Organizing for SPDX v 2 and Beyond

Draft Discussion Document

May 9th 2012

Topics

- Update SPDX Vision / Mission / Scope
- Define SPDX roadmap for v2 and beyond
- Consider organization changes
  - Product management role
  - Governance

Original Mission

- Charter
  - Create a set of data exchange standards that enable companies and organizations to share license and component information (metadata) for software packages and related content with the aim of facilitating license and other policy compliance.
- Goal
  - Create a defined format for a file of license fact information describing a software package.
- Guiding Principle
  - Focus on capturing facts; avoid interpretations.

SPDX Solution

- A file format for license information to accompany open source packages
- A standardized short form to refer to the official version of common licenses
- Benefits
  - Allows easy exchange of license information between companies reducing burden on both suppliers and consumers
  - Avoids due diligence redundancy where the same source code package is analyzed multiple times by different recipients
  - Provides a unified method for exchanging license information

What is the problem?

- Our current Solution approach may not be sufficient to provide the desired Benefits
- Some discussions from the recent SPDX Forum indicate that:
  - Many current participants do not see how we can get to the desired Benefits without expanding the mission and scope to encompass more of the compliance cycle
  - We may need organization changes to support an expanded mission and scope, especially some form of product management

Expanded Mission

- Many SPDX members are now talking about a broader and deeper mission beyond a data exchange format specification including a broader/deeper role in:
  - Providing standards to facilitate licensing due diligence and compliance activities across the supply chain
  - Fostering the development of open source tools to support due diligence and compliance activities
  - Establishing a trusted repository of data about licenses and possibly also components

Expanded Mission [2]

Some recent topics (across teams)

- Should we have tools to support generation of attribution documentation from an SPDX file?
- Is the License List intended to be used only as a “lookup list” or
  - Should it also include additional information that could be used by license detection tools?
  - Should it also help people understand licenses?

Specification vs. Implementation

- SPDX original charter was to create a specification
- We also agreed to create basic software tools to read and write SPDX files
  - And encourage commercial vendors to do the same in their existing products
- Now many members are talking about software to implement lifecycle support for use of the specification, such as open source tools to:
  - Analyze licenses in a package and generate an SPDX file
  - Manage large volume of SPDX files – inbound and outbound

New Vision Statement?

Draft new Vision statement for website from Phil Odence:

“The vision of SPDX is to achieve license compliance with minimal cost across the supply chain. Ideally, upstream component developers begin the process by supplying SPDX flies as part of their downloads. Users of those components therefore have a starting point with the SPDX files they create for their "customers," and so on. If everything is working properly, the provenance of each piece of code is researched and documented only once during its journey through a supply chain, and that information is passed on in parallel with the code in the SPDX format.”

New Mission Statement?

Draft new Mission statement from Cisco:

"To enable any party in the software supply chain, from the original author to the final end user, to accurately communicate and understand the licensing information for any piece of copyrightable material that such party may create, alter, combine, pass on, or receive, and to make such information available in a consistent, understandable, and re-usable fashion, with the aim of facilitating license and other policy compliance."

Roadmap

- Current release schedule
  - Version 1.1– Q2 2012
  - Version 2.0– Targeted H2 2012
- Questions about v2.0
  - Collection of use cases by Technical Team is a strong grass-roots effort, but we also need an agreed strategic goal
  - How much of v2.0 is a specification update? And how much is software?
  - No cross-team agreement yet on scope or how we will decide scope

Roadmap [2]

- Define target markets (users and stakeholders) more clearly:
  - Upstream – Open source projects
  - Midstream – Packagers and small/medium products
  - Downstream - End-customers and large products
- Define features per release and how they map to target markets
- Keep at least three releases in sight:
  - Current -- v1.1
  - Next -- v2.0
  - Future – 3.0 (home for the backlog)

Product Management

- We need some product management function to define a roadmap and manage development and roll-out of new releases across teams
  - SPDX is not a “product” but a software company product management model may still apply
  - Typical software company model is for product management to be combined business and technical function

Governance

- It also seems time to revisit / redefine organization roles
  - Current website says:
    - Business Team - This team has primary responsibility for planning and coordinating the rollout of SPDX.
    - Legal Team – (role not listed)
    - Technical Team - This team has primary responsibility for drafting the specification and developing documentation, templates, samples and tools.
  - General meeting is primarily for communications, but no decision-making role
- We may need changes to improve decision-making
  - Steering committee based on a simple nomination and election process?
  - Another more formal decision-making process?

Governance [2]

- Current description of our operation
  - Runs like an open source project without centralized constitution or bylaws
- This structure may not be robust enough to support an expanded mission
  - Running like an open source project is a nice idea, but may not be best for the work that we actually do
  - Today’s structure is really a set of volunteer committees with light cross-team coordination
  - Standards organization like IETF may be a better model
  - Or something similar to other Linux Foundation workgroups like the Linux Standards Base ?

Resources

- If we expand the mission for SPDX, then we probably also need to find more resources
  - Corporate sponsors who can assign full-time staff to projects or roles
  - Reach out to IBM, Intel and others

Reference slides

- Reference Slides from spxd_slides_v2.6
  - SPDX v1.0 Background Slides
  - Working Group Slides

Current one-slide summary

- Standard:
  - A standard format for communicating the components, licenses and copyrights associated with a software package.
  - Key pillar in Linux Foundation’s Open Compliance Program
- SPDX™ Group:
  - Working group of Linux Foundation
  - Participation from over 20 organizations including software, systems and tool vendors, consultants and foundations
- Charter is to create a defined format for a file of license factual information describing a software package
- Status: V1.0 of spec released August, 2011

The SPDX™ File

Document Information	SPDX Version and Licensing
Creation Information	How and when created
Package Information	Package identification, copyright and licensing
File Information	File by file identification, copyright and licensing
Licensing Information	Text of licenses that are not in SPDX™ standard list
Review Information	Log of 3rd party reviews

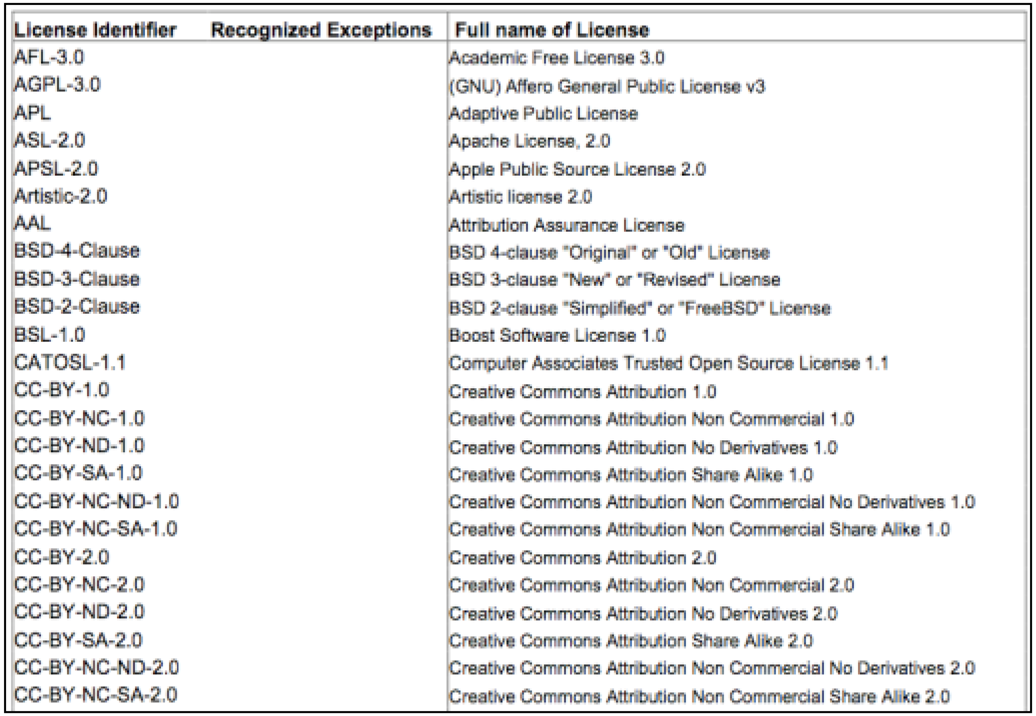
File is in RDF/XML or Tag Value form; can be converted to spreadsheet and other formats.

Tools for SPDX™

- Open Source Tools (hosted on SPDX Git Repo)
  - Viewer
  - Spreadsheet to RDF xlator
  - RDF to Spreadsheet xlator
  - License file generator (from Spreadsheet)
  - Spreadsheet template
- Commercial Tools
  - Scanning tools output SPDX™

Data for SPDX™

SPDX™ license repo



License Identifier	Recognized Exceptions	Full name of License
AFL-3.0		Academic Free License 3.0
AGPL-3.0		(GNU) Affero General Public License v3
APL		Adaptive Public License
ASL-2.0		Apache License, 2.0
APSL-2.0		Apple Public Source License 2.0
Artistic-2.0		Artistic license 2.0
AAL		Attribution Assurance License
BSD-4-Clause		BSD 4-clause "Original" or "Old" License
BSD-3-Clause		BSD 3-clause "New" or "Revised" License
BSD-2-Clause		BSD 2-clause "Simplified" or "FreeBSD" License
BSL-1.0		Boost Software License 1.0
CATOSL-1.1		Computer Associates Trusted Open Source License 1.1
CC-BY-1.0		Creative Commons Attribution 1.0
CC-BY-NC-1.0		Creative Commons Attribution Non Commercial 1.0
CC-BY-ND-1.0		Creative Commons Attribution No Derivatives 1.0
CC-BY-SA-1.0		Creative Commons Attribution Share Alike 1.0
CC-BY-NC-ND-1.0		Creative Commons Attribution Non Commercial No Derivatives 1.0
CC-BY-NC-SA-1.0		Creative Commons Attribution Non Commercial Share Alike 1.0
CC-BY-2.0		Creative Commons Attribution 2.0
CC-BY-NC-2.0		Creative Commons Attribution Non Commercial 2.0
CC-BY-ND-2.0		Creative Commons Attribution No Derivatives 2.0
CC-BY-SA-2.0		Creative Commons Attribution Share Alike 2.0
CC-BY-NC-ND-2.0		Creative Commons Attribution Non Commercial No Derivatives 2.0
CC-BY-NC-SA-2.0		Creative Commons Attribution Non Commercial Share Alike 2.0

- List of most common licenses (100+)
- Include common exceptions
- Guidelines for matching
- Standardized license names (OSI adopted)
- Exact text of licenses
- Available on SPDX™ website – URLs won't change

Working Group

- Runs like an open source project without centralized constitution or bylaws
- Intellectual property contributed by participants members is covered under the Creative Commons license (CC-BY-3.0)
- http://spdx.org

Working Group Operation

- Structure
  - General Meeting and mailing list
  - Teams with separate meetings and lists
    - Technical
    - Business
    - Legal

- Very inclusive process
  - Self-subscription for interested participants
  - Those willing to “do” can influence direction
  - Mail-list, WIKI, phone calls, BOFs…
  - Face to face meetings at Linux Foundation and other events