OpenChain Telco SBOM Guide version 1.1

Marc-Etienne Vargenau

OpenChain Telco SBOM Guide

Version 1.0 of the OpenChain Telco Guide was approved in May 2024

It has been put into practice at Nokia

The Guide is the foundation of the **Nokia SBOM schema**

Nokia internal tools produce (or will produce) SBOMs compatible with the Guide

Nokia provided a validator

https://pypi.org/project/openchain-telco-sbom-validator/

What about commercial and open source tools?

SCANOSS produces SPDX compliant with the OpenChain Telco SBOM Guide since version **v1.20.5**

https://github.com/scanoss/scanoss.py/releases/tag/v1.20.5

Yocto

Yocto generates code that is not compliant with the Guide version 1.0 because:

- It does not output **FilesAnalyzed** but uses the default value of **true**
- It does not provide **PackageChecksum** but **PackageVerificationCode** instead

The CISA document Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM), Third Edition

https://www.cisa.gov/resources-tools/resources/framing-software-component-transparency-2024

allows both, see table in section 2.5. for the hash (NTIA minimum elements).

(in some cases, the Yocto SPDX is not compliant to the guide

because it is not valid SPDX)

Differences between version 1.0 and 1.1 of the Guide 1/2

- Both PackageChecksum and PackageVerificationCode are allowed as package hash.
- The package hash is RECOMMENDED instead of MANDATORY.
- ExternalRef is RECOMMENDED instead of MANDATORY.
  - (ExternalRef is used to put the **purl** of packages)
- FilesAnalyzed is no longer MANDATORY.

Differences between version 1.0 and 1.1 of the Guide 1/2

- Examples are provided for the CISA SBOM Types.
- A RECOMMENDED syntax is given for CISA SBOM Types.
  - The SBOM Type RECOMMENDED syntax is “SBOM Type: xxx” where “xxx” is one of the 6 keywords “Design”, “Source”, “Build”, “Analyzed”, “Deployed” and “Runtime”.

    We do not require a specific format. We only require that at least one of the words “Design”, “Source”, “Build”, “Analyzed”, “Deployed”, “Runtime” is present, regardless of the case.

    So, the following possibilities are all valid, and the first one is the recommended one:

    CreatorComment: SBOM Type: Deployed

    CreatorComment: Analyzed

    CreatorComment: This SBOM was created during build phase.

- sbomasm is a better example of SBOM merge tool.
  - https://github.com/interlynk-io/sbomasm

- Add reference to new CISA document

Compatibility

An SBOM that conforms to version 1.0 of the Guide will also conform to version 1.1 of the Guide.

The reverse is not true.

Next steps

The validator will be updated for version 1.1 of the Guide.

The validator will also allow for recursive validation of SBOMs, i.e. it will validate an SBOM and all linked SBOMs.

We will continue to test the SPDX output of tools and try to convince tool vendors and developers to produce SPDX compliant with the OpenChain Telco SBOM Guide.


NOKIA