OpenChain Telco SBOM Guide:

A Guide From The OpenChain Project

Version 1.0

Table of Contents

1. Scope

This document "OpenChain Telco SBOM Guide" aims to outline certain requirements related to how an entity creates, delivers, and consumes Software Bill of Materials (SBOM), so that entities that produce and/or consume SBOMs that conform to this guide can ensure repeatability and streamlining of tools and processes for generating and consuming SBOMs. **Please Note** that this guide does not require a conforming entity to adopt OpenChain (in any version) but doing so is greatly encouraged.

This guide is designed to work on a per SBOM level: an entity can use it as its sole way of delivering SBOMs but it is the individual SBOM that the guide refers to, not the entity that provides the SBOM. An SBOM using this guide can be called "OpenChain Telco SBOM Guide Compatible."

Releasing SBOMs that match the requirements outlined in this guide does not preclude an entity from also delivering SBOMs for the same software in alternate ways or formats.

2. Terms and definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 RFC2119 (https://www.ietf.org/rfc/rfc2119.txt) and RFC8174 (https://www.ietf.org/rfc/rfc8174.txt) when, and only when, they appear in all capitals, as shown here.

Data Format

Data Format means the data format of the information in the SBOM. Possible Data Formats include SPDX, Cyclone DX, SWID, or other proprietary formats.

Entity

Entity shall mean the legal entity (for profit, non profit, or natural person) that distributes software to third parties (e.g., other organizations or individuals). Entity does not include other group companies, or companies under common control of the Entity.

SBOM

A Software Bill of Materials (SBOM) is a formal record containing the details and supply chain relationships of various components used in building software.

SBOM Type

An SBOM can be of one of the following types:

- Design,
- Source,
- Build,
- Analyzed,
- Deployed,
- Runtime.

The definition of these types can be found in the CISA document (https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf).

SPDX

SPDX (Software Package Data Exchange) is ISO/IEC 5962:2021 (https://www.iso.org/standard/81870.html) for exchanging SBOM for a given software package, including associated license and copyright information. The standard was created by the Linux Foundation's SPDX Project (https://spdx.dev/).

OpenChain

OpenChain means OpenChain ISO/IEC 5230:2020 (https://www.iso.org/standard/81039.html), the international standard that specifies the key requirements of a quality open source license compliance program in order to provide a benchmark that builds trust between organizations exchanging software solutions that incorporate open source software. The OpenChain standard is produced by the OpenChain Project (https://www.openchainproject.org) of the Linux Foundation.

Transitive dependencies

Transitive dependencies are all components that are necessary for the software to run. They include any dependency of the package that is not a direct dependency.

Package URL (PURL)

Package URL (PURL) is a *de facto* standard to uniquely identify software packages.

3. Requirements

3.1 Data Format

An OpenChain Telco SBOM Guide compatible document SHALL adhere to the version 2.2 of the SPDX Data Format as standardized in ISO/IEC 5962:2021, or to the version 2.3 of the standard, and as further described below with respect to the included elements.

3.1.1 Verification and reference material

- ISO/IEC 5962:2021 Information technology – SPDX® Specification V2.2.1
- SPDX Specification V2.3: https://spdx.github.io/spdx-spec/v2.3/

3.1.2 Rationale

To ensure simplified handling and streamlining of tooling and competences in the telecommunications supply chain, both for suppliers and consumers of software, OpenChain Telco SBOM Guide Compatible documents shall adhere to the SPDX Data Format as standardized in ISO/IEC 5962:2021. By harmonizing on the use of this standard SBOM Data Format in an organization's external interfaces, the complexities for organizations supplying and consuming software are simplified, as only one set of unified requirements will be applicable.

As clarification, an entity is free to use alternative Data Formats for internal use, or deliver SBOMs in alternative Data Formats to organizations that so request or on its own initiative. The OpenChain Telco SBOM Guide is a SBOM-level specification to adhere to, and not an organizational specification to adhere to. There are no conforming entities, only conforming SBOMs, delivered by entities that have implemented the OpenChain Telco SBOM Guide.

3.2 SPDX Elements to be included in an OpenChain Telco SBOM Guide Compatible document

The following elements are REQUIRED.

Document creation information

- SPDXVersion: mandatory in SPDX
- DataLicense: mandatory in SPDX
- SPDXID: mandatory in SPDX
- DocumentName: mandatory in SPDX
- DocumentNamespace: mandatory in SPDX
- Creator: mandatory in SPDX
- Created: mandatory in SPDX
- CreatorComment: to be able to put "SBOM Build information"

Package information

- PackageName: mandatory in SPDX
- SPDXID: mandatory in SPDX
- PackageVersion: needed by "NTIA SBOM Minimum elements"
- PackageSupplier: needed by "NTIA SBOM Minimum elements"

- PackageDownloadLocation: mandatory in SPDX
- FilesAnalyzed
- PackageChecksum: recommended by "NTIA SBOM Minimum elements"
- PackageLicenseConcluded: mandatory in SPDX
- PackageLicenseDeclared: mandatory in SPDX
- PackageCopyrightText: mandatory in SPDX
- ExternalRef: to be able to put the Package URL

A package SHOULD be identified by a Package URL (PURL).

The PURL SHOULD be put in ExternalRef field, e.g.

```
ExternalRef: PACKAGE-MANAGER purl pkg:pypi/django@1.11.1
```

Relationships between SPDX elements

- Relationship: at least DESCRIBES and CONTAINS, needed by "NTIA SBOM Minimum elements"

3.2.1 Verification and reference material

NTIA minimum elements

3.2.2 Rationale

Recognizing the Telco industry need for harmonization and special requirements, possibly beyond the NTIA minimum elements, the "OpenChain Telco SBOM Guide" is proposed to ensure predictability to the industry as to the elements of an SBOM that is expected.

"Component Hash" is recommended, but not required by the "NTIA SBOM Minimum elements". In SPDX, it maps to PackageChecksum. We make it mandatory as it is important to uniquely identify a package. Most SCA tools have the capability to produce hashes.

Package URL (PURL) is a *de facto* standard to uniquely identify software packages.

3.3 Machine Readable Data Format

An OpenChain Telco SBOM Compatible document SHALL include, at a minimum, SPDX in one of the following machine readable formats: Tag:Value or JSON.

3.3.1 Verification and reference material

Tag:Value and JSON formats are described here:

- in SPDX 2.2: https://spdx.github.io/spdx-spec/v2.2.2/conformance/#44-standard-data-format-requirements
- in SPDX 2.3: https://spdx.github.io/spdx-spec/v2.3/

conformance/#44-standard-data-format-requirements

3.3.2 Rationale

There are 3 majors formats for SBOMs: SPDX, CycloneDX, and SWID.

These 3 formats are the ones recommended by NTIA document "The Minimum Elements For a Software Bill of Materials (SBOM)" (see References section).

The reasons for selecting SPDX as data format of the OpenChain Telco SBOM Guide include the following:

- SPDX is an ISO standard,
- SPDX has more features than CycloneDX for license compliance,
- SPDX has a human-readable format (CycloneDX has only JSON and XML),
- SWID is more a software identifier than a fully fledged SBOM format.

To facilitate a simplified toolchain, a machine readable version of the SBOM needs to be included. To ensure repeatability and harmonization a conformant SBOM must be in Tag:Value or JSON format. An entity can release additional machine readable formats but they are not required to conform to the Guide.

Tag:Value is the most human-readable format, and there are converters between the various SPDX formats (e.g. https://tools.spdx.org/app/convert/). JSON is a format produced by several tools.

3.4 Human Readable Data Format

An OpenChain Telco SBOM Compatible document SHALL include, at a minimum, the SPDX in one of the following machine readable formats: Tag:Value or JSON.

3.4.1 Verification and reference material

Tag:Value and JSON formats are described here:

- in SPDX 2.2: https://spdx.github.io/spdx-spec/v2.2.2/conformance/#44-standard-data-format-requirements
- in SPDX 2.3: https://spdx.github.io/spdx-spec/v2.3/conformance/#44-standard-data-format-requirements

3.4.2 Rationale

As the Tag:Value format is also human readable it has been chosen so that both the requirements for a standardized machine readable and human readable version can be met using one file. An entity can release additional human readable formats but they are not required to conform to the OpenChain Telco SBOM Guide.

3.5 SBOM Build information

SBOMs conforming to the OpenChain Telco SBOM Guide MUST contain information as when they were created (using the SPDX `Created` field) and to which version of the software they were created (using the SPDX `CreatorComment` field).

The `Creator` field MUST:

- contain a line with the `Organization` keyword;
- contain a line with the `Tool` keyword; in this line we MUST have after the `Tool` keyword the tool name and the tool version.

The tool name and the tool version SHOULD be separated by hyphen ("-"), no other hyphen SHOULD appear on the line.

SBOMs conforming to the OpenChain Telco SBOM Guide MUST provide their SBOM Type as defined by CISA (https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf) in the `CreatorComment` field.

3.5.1 Verification and reference material

SPDX standard

3.5.2 Rationale

It is important to know which tool and which version of the tool have created the SBOM.

The SPDX standard gives "toolidentifier-version" as an example, but it is not mandatory to have this syntax.

For example, there is a tool that outputs:

> Creator: Tool: sigs.k8s.io/bom/pkg/spdx

We have also:

> Creator: Tool: scancode-toolkit 30.1.0

and

> Creator: Tool: SCANOSS-PY: 1.5.1

where the name contains an hyphen, and the tool name and tool version are not separated by an hyphen.

So we cannot require a precise syntax.

3.6 Timing of SBOM delivery

The SBOM SHALL be delivered no later than at the time of the delivery of the software (in either binary or source form).

3.6.1 Verification and reference material

"NTIA SBOM Minimum elements", section "Distribution and Delivery"

3.6.2 Rationale

To ensure that the receiving entity can ingest the software and its SBOM, it shall be delivered no later than at the delivery of the software. An SBOM may be delivered before the software if an adopting entity so elects, but the software delivery must nevertheless be accompanied by the corresponding SBOM to ensure compliance with the Guide.

3.7 Method of SBOM delivery

The SBOM SHALL be embedded into the software "package" where technically feasible. If it is not technically feasible to embed the SBOM into the software "package" being delivered, such as in the case of space-constrained embedded systems, the supplying party will supply a web hosted version of the SBOM that is available for at least 18 months and SHALL NOT in any way restrict recipients' ability to copy and store these locally for their own use. Such restrictions MAY NOT be placed on the recipient in additional confidentiality agreements.

3.7.1 Verification and reference material

"NTIA SBOM Minimum elements", section "Distribution and Delivery"

3.7.2 Rationale

Other options of SBOM delivery such as webhosting are less stable and access is not guaranteed over time; however "embedding" may not be technically feasible. Thus, in scenarios where it is not possible on technical grounds to include the SBOM in the software delivery, publishing the SBOM online is permitted provided that the SBOM is accessible for the recipients of the software for 18 months. This duration is in line with the OpenChain specification requirements on recertification.

3.8 SBOM Scope

The SBOM SHALL contain all open source software that is delivered with the product including all of the transitive dependencies. The SBOM SHOULD contain all commercial components.

If some components are not included, they MUST be reported as "known unknowns."

3.8.1 Verification and reference material

"NTIA SBOM Minimum elements", section "Known Unknowns"

3.8.2 Rationale

It might not be possible, advisable or feasible to have the commercial component information in the SBOM. However, it is advisable that the SBOM should be as complete as possible.

3.9 SBOM in a SaaS deployment

As the OpenChain Telco SBOM Guide is only applied on the SBOM level, there is no

requirement on an entity that have elected to supply an OpenChain Telco SBOM Compatible document for some or even all of its software deliveries to also provide this for its SaaS offerings. However, an entity may elect to apply the OpenChain Telco SBOM Guide also to its SaaS offerings and thus also deliver the open source software used in the SaaS offerings with their transitive dependencies as an SBOM.

3.9.1 Verification and reference material

3.9.2 Rationale

There is currently no consensus in the industry on what an SaaS SBOM should contain.

3.10 SBOMs for containers

SBOMs for containers SHOULD include all open source components delivered in the container. This includes the packages installed into the container, components copied or downloaded to the container and dependencies used to build the compiled components in the container.

3.10.1 Verification and reference material

3.10.2 Rationale

Every open source component delivered should be part of the SBOMs.

3.11 SBOM Verification

It is RECOMMENDED to provide a digital signature of the SBOM in order to guarantee the integrity of the SBOM.

3.11.1 Verification and reference material

Sigstore https://www.sigstore.dev/ is an example of such capability.

3.11.2 Rationale

While the verification of SBOMs is an important topic, OpenChain Telco defers this work to other initiatives for the moment and intends to revisit this topic in future iterations of this document.

3.12 SBOM Merger

SBOMs following this Guide can be built from several SBOM files with a well-defined relationship to each other using the relationship definition features in SPDX.

3.12.1 Verification and reference material

There exist tools to merge several SBOMs into one, e.g. https://github.com/opensbom-generator/sbom-composer

3.12.2 Rationale

It is often easier when dealing with a large software product to provide individual SBOMs of its parts than a single SBOM.

3.13 SBOM Confidentiality

SBOMs MAY be subject to confidentiality agreements. A conformant SBOM MUST NOT, however, be subject to any confidentiality agreements that would prevent a recipient from redistributing the parts of the SBOM applicable to software that such recipient has a right to redistribute.

3.13.1 Verification and reference material

"NTIA SBOM Minimum elements", section "Access Control"

3.13.2 Rationale

Some open source software licenses enable any recipient to redistribute the software. In these situations, the recipients should be also able to redistribute the relevant parts of the SBOMs.

4. Conformant notice

To indicate that the software has a conformant SBOM available, you MAY use the following statement: "This software is supplied with an SBOM conformant to the OpenChain Telco SBOM Guide v1.0, the Guide is available at: https://github.com/OpenChain-Project/Reference-Material/tree/master/SBOM-Quality/Version-1"

You MAY at your choosing use the following statement in your Telco Guide conformant SBOM "This SBOM conforms to the OpenChain Telco SBOM Guide v1.0 (https://github.com/OpenChain-Project/Reference-Material/tree/master/SBOM-Quality/Version-1), it is provided to the recipient free of charge, and the recipient is free to redistribute this SBOM to any third party that they distribute the corresponding software to, provided that they have all the necessary right to distribute the software to such third party"

The following statement MAY be used as statement in the RFP document, order document, or contract document when requesting an RFP, purchasing orders, or outsourced development orders from a software vendor or telco system suppliers.

"When releasing software, it is REQUIRED to provide an SBOM compliant with the OpenChain Telco SBOM Guide v1.0 for all software released. This Guide is available at (https://github.com/OpenChain-Project/Reference-Material/tree/master/SBOM-Quality/Version-1)"

5. References

SPDX (ISO/IEC 5962:2021)

- https://spdx.dev/
- https://www.iso.org/standard/81870.html
- https://standards.iso.org/ittf/PubliclyAvailableStandards/c081870_ISO_IEC_5962_2021(E).zip
- SPDX Specification V2.3: https://spdx.github.io/spdx-spec/v2.3/

OpenChain (ISO/IEC 5230:2020)

- https://www.openchainproject.org/
- https://www.iso.org/standard/81039.html
- https://standards.iso.org/ittf/PubliclyAvailableStandards/c081039_ISO_IEC_5230_2020(E).zip

The Minimum Elements For a Software Bill of Materials (SBOM) a.k.a. "NTIA minimum elements"

- https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom

Package URL (PURL)

- https://github.com/package-url/purl-spec


OPENCHAIN

About OpenChain Project

The OpenChain Project is building a supply chain where open source is delivered with trusted and consistent process management information. It maintains OpenChain ISO/IEC 5230:2020, the international standard for open source license compliance, and ISO/IEC 18974:2023, the international standard for open source security assurance.

There is an extensive global community of over 1,000 companies collaborating around the OpenChain Project to make the supply chain quicker, more effective and more efficient.

https://www.openchainproject.org/

About The Linux Foundation

The Linux Foundation is dedicated to building sustainable ecosystems around open source projects to accelerate technology development and industry adoption.

Founded in 2000, The Linux Foundation provides unparalleled support for open source communities through financial and intellectual resources, infrastructure, services, events, and training. Working together, The Linux Foundation and its projects form the most ambitious and successful investment in the creation of shared technology.

https://www.linuxfoundation.org/