

FOSSBazaar – Working Group on OSS Package Data

Meeting Minutes 25-FEB-2010

Attendance

Name	Company	Active (voting)	Observer	Present 25-2-10
Barry Freedman	Alcatel-Lucent			X
Eran Strod (Co-Chair)	Black Duck Software	X		X
Dave Maxwell	Coverity			X
Kate Stewart (Co-Chair)	Freescall	X		X
Martin von Willebrand	HH Partners	X		X
Martin Michlmayr	HP			
Phil Robb	HP	X		X
Esteban Rockett	Motorola			X
Michael Herzog	nexB	X		X
Phillipe Ombredanne	nexB		X	X
Kim Weins	Open Logic			X
Shane Coughlan	Opendawn	X		X
Jeff Luszcz	Palamida			X
Debra McGlade	Qualcomm			X
Eric Thomas	TI			X
Jack Manbeck	TI			X

Conf call dial-in:

North America: 1-800-867-1147

Direct dial number is: 1-303-474-8558

For those dialing in from other regions, a list of toll free numbers can be found:

<https://g8.cfer.com/g8.jsp?an=8008671147&ac=9965310&login=true>

Passcode: 3096092

Minutes

Administrative Agenda

-Took attendance.

-Adopted the following Charter by consensus. The blue text represents modification from Michael's original proposal discussed during the call.

Charter

Create a set of data exchange standards to enable organizations to share license and component information (metadata) for software packages [and related content](#) with the aim of facilitating license and other policy compliance.

Working Group Name

-Adopted the following name by consensus:

Software Package Data Exchange (SPDX)

See follow-up action items related to the name.

-Eran reported back on action item to consult with Linux Foundation legal team about patent/copyright questions related to our working group. We decided per Martin V.W.'s suggestion to use CC-BY for the SPDX field format document and proceed using the principles of an open source project for the creation of the SPDX documentation. Discussion about whether we need a contributor agreement. We will look at registering a trademark and domain. See action items.

Technical Agenda

-Fedora's license list was agreed to be a good starting point for this discussion. Should we reference the fedora page or replicate the information on an SPDX page somewhere? Before we finalize on it though, we need to understand how they updated it. Can we suggest changes as the need arises? (Eran's note – Let's ask Tom at Fedora if he can clarify this for us.)

-Debian field specifications has some good ideas (notation for grouping files with same license together, simple text), but before we adopt, we should look at use cases. Volunteer: Kim to draft a proposal for file groupings syntax.

- XML vs. simple text specification discussed from mail list threads. Syntax for expressing fields will be revisited after use cases better understood. Group agreed on need for human and machine read/writable. Concern is extent it is "human understandable".

-Group agreed to first create use cases to help drive the needs of the SPDX data format. Volunteers: Jack M, Jeff L, David M, Michael H. They should draft use cases and we'll harmonize the format later if needed.

-Field 3.2.6 (Expected Usage) – no objections to removing this field

- Discussion to consider adding an optional "purpose" for a file, the "why" it is there. Example cited was GPL build infrastructure in non GPL projects.

-Wiki – The email list is hard to follow. It would be desirable to have a better collaboration platform. Eran to talk to Martin M. about FOSSBazaar supporting this. Michael H. to look into alternative (nexB supported?).

Action Items

- Rockett – report back in 2 weeks about possibility of working with member council
- Michael – check trademark, domain and other usage of proposed name.
- Eran – Ask LF if we they can assist us in registering the trademark SPDX and investigate reserving the domain name SPDX.org (and perhaps others). Also, is it appropriate for LF to serve as the agent to own these registrations?
- Kim – draft syntax proposal for file grouping with license and copyrights.
- Jack M, Jeff L, David M, Michael H. to post use cases for consideration.
- Eran - talk to Martin M. about FOSSBazaar supporting WIKI.
- Michael H. - look into alternative WIKI temporary support if FOSSBazaar options not available. (nexB supported?).
- Eran/Rockett – Talk about confidentiality versus transparency
- DONE - Kate –reach out to Debian to invite participation
- DONE - Eran – inquire if we can get some legal guidance from Linux Foundation on how LF typically prevents patent issues in standards

SPDX Background Information

Introduction

Companies and organizations are widely using and reusing open source [and other](#) software packages. Compliance with the associated ~~open source~~ licenses requires a set of due diligence activities that each organization performs independently: a manual or automated scan of software and identification of associated licenses. Software development teams across the globe use the same open source packages, but they have not yet set-up a way to collaborate on ~~OSS~~ license discovery – many groups are performing the same work leading to duplicated effort and redundancy. This working group seeks to create [a data exchange format](#) ~~standards~~ so that information about ~~OSS~~ software packages and ~~projects~~ [related](#) content, ~~such as licenses,~~ may be collected and shared in a common format ~~and repository~~ with the goal of saving time and improving data accuracy.

Charter

Create a set of data exchange standards to enable organizations to share license and component information (metadata) for software packages [and related content](#) with the aim of facilitating license and other policy compliance.

Key elements for standardization

- Common definitions for fields in the data template (ie. License identifiers, etc)

- Unique way to match template information against a package
- Summary information for entire package
- Summary information on a per file basis inside package.
- Mechanism to share information among participants (later phase)