdx.org/licenses/exceptions-index.html

2 ~~3~~.2 Non-normative References

Software Package Data Exchange (SPDX®) Specification Version 1.0 and 1.1, 1.2, 2.0, 2.1, and 2.2; SPDX.dev, https://spdx.dev/specifications

Open Source Initiative (OSI); https://opensource.org/licenses

Bring references at end up here

4 Terms and Definitions

For the purposes of this specification, the following terms and definitions apply.

4.1 annotations information section

section (4.9) type, an instance of which contains comments about an SPDX document, SPDX file, SPDX package, or SPDX snippet

4.2 field

a piece of information contained in a section (4.9)

4.3 file information section

section (4.9) type, an instance of which contains facts specific to files

4.4 other licensing information detected section

section (4.9) type, an instance of which contains a way to capture information about and refer to licenses that are not on the SPDX license List

4.5 package

any unit of content that can be associated with a distribution of software

4.6 package information section

section (4.9) type, an instance of which contains facts that are common properties of a package

4.7 relationships between SPDX elements information section

section (4.9) type, an instance of which contains information on how documents, packages (3.5), files and snippets relate

Annex C: References

(Informative)

[1] NTIA, “Notice of 07/19/18 Meeting of Multistakeholder Process on Promoting Software Component Transparency”, July 2018. https://www.ntia.gov/federal-register-notice/notice-071918-meeting-multistakeholder-process-promoting-software-component

[2] Dan Geer and Joshua Corman, “Almost Too Big to Fail”, Usenix ;login article, Vol. 39. No. 4, August 2014, https://www.usenix.org/system/files/login/articles/15_geer_0.pdf

2

[3] Josh Corman, testimony at the Cybersecurity of the Internet of Things Hearing Before the Subcommittee on
Information Technology of The Committee on Oversight and Government Reform House of Representatives One
Hundred Fifteenth Congress First Session calling for software bill of materials in pending legislation, October 3, 2017,
2 page 38, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.govinfo.gov/content/pkg/CHRG-115hhrg27760/pdf/CHRG-115hhrg27760.pdf

[4] CISQ Software Bill of Materials project, “Tool-to-Tool Software Bill of Materials Exchange”, https://www.it-cisq.org/software-bill-of-materials/

[5] MITRE, “Standardizing SBOM within the SW Development Tooling Ecosystem”, Nov 2019, https://www.mitre.org/sites/default/files/2021-10/pr-19-01876-16-standardizing-sbom-within-the-sw-development-tooling-ecosystem.pdf

[6] NTIA Software Bill Of Materials web page, https://ntia.gov/sbom/

[7] MITRE, “Deliver Uncompromised: Securing Critical Software Supply Chains Proposal to Establish an End-To-End Framework For Software Supply Chain Integrity”, Jan 2021, https://www.mitre.org/sites/default/files/2021-11/prs-21-0278-deliver-uncompromised-securing-critical-software-supply-chain.pdf

[8] White House, “Executive Order on Improving the Nation’s Cybersecurity”, May 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[9] The United States Department of Commerce, “The Minimum Elements For a Software Bill of Materials (SBOM) Pursuant to Executive Order 14028 on Improving the Nation’s Cybersecurity”, Jul 2021, https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf