The OpenChain Telco SBOM Guide

Marc-Etienne Vargenau

2024-09-25

Agenda

1. The OpenChain Telco work group
2. Work result: the OpenChain Telco SBOM Guide
3. Content of the Guide
4. OpenChain Telco SBOM validator

The OpenChain Telco work group

The OpenChain Telco work group was formed in May 2021

Vision: industry alignment on SBOM

- SBOM fragmentation is bad for the industry, it will only drive cost & complexity
- SBOM format is not a competitive advantage

Goals:

- Define what a quality SBOM is for the telco industry
- Define a precise format for the SBOM
- Follow industry best practices
- Define how and when the SBOM should be distributed

OpenChain Telco work group

We work by consensus.

Everyone can join.

We have calls the first Thursday of the month (morning and afternoon CET, so all time zones can participate)

Big and small companies, some not from the telco industry.

NOKIA

TOSHIBA

KDDI

SMART TALK
BEACON
BULLETPROOF SECURITY

ERICSSON

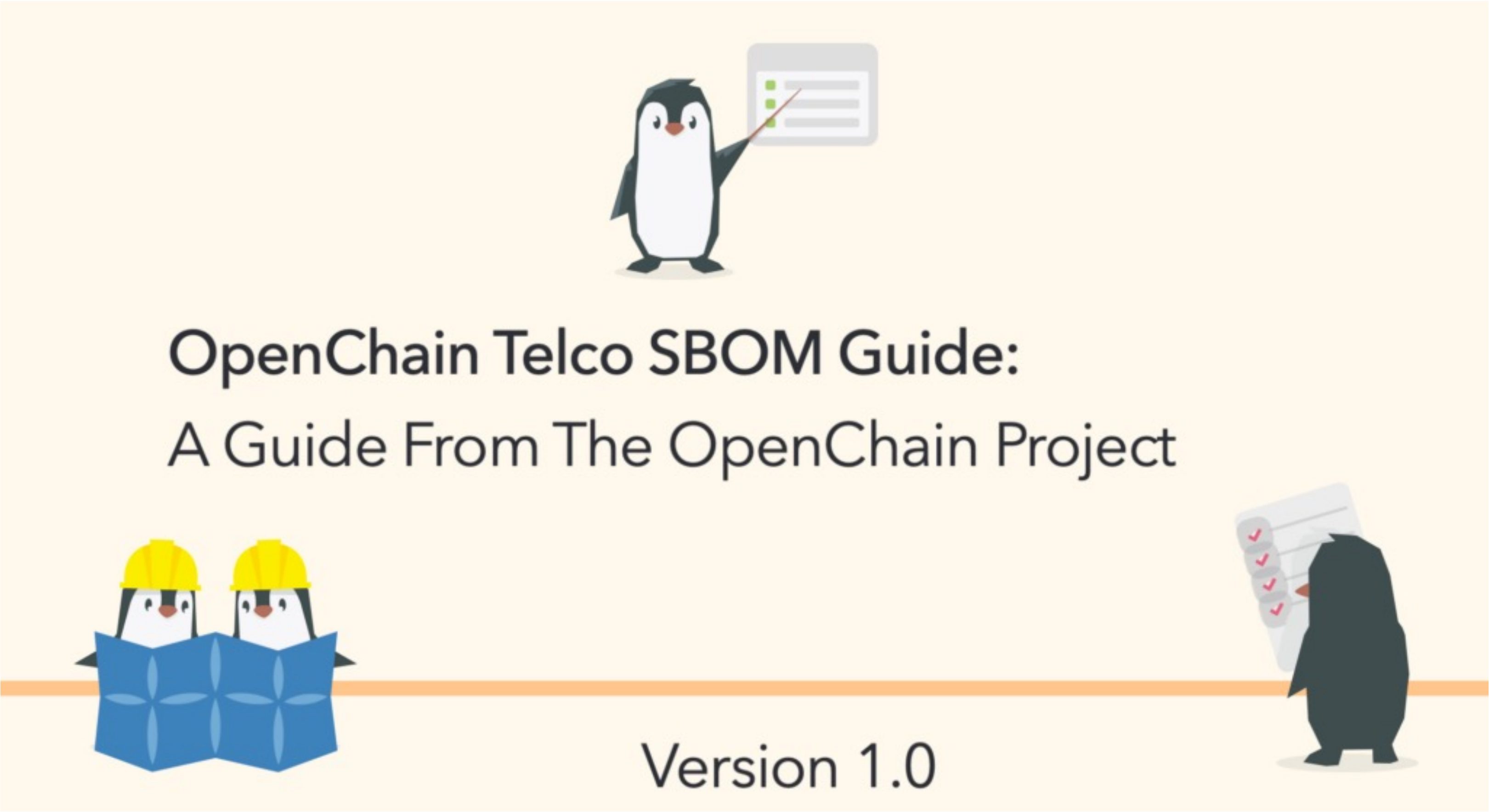
SONY

FUJITSU

BOSCH

MBITION

Work result: the OpenChain Telco SBOM Guide



OpenChain Telco SBOM Guide:

A Guide From The OpenChain Project

Version 1.0

The OpenChain Telco SBOM Guide

The Guide was approved by the work group in September 2023.
Then it was approved by the OpenChain steering committee to make it an **official OpenChain document**.

https://openchainproject.org/news/2024/07/30/openchain-telco-sbom-guide-general-availability

Translations exist in **French**, **Japanese** and **simplified Chinese**.

We did not find requirements very specific to telco, the **guide can be used by other industries**.

Content of the Guide

Result is practical and operational: precise definition of the SBOM content and format.

SBOM format is SPDX:

- Version 2.2 (ISO version) or 2.3
- JSON or tag:value (both human-readable and machine-readable)

We follow industry requirements:

- NTIA minimum elements
- CISA SBOM types (Design, Source, Build, Analyzed, Deployed)

Requirements have different levels: MUST, SHALL, SHOULD as described in BCP 14 [RFC2119] [RFC8174]

Each requirement is described and followed by a “Verification and reference material” and a “Rationale” section.

Creation 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** in the CreatorComment field.

Package information

Each package contains:

- PackageName
- PackageVersion: needed by “NTIA SBOM Minimum elements”
- PackageSupplier: needed by “NTIA SBOM Minimum elements”
- PackageDownloadLocation
- PackageChecksum: recommended by “NTIA SBOM Minimum elements”
- PackageLicenseConcluded
- PackageLicenseDeclared
- PackageCopyrightText
- ExternalRef: to be able to put the Package URL

A package SHOULD be identified by a **Package URL (PURL)**. See https://github.com/package-url/purl-spec

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.”

SBOM delivery

Timing:

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

Method of delivery:

The SBOM SHALL be embedded into the software “package” where technically feasible.

If it is not technically feasible, a web hosted version of the SBOM SHALL is available for at least 18 months.

Other recommendations

SBOM Verification

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

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.

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.

OpenChain Telco SBOM validator

Nokia has provided to the community the “**OpenChain Telco SBOM validator**.”

It is available at: https://github.com/OpenChain-Project/Telco-WG/tree/main/tools/openchain_telco_sbom_validator

- Python program
- Licensed under Apache-2.0

Contributions are warmly welcome in the form of GitHub merge requests.

Example run

```
openchain-telco-sbom-validator test-sbom-01.spdx
2024-09-24 17:58:26,202 - INFO - Input file is test-sbom-01.spdx
+---+------------------------+------------------------+---------------+-----------------------------------------------+
| # | Error type             | SPDX ID                | Package name  | Reason                                        |
+---+------------------------+------------------------+---------------+-----------------------------------------------+
| 1 | NTIA validation error  | SPDXRef-Package-deb-li | libldap-2.4-2 | Package without a package supplier or package |
|   |                        | bldap-2.4-2-           |               | originator                                    |
|   |                        | 796a192b709a2a2b       |               |                                               |
+---+------------------------+------------------------+---------------+-----------------------------------------------+
| 2 | Missing mandatory      | SPDXRef-Package-deb-li | libldap-2.4-2 | Supplier field is missing                     |
|   | field from Package     | bldap-2.4-2-           |               |                                               |
|   |                        | 796a192b709a2a2b       |               |                                               |
+---+------------------------+------------------------+---------------+-----------------------------------------------+
| 3 | Missing mandatory      | SPDXRef-Package-deb-li | libldap-2.4-2 | Checksum field is missing                     |
|   | field from Package     | bldap-2.4-2-           |               |                                               |
|   |                        | 796a192b709a2a2b       |               |                                               |
+---+------------------------+------------------------+---------------+-----------------------------------------------+
The SPDX file test-sbom-01.spdx is not compliant with the OpenChain Telco SBOM Guide
```

Example run

```
openchain-telco-sbom-validator open-chain-telco-sbom-validator-0.1.spdx
2024-09-24 18:04:01,308 - INFO - Input file is open-chain-telco-sbom-validator-0.1.spdx
The SPDX file open-chain-telco-sbom-validator-0.1.spdx is compliant with the OpenChain
Telco SBOM Guide
```

NOKIA