SPDX®
SOFTWARE PACKAGE DATA EXCHANGE®

Overview for OMG Open Source Standards Workshop

Phil Odence- SPDX Chair, VP of Corp and Business Dev, Black Duck

11 December 2013

Agenda

- Context
- Workgroup
- SPDX
- Status
- Scope vis a vis Michel’s vision
- Questions/Discussion

Software Package Data Exchange® (SPDX®)

- A standard format for communicating the components, licenses and copyrights associated with a software package.
- Key pillar in Linux Foundation's Open Compliance Program which comprises:
  - Tools, Self-Assessment, SPDX, Rapid Alert System, Training, Community

The Need

I don't mind vetting our code, but I'm sure this imported package has been analyzed a dozen times before.

Our suppliers aren't giving us complete licensing information for open source packages.

Every customer wants a bill of materials in a different form.

software in

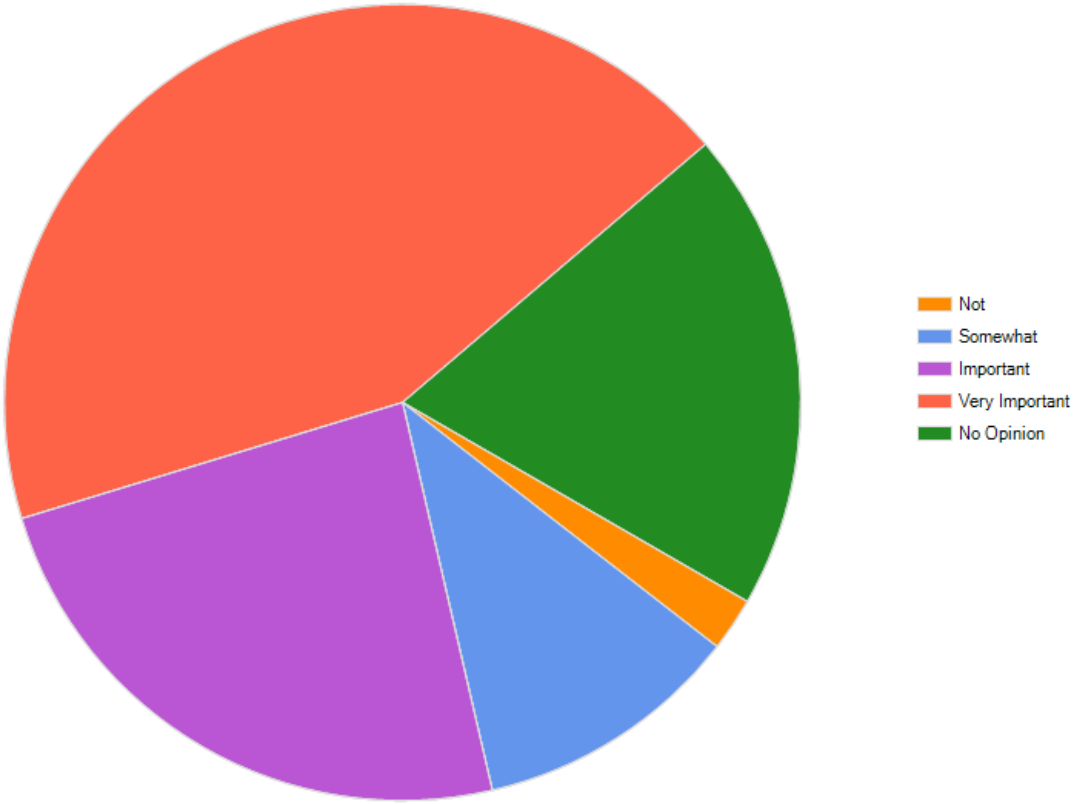
software out

(Important Part of the) Solution

- *A file format for license information* to accompany open source packages
  - Guiding Principle: Focus on capturing facts; avoid interpretations.
- 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 receivers
  - Ultimately yields better compliance with less effort

How much of a problem is it?

How important is an industry standard for exchanging software BOMs?



SPDX® Group

- A work group of Linux Foundation
- Goal
  - To create a defined format for a file of license fact information describing a software package
- History
  - A grass roots effort started by corporate counsels, business leads, and release managers responsible for ensuring release compliance with applicable licenses of FOSS included in the release
- Operation
  - Open participation through www.spdx.org

Participants

- Open Source Organizations
- End-Users
- Integration & Services
- Device OEMs
- Applications
- OS Distributions
- Systems
- Semiconductor Vendors

Participation is from a range of organizations and across various roles

The SPDX License List

SPDX® license repo

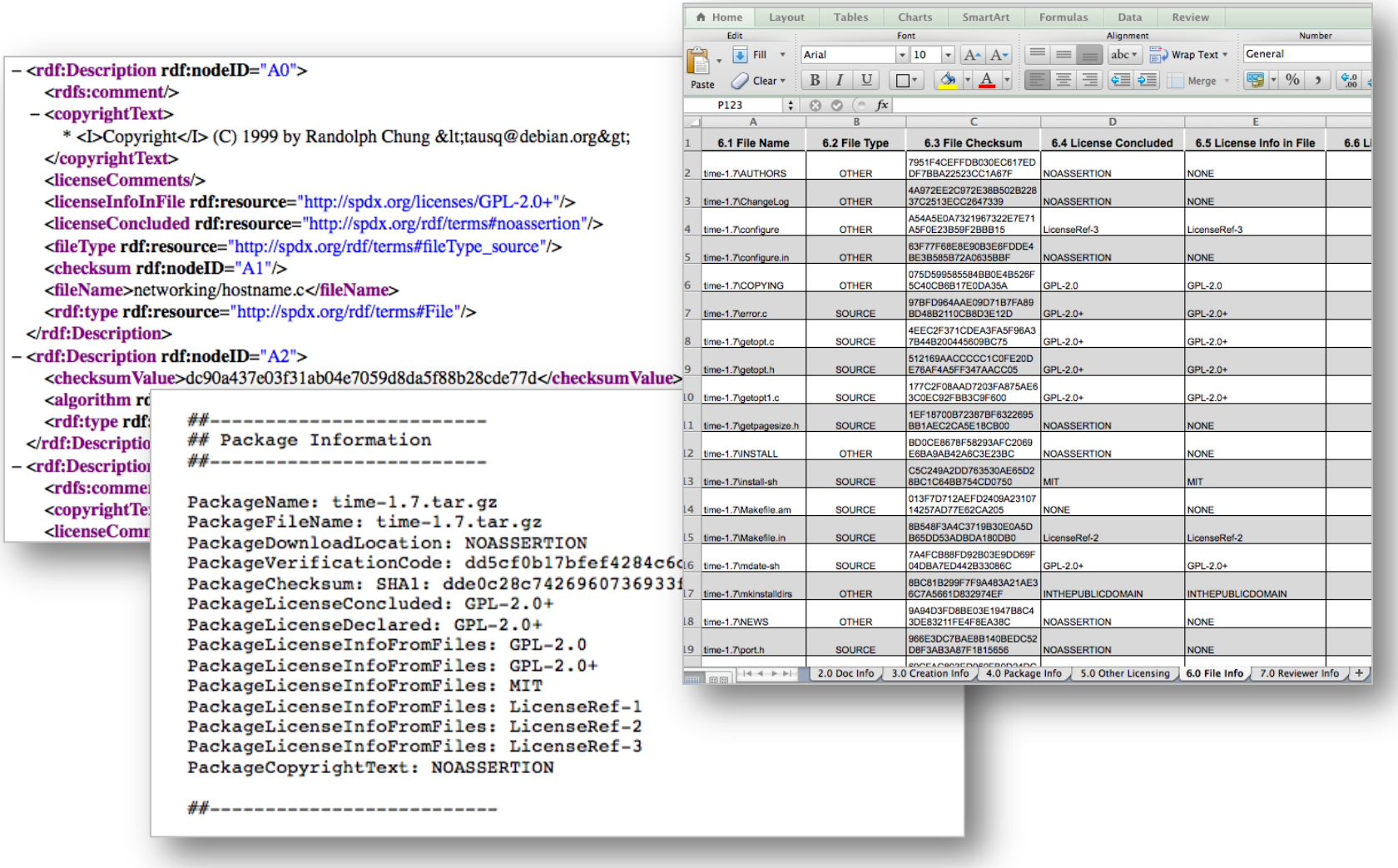
License Identifier	Recognized Exceptions	Full name of License
AFL-3.0		Academic Free License 3.0
AGPL-3.0		(GNU) Affero General Public License v3
APL		Adaptive Public License
ASL-2.0		Apache License, 2.0
APSL-2.0		Apple Public Source License 2.0
Artistic-2.0		Artistic license 2.0
AAL		Attribution Assurance 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 (200+)
- Include common exceptions
- Standardized license names
- Exact text of licenses
- Available on SPDX® website – URLs won't change

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 License List
Review Information	Log of 3rd party reviews

Support Forms: RDF & Tag Value Spreadsheet thru translation



```
– <rdf:Description rdf:nodeID="A0">
    <rdfs:comment/>
  – <copyrightText>
      * <I>Copyright</I> (C) 1999 by Randolph Chung &lt;tausq@debian.org&gt;
    </copyrightText>
    <licenseComments/>
    <licenseInfoInFile rdf:resource="http://spdx.org/licenses/GPL-2.0+"/>
    <licenseConcluded rdf:resource="http://spdx.org/rdf/terms#noassertion"/>
    <fileType rdf:resource="http://spdx.org/rdf/terms#fileType_source"/>
    <checksum rdf:nodeID="A1"/>
    <fileName>networking/hostname.c</fileName>
    <rdf:type rdf:resource="http://spdx.org/rdf/terms#File"/>
  </rdf:Description>
– <rdf:Description rdf:nodeID="A2">
    <checksumValue>dc90a437e03f31ab04e7059d8da5f88b28cde77d</checksumValue>
    <algorithm rd
    <rdf:type rdf:
  </rdf:Descriptio
– <rdf:Descriptio
    <rdfs:comme
    <copyrightTe
    <licenseComm
```

```
##-------------------------
## Package Information
##-------------------------

PackageName: time-1.7.tar.gz
PackageFileName: time-1.7.tar.gz
PackageDownloadLocation: NOASSERTION
PackageVerificationCode: dd5cf0b17bfef4284c6c
PackageChecksum: SHA1: dde0c28c74269607369331
PackageLicenseConcluded: GPL-2.0+
PackageLicenseDeclared: GPL-2.0+
PackageLicenseInfoFromFiles: GPL-2.0
PackageLicenseInfoFromFiles: GPL-2.0+
PackageLicenseInfoFromFiles: MIT
PackageLicenseInfoFromFiles: LicenseRef-1
PackageLicenseInfoFromFiles: LicenseRef-2
PackageLicenseInfoFromFiles: LicenseRef-3
PackageCopyrightText: NOASSERTION

##-------------------------
```

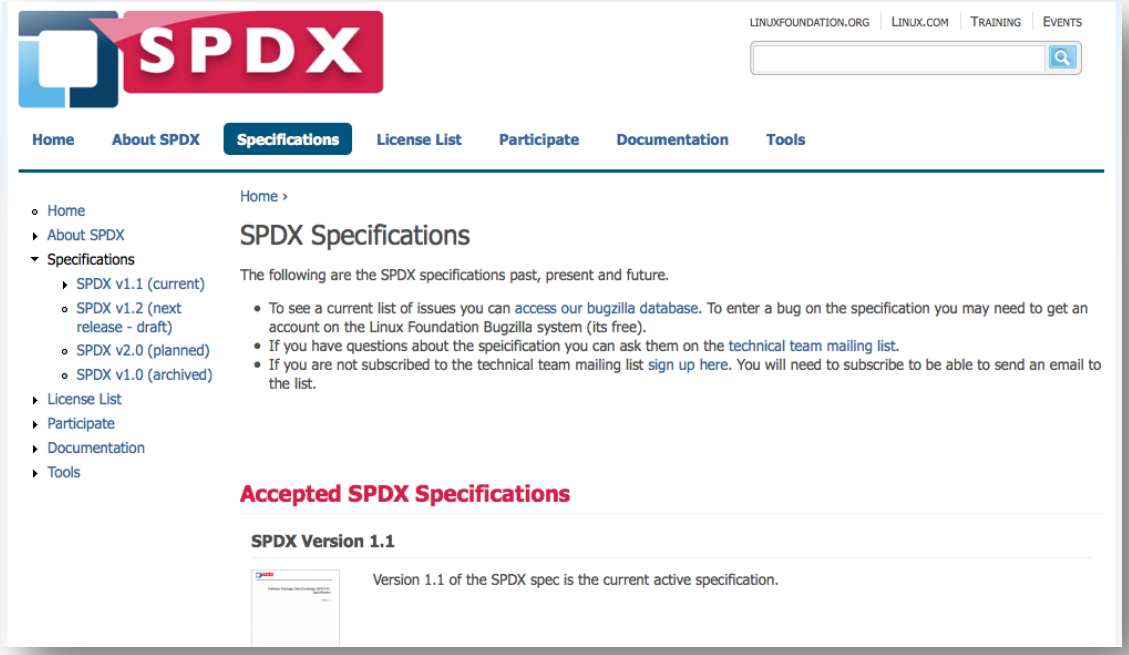
	6.1 File Name	6.2 File Type	6.3 File Checksum	6.4 License Concluded	6.5 License Info in File
2	time-1.7\AUTHORS	OTHER	7951F4CEFFDB030EC617ED DF7BBA22523CC1A67F	NOASSERTION	NONE
3	time-1.7\ChangeLog	OTHER	4A972EE2C972E38B502B228 37C2513ECC2647339	NOASSERTION	NONE
4	time-1.7\configure	OTHER	A54A5E0A7321967322E7E71 A5F0E23B59F2BBB15	LicenseRef-3	LicenseRef-3
5	time-1.7\configure.in	OTHER	63F77F68E8E90B3E6FDDE4 BE3B585B72A0635BBF	NOASSERTION	NONE
6	time-1.7\COPYING	OTHER	075D599585584BB0E4B526F 5C40CB6B17E0DA35A	GPL-2.0	GPL-2.0
7	time-1.7\error.c	SOURCE	97BFD964AAE09D71B7FA89 BD48B2110CB8D3E12D	GPL-2.0+	GPL-2.0+
8	time-1.7\getopt.c	SOURCE	4EEC2F371CDEA3FA5F96A3 7B44B200445609BC75	GPL-2.0+	GPL-2.0+
9	time-1.7\getopt.h	SOURCE	512169AACCCCC1C0FE20D E76AF4A5FF347AACC05	GPL-2.0+	GPL-2.0+
10	time-1.7\getopt1.c	SOURCE	177C2F08AAD7203FA875AE6 3C0EC92FBB3C9F600	GPL-2.0+	GPL-2.0+
11	time-1.7\getpagesize.h	SOURCE	1EF18700B72387BF6322695 BB1AEC2CA5E18CB00	NOASSERTION	NONE
12	time-1.7\INSTALL	OTHER	BD0CE8678F58293AFC2069 E6BA9AB42A6C3E23BC	NOASSERTION	NONE
13	time-1.7\install-sh	SOURCE	C5C249A2DD763530AE65D2 8BC1C64BB754CD0750	MIT	MIT
14	time-1.7\Makefile.am	SOURCE	013F7D712AEFD2409A23107 14257AD77E62CA205	NONE	NONE
15	time-1.7\Makefile.in	SOURCE	8B548F3A4C3719B30E0A5D B65DD53ADBDA180DB0	LicenseRef-2	LicenseRef-2
16	time-1.7\mdate-sh	SOURCE	7A4FCB88FD92B03E9DD69F 04DBA7ED442B33086C	GPL-2.0+	GPL-2.0+
17	time-1.7\mkinstalldirs	OTHER	8BC81B299F7F9A483A21AE3 6C7A5661D832974EF	INTHEPUBLICDOMAIN	INTHEPUBLICDOMAIN
18	time-1.7\NEWS	OTHER	9A94D3FD8BE03E1947B8C4 3DE83211FE4F8EA38C	NOASSERTION	NONE
19	time-1.7\port.h	SOURCE	966E3DC7BAE8B140BEDC52 D8F3AB3A87F1815656	NOASSERTION	NONE

Adoption

- License List
  - Internal- TI, Wind River, Microfocus, HP, Siemens
  - Tools Utilizing- Black Duck, nexB, Protecode, FOSSology
  - OSI, Debian
- Format
  - TI, Wind River, Alcatel-Lucent, Samsung, unnamed others
- Tagging Files
  - U-Boot, Wind River, Other OSS projects under discussion
- Tooling http://spdx.org/tools
  - Wind River, Black Duck, FOSSology/UNO, SPDX OSS

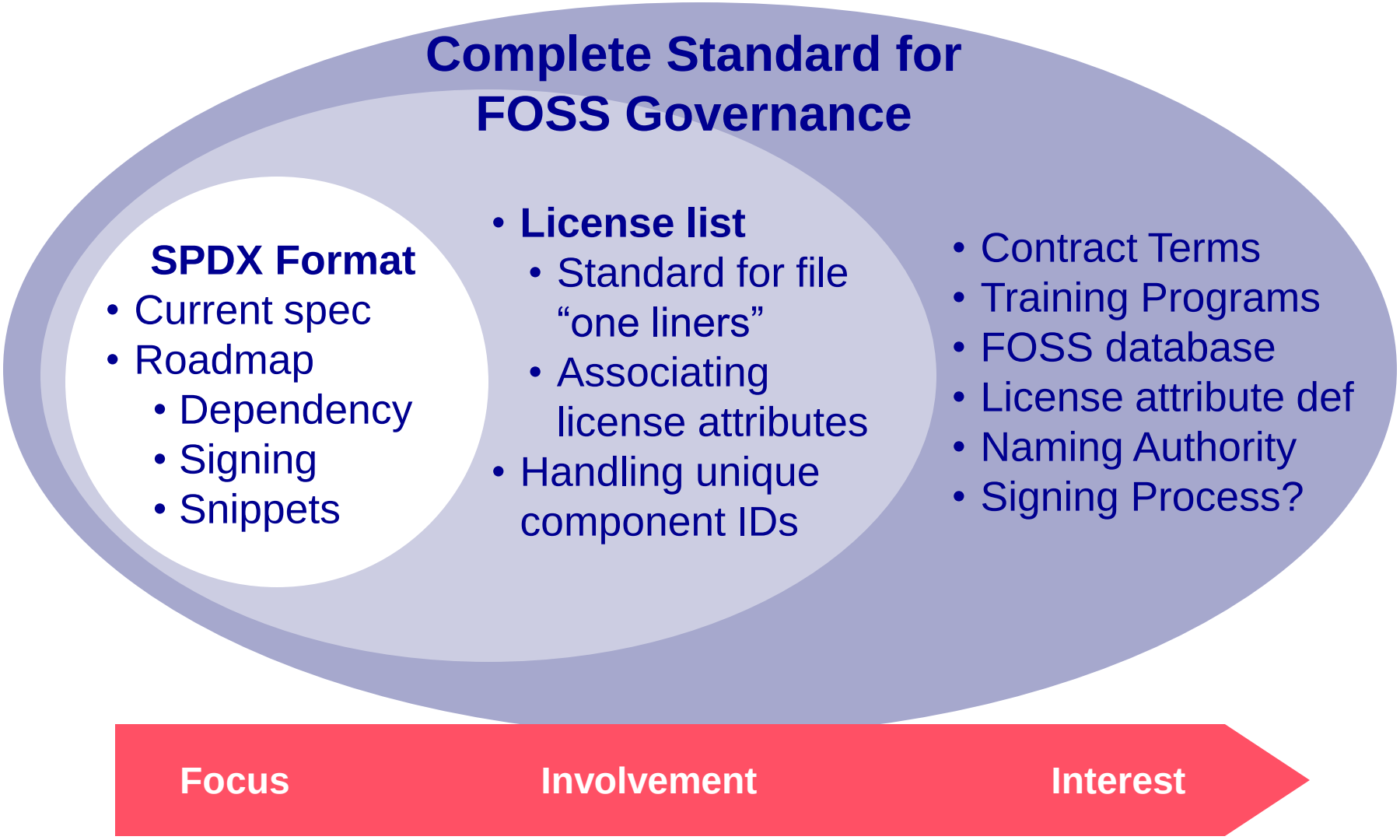
Status

- Version 1.1– August 2012
- Version 1.2– October 2013
- Version 2.0– Targeted 2014



http://www.spdx.org

SPDX Scope and Interest



Discussion Questions?

Phil Odence 

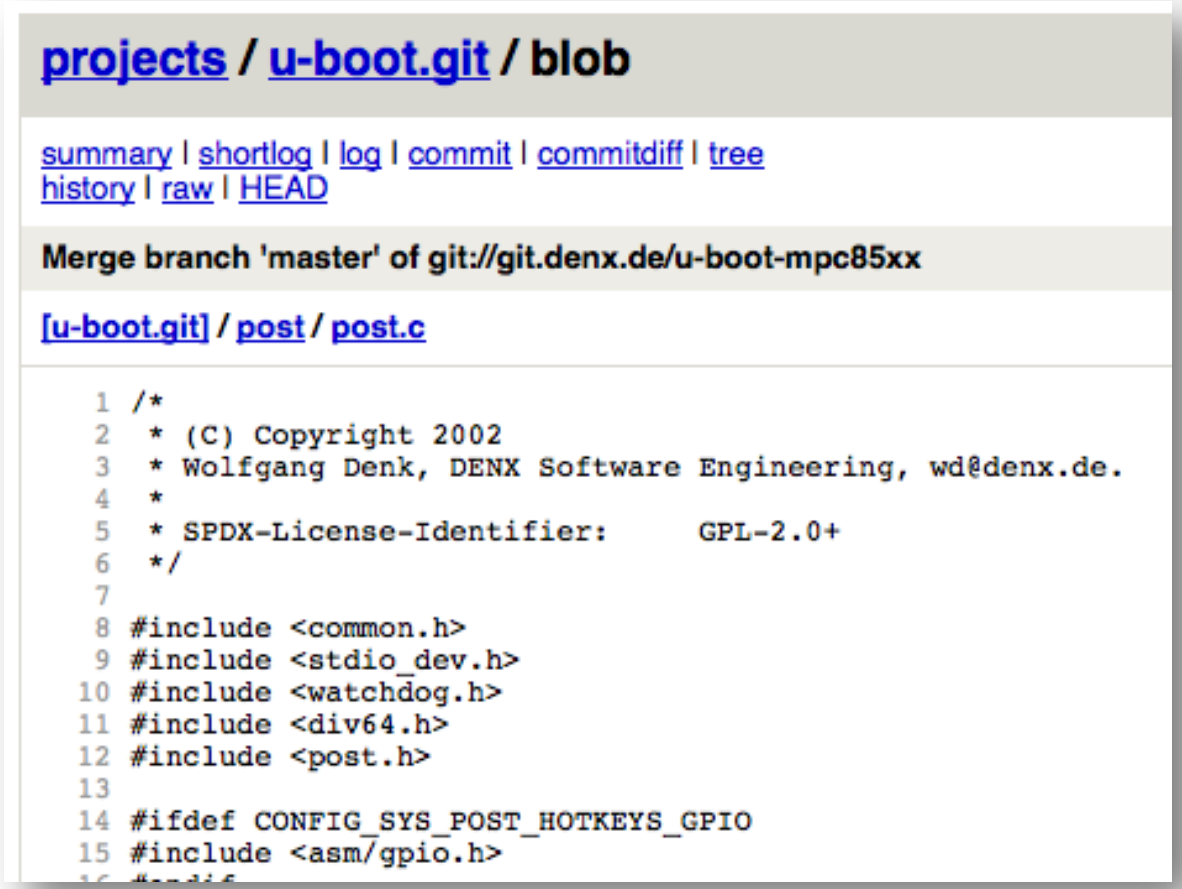
podence@blackducksoftware.com

Please get involved:
http://www.spdx.org

SPDX Colleagues here today

Thomas Vidal	AGMB Law
Gary O'Neall	Source Auditor
Mark Gisi	Wind River
Dennis Clark	nexB
Pierre Lapointe	nexB
Michael Herzog	nexB

U-Boot One-liner



projects / u-boot.git / blob

summary | shortlog | log | commit | commitdiff | tree
history | raw | HEAD

Merge branch 'master' of git://git.denx.de/u-boot-mpc85xx

[u-boot.git] / post / post.c

```
 1 /*
 2  * (C) Copyright 2002
 3  * Wolfgang Denk, DENX Software Engineering, wd@denx.de.
 4  *
 5  * SPDX-License-Identifier:     GPL-2.0+
 6  */
 7
 8 #include <common.h>
 9 #include <stdio_dev.h>
10 #include <watchdog.h>
11 #include <div64.h>
12 #include <post.h>
13
14 #ifdef CONFIG_SYS_POST_HOTKEYS_GPIO
15 #include <asm/gpio.h>
```

Tools for SPDX®

- Open Source Tools (hosted on SPDX Git Repo)
  - Viewer
  - Spreadsheet to RDF/Tag Value xlator
  - RDF/Tag Value to Spreadsheet xlator
  - License file generator (from Spreadsheet)
  - Spreadsheet template
  - FOSSology via University of Nebraska Omaha
- Commercial Tools
  - Black Duck Protex
  - Wind River