NTIA Software Component Transparency
February 20, 2019

Standards and Formats WG

JC Herz

Kent Landfield

Kate Stewart

Agenda

- Charter Review
- Summary of Survey Work to Date
- White Paper Outline
- Next Steps

Charter of the Standards and Formats WG

Will investigate existing standards and initiatives as they apply to identifying the external components and shared libraries, commercial or open source, used in the construction of software products. The group will analyze efforts underway in the community and industry related to assuring this transparency is readily available in a machine-readable manner.

Review Goals of This Group

- Investigate the options available today
- Determine how the solutions can work in harmony
- Document a workable and actionable machine-readable format(s)
- There is NOT a requirement to find a single solution/format
- Consider International aspects of proposed solutions as this is not a US problem. EU is already talking about this.

- ***There is a Win-Win for all – our job is to find it***

Survey of Ecosystem

Formats Reviewed:

- SWID - https://csrc.nist.gov/Projects/Software-Identification-SWID/lifecycle
- SPDX - https://spdx.github.io/spdx-spec/
- Package-URL (PURL) - https://github.com/package-url/purl-spec
- Software Heritage - Persistent IDs

Related Efforts:

- SParts - https://github.com/hyperledger-labs/SParts

Whitepaper Outline (WIP)

- **Background & Problem statement**
- **SWID**
  - Description
  - Strengths
  - Areas to Improve
  - Simple example
- **SPDX**
  - Description
  - Strengths
  - Areas to Improve
  - Simple example
- **Translation and Linkage Guidance**
- **How to Apply**
- **Related Format Efforts Surveyed**
  - Software Heritage Index
  - SParts
  - Package-URL (purl)
  - CPE
- **Future Research areas**

May split out into its own document

Next Steps

- Coordinate with Framing to ensure common language used
- Finish first draft of Survey Whitepaper
- Work on “How-to” document to reflect sources of tooling and support for current formats and standards
- Incorporate feedback of minimum viable SBoM fields compared to existing standards.
- Incorporate feedback from Hospital PoC
- Include areas for future research & improvement in survey

Questions?

More Info...

Co-Chairs:

- J. C. Herz (Ion Channel) jc.herz@ionchannel.io
- Kent Landfield (McAfee) kent_landfield@mcafee.com
- Kate Stewart (Linux Foundation) kstewart@linuxfoundation.org

Mailing List: ntia-sbom-formats@linuxfoundation.org

Subscribe at: https://lists.linuxfoundation.org/mailman/listinfo/ntia-sbom-formats

Shared Drive: https://drive.google.com/drive/folders/1KAQ7AWlWMKcSFnRc_S-7XB76xFRRWLmT