ys

OpenChain Telco Group: Telco SBOM work package DRAFT 1.0

Intro

Throughout the various Telco Group meetings and workshops as well as in email communication the idea to harmonize and standardize certain aspects around Software Bill of Materials (SBOMs) that goes beyond its data format has emerged.

The background of which is the different requirements on SBOMs that are currently emerging in the industry, and the unsustainable situation that would occur if further fragmentation happens in this area where each organization places its own requirements on SBOMs.

As SBOM format is a non-differentiating factor and not a competitive advantage for any one actor in the telco industry it would seem that all parts of the telco ecosystem and supply chain would benefit from harmonization of requirements. The Telco Work Group has thus adopted the “Telco SBOM work package” where we intend to standardize and harmonize the different variables associated with SBOMs into the “Telco Standard SBOM Package”.

Goals for the “Telco Standard SBOM”

The goal is to standardize the variables most commonly causing issues in the SBOM space that is not addressed by existing standards in the field today.

By unifying the telco industry around a set of requirements concerning SBOMs we can reduce the complexity and fragmentation of tooling, processes and negotiations needed. Lowering the transaction costs in the entire software supply chain, the end goal is for a “Telco Standard SBOM” to be “plug and play” for anyone who receives it. By unifying our requirements on SBOM we take responsibility for the ecosystem by simplifying for suppliers as they only have to produce one set of SBOM for their Telco customers, the end customer on the other hand only needs one set of tools and processes to manage the uptake of the SBOM.

Founding principles

The Telco Work Group has agreed on the following cornerstone principles for its work.

1. The Telco Group does not via the SBOM work package intend to change or modify the OpenChain specification.

2. The Telco Standard SBOM Package should be implementable independently of the OpenChain Specification.

3. The Telco Standard SBOM Package should be conformant with all relevant regulatory requirements applicable.

Meeting cadence and meeting governance:

The Telco Group meetings will occur the first Thursday of each month, The Telco Group will host 2 meetings on each such occasion the first at 09.00-10.00 CET and the second meeting at 17.00-18.00 CET to ensure that all interested parties have an equal opportunity to participate. The meetings can be found in the global OpenChain calendar, and are open to anyone who wishes to participate regardless of company affiliation, industry, or membership status in OpenChain or Linux Foundation.

The agenda of the two meetings shall to the extent possible be substantially similar to ensure that all are able to participate in all parts of the agenda. The chair will facilitate the discussion in the group and relay information between the meetings.

The Telco Group keeps open the option to at times call for ad hoc meetings outside the regularly scheduled meeting cadence, such meetings should if possible alternate between time slots so that no one geography is unduly impacted by the timing of such meetings.

The Telco Group will strive for consensus in its decision making, if consensus is not found between the two meetings and the Telco Group is unable to resolve the matter using the email list https://lists.openchainproject.org/g/telco (telco@lists.openchainproject.org). If the matter cannot be resolved over email an ad hoc meeting may be called to discuss and hopefully resolve the matter.

Work items:

In workshops and over email the following areas where standardization would be of common value to the telco industry has emerged. All of these could then possibly make their way into a “Telco Standard SBOM”.

SBOM Dataformat: The Telco work group sees a value in standardizing the SBOM dataformat (such as SPDX, Cyclone DX, SWID) to reduce the burden involved in supporting multiple formats or converting between the various formats.

Status: The group sees no additional value in creating a custom data format that would be in competition/incompatible with existing data format. The group has concluded that it seems best to adopt an existing format. Currently there seems to be broad consensus on SPDX as specified in ISO iteration ISO/IEC 5962:2021. **Further we need to investigate if we have any telco specific requirements not currently covered by SPDX.**

Machine readable SBOM & Human Readable SBOM: The Telco Group sees a value in standardizing the delivery of these artifacts so that internal processes and tools can be optimized to consume these. Areas of harmonization includes:

Mandating a Machine Readable SBOM, Do we want to mandate the requirement that such is available? Which SPDX “element” must at a minimum be included, what file format should it be delivered in (tag:value format has the benefit of being convertible as well as Human and Machine readable).

Recommended tool set for conversion: https://spdx.dev/spdx-tools/ https://spdx.dev/spdx-tools/

Human Readable SBOM: Do we want to mandate the requirement that such is available? Which SPDX “modules” must at a minimum be included, what file format should it be delivered in (For example XLSX).

Status: Broad consensus that a machine-readable version must be included, we need to further consider if we also want to mandate a human readable version, if it is optional, or if we only mandate a tooling set to be used for conversion between the formats to ensure that this is done in a consistent way. A comparison document outlining Pros and Cons of the various options to be created.

Timing of SBOM delivery: When should the SBOM be delivered?

Status: Broad consensus that the SBOM should be delivered at latest WITH(no later than with the software) the software delivery, this caters to the use case that an SBOM on a voluntary basis could be made available before a software is delivered, as an example for marketing, as part of the documentation for open source projects, or as part of a call for tenders or similar.

Method of delivery: With software. possibly + online hosting.

Verification: How do we verify that an SBOM is actually corresponding to a binary or source code deliverable?

Status: To be investigated if SPDX contains suitable support for this or if we need additional tooling.

Hash of the delivery, hash attached to the SBoM and then matching

Blockchain?

https://anchore.com/sbom/creating-sbom-attestations-using-syft-and-sigstore/

https://www.sigstore.dev/

Standard contract clauses: Drafting of example or template clauses that captures the “Telco Standard SBOM Format” requirements.

Status: Already having the “Telco Standard SBOM Format” in place will negate some of this need, however we should investigate if SME’s see a benefit in having such standard contract clauses available for use. We should also investigate if we should create case studies or playbooks to eventually help the uptake of the “Telco Standard SBOM Format”

SaaS SBOM: Should we also specify the requirements in a SaaS scenario, if we are to specify that then do they differ from the requirement in a non SaaS scenario?

Status: Not yet discussed

Coverage: All software or only 3rd party software?

Merging SBOMs: A big potential benefit of a “Telco Standard SBOM" would be to be able to easily merge it with ones own SBOM if it makes up part of a larger product. What is needed in terms of tooling/processes to enable this? (Tooling exists, but prefered method is to use the relationship (Depends on feature) feature in SPDX and keep existing SBOM and generate a new for the entirety). a tree of SBOMs.

Status: Not yet discussed.

Tools: Is there a need to standardize certain tools or only the function of the tools? If we make a tool necessary in the “Telco Standard SBOM” what should the requirements on such a tool be?

Status: Not yet discussed.