SPDX™
SOFTWARE PACKAGE DATA EXCHANGE™

Kim Weins

SVP Products & Marketing

OpenLogic®

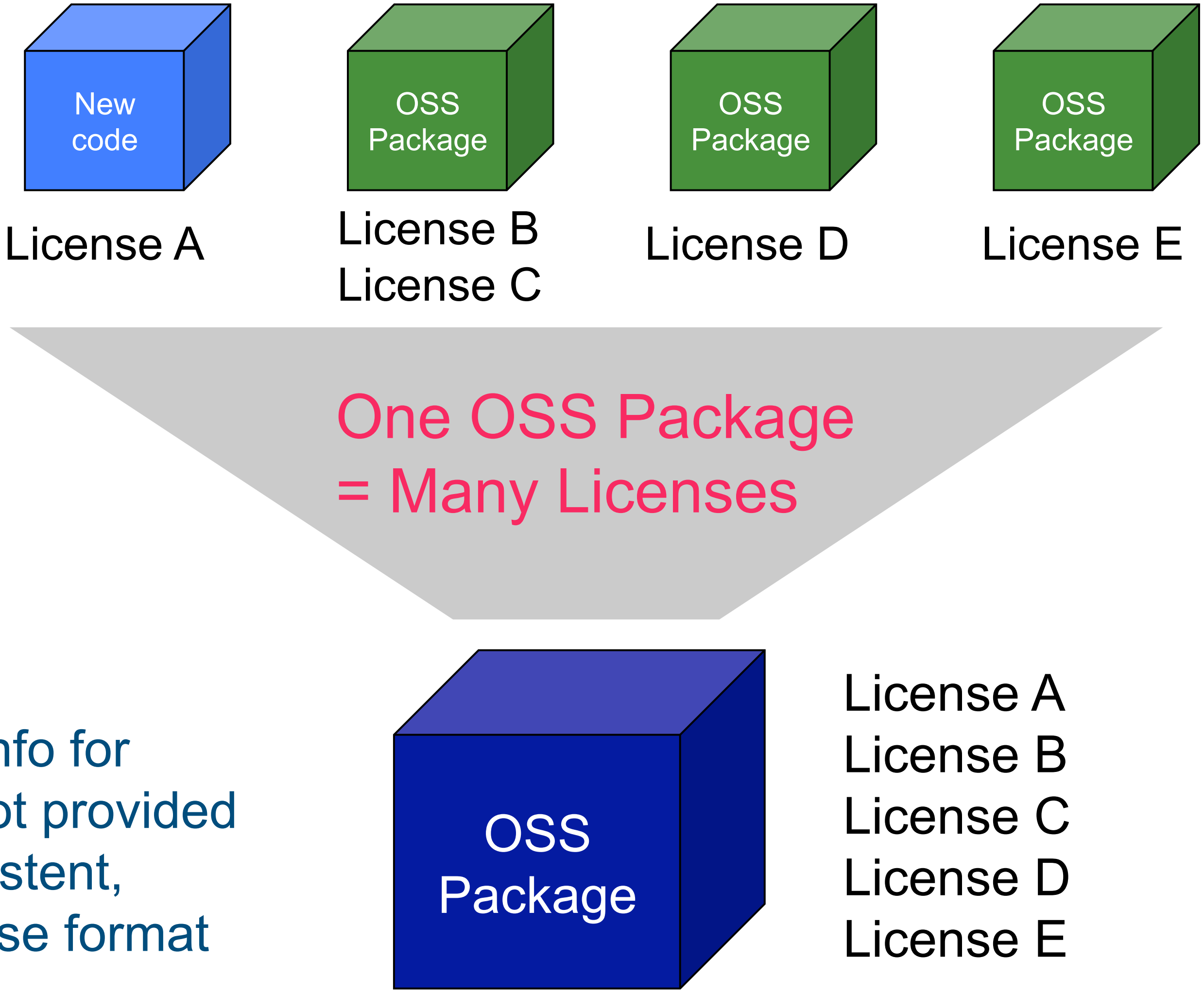
What You’ll Learn

- The Challenges of Open Source Compliance
- How SPDX™ Can Help
- What it Means to You
- How to Participate

Open Source Compliance

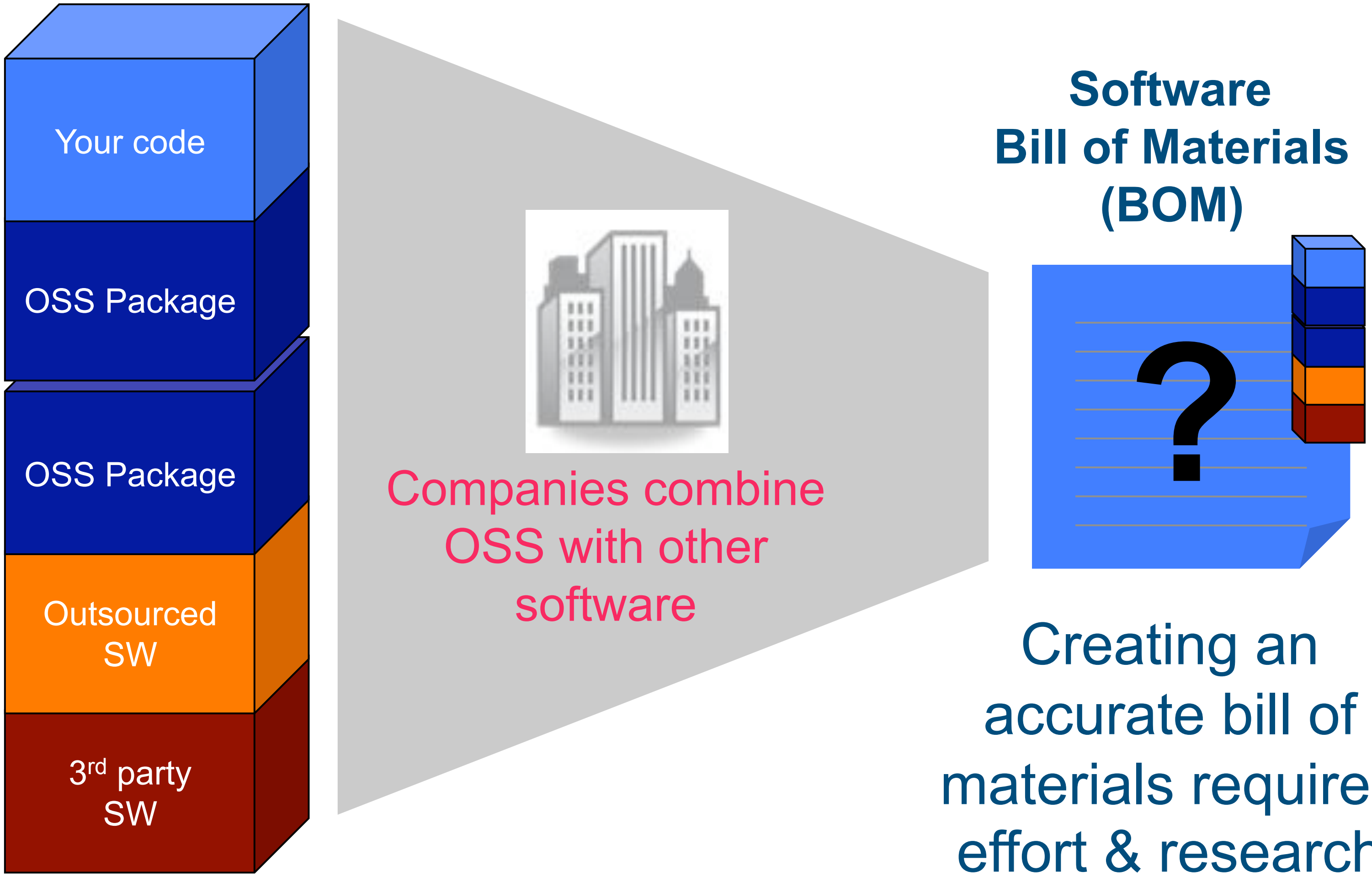
Companies know they need to comply with open source licenses, but doing so can be challenging

Open Source Compliance: The Challenge



License info for OSS is not provided in a consistent, easy-to-use format

Open Source Compliance: The Challenge



Your code

OSS Package

OSS Package

Outsourced SW

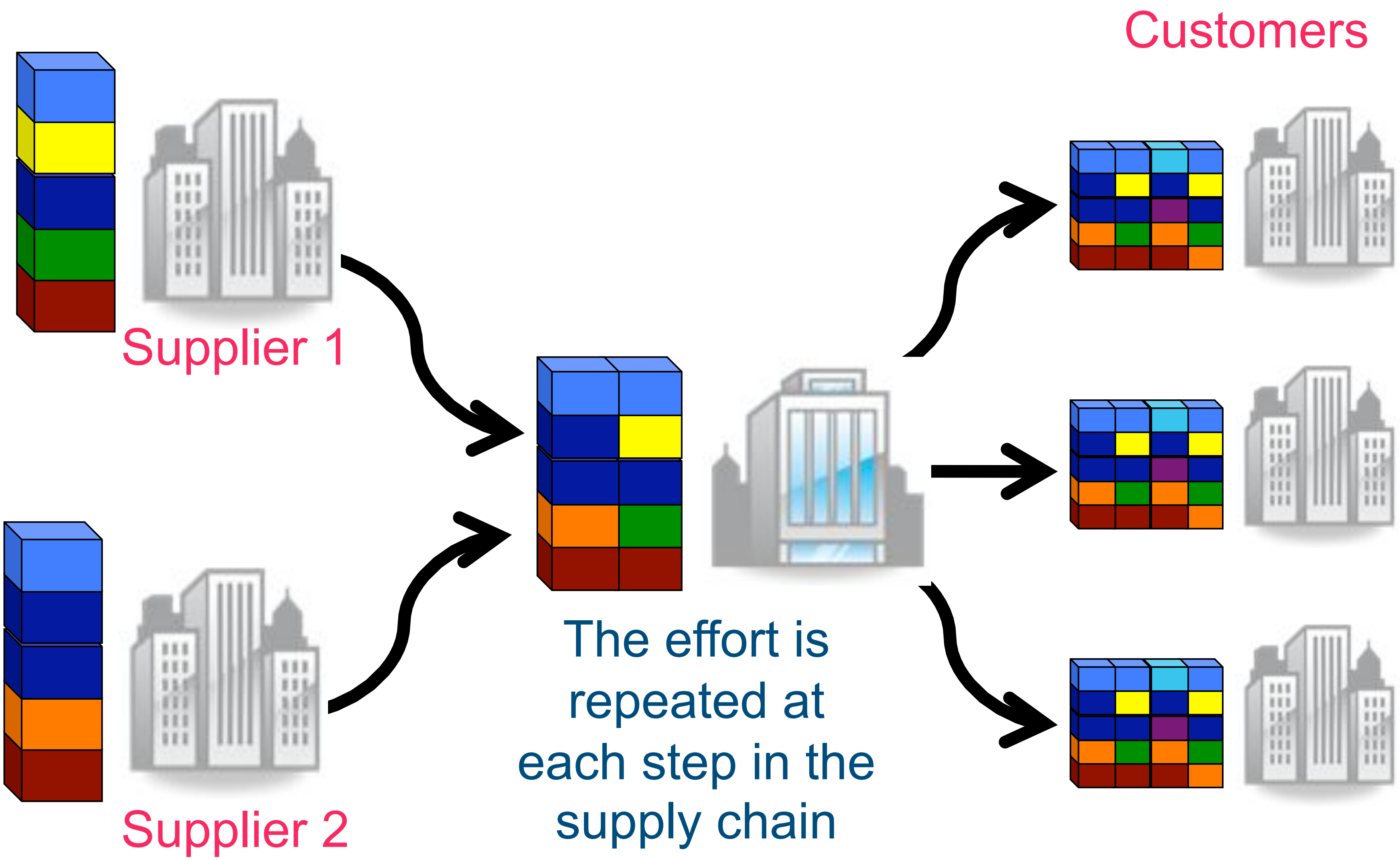
3rd party SW

Companies combine OSS with other software

Software Bill of Materials (BOM)

Creating an accurate bill of materials requires effort & research

Open Source Compliance: The Challenge



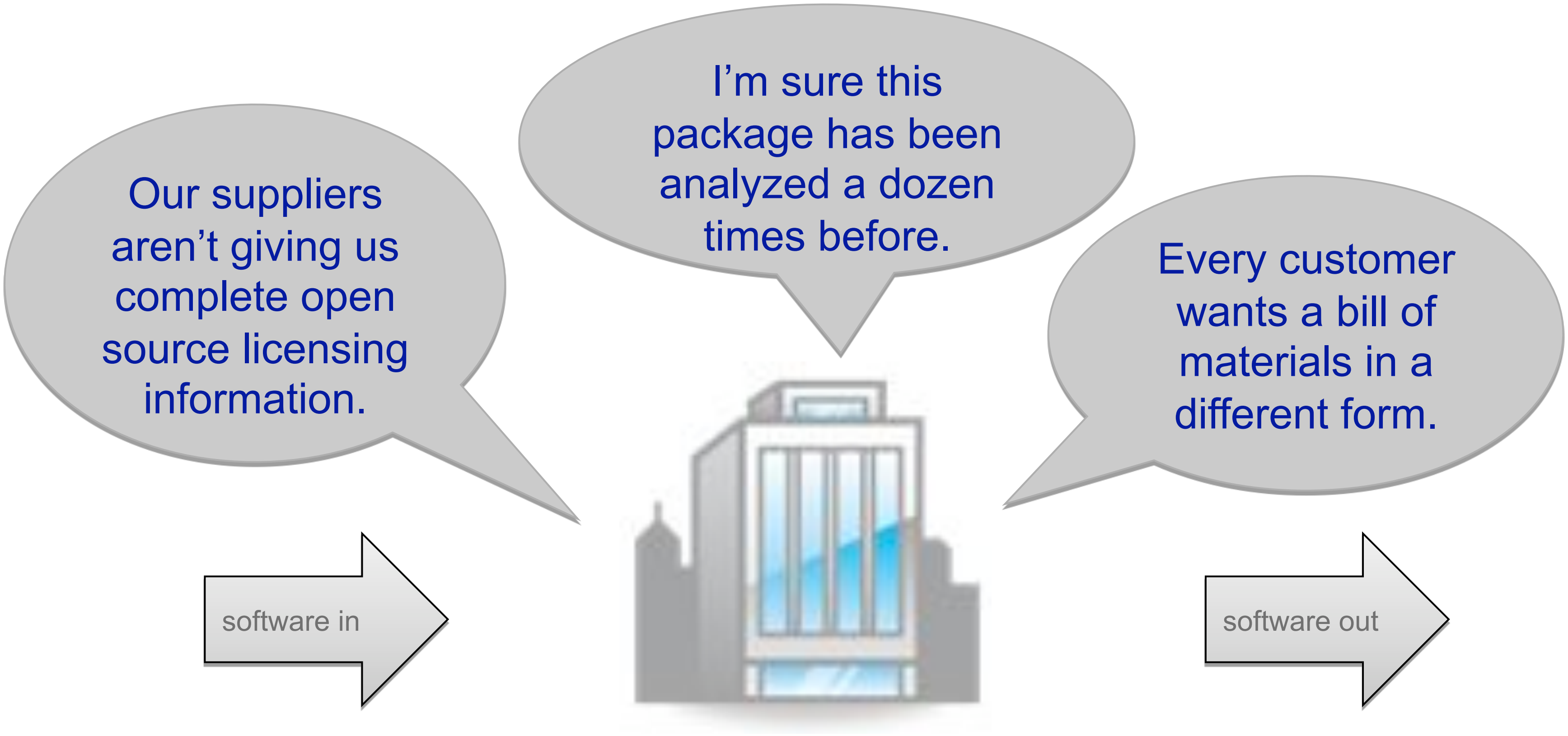
Customers

Supplier 1

Supplier 2

The effort is repeated at each step in the supply chain

The Motivation for SPDX™



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

I'm sure this package has been analyzed a dozen times before.

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

software in

software out

We need a standardized format for a software Bill of Materials that can be used throughout the supply chain

Software Package Data Exchange™ (SPDX™)

- 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

Benefits

- Reduce burden of providing information in different formats for different consumers
- Avoids due diligence redundancy where packages are re-analyzed
- Enable better compliance with open source licenses

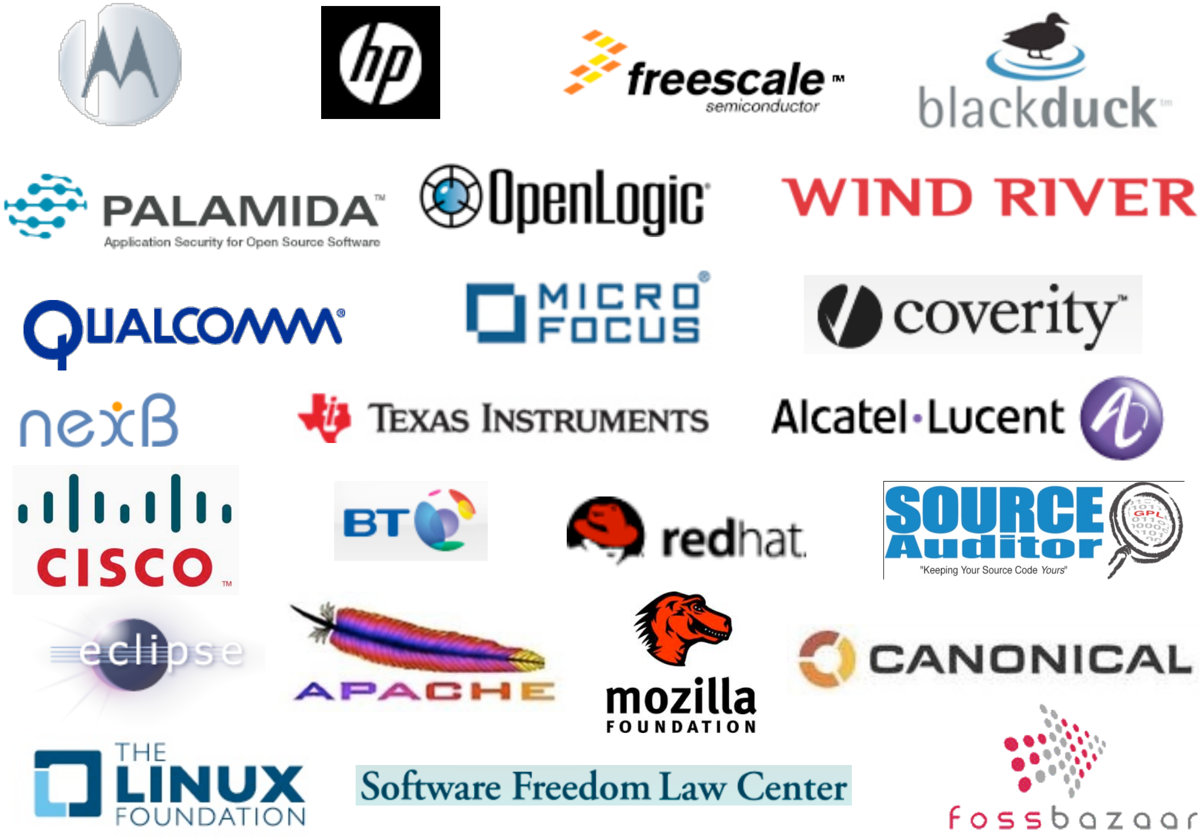
Guiding Principle

✔ Just the facts!

🚫 Interpretation

The SPDX™ Group

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

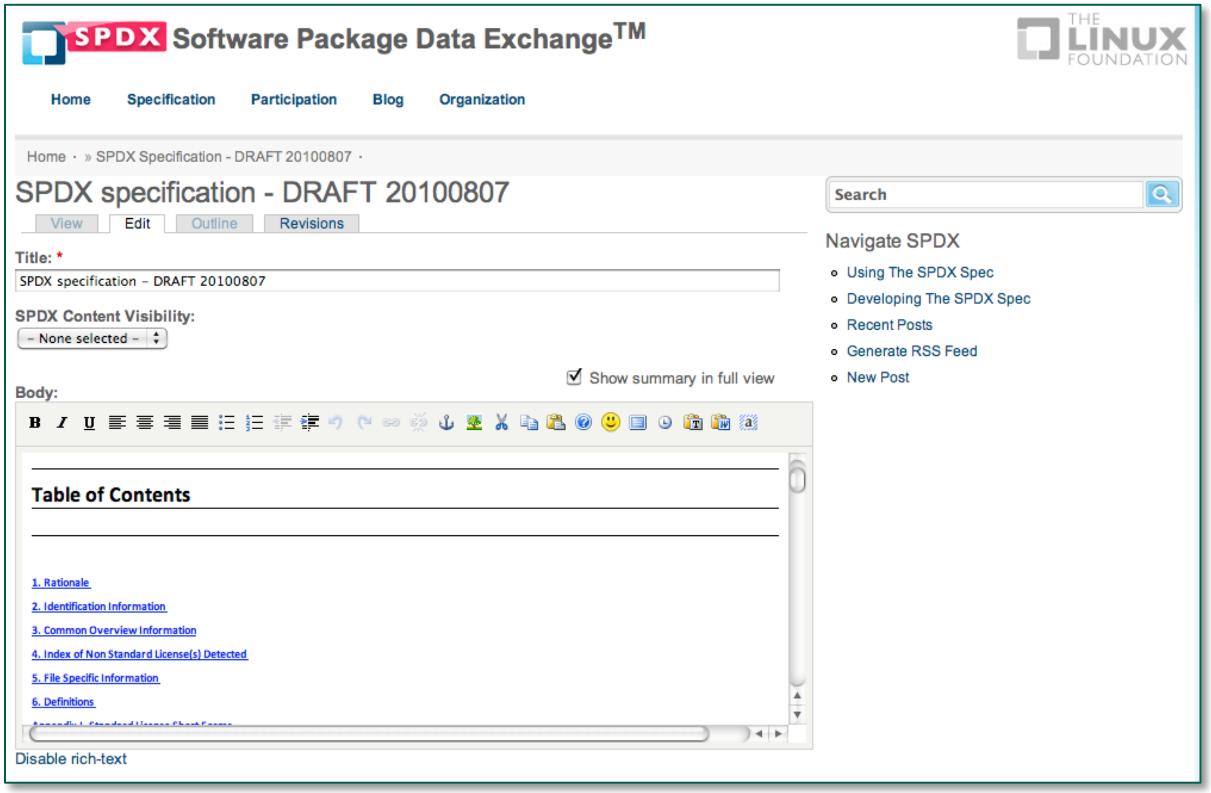


…and others

Participation is from a range of organizations and across various roles

The SPDX™ Specification

- Version 1.0 beta - available
- Soliciting Beta sites and feedback



Home · » SPDX Specification - DRAFT 20100807 ·

SPDX specification - DRAFT 20100807

Title: *

SPDX specification – DRAFT 20100807

SPDX Content Visibility:

– None selected –

☑ Show summary in full view

Body:

Table of Contents

1. Rationale

2. Identification Information

3. Common Overview Information

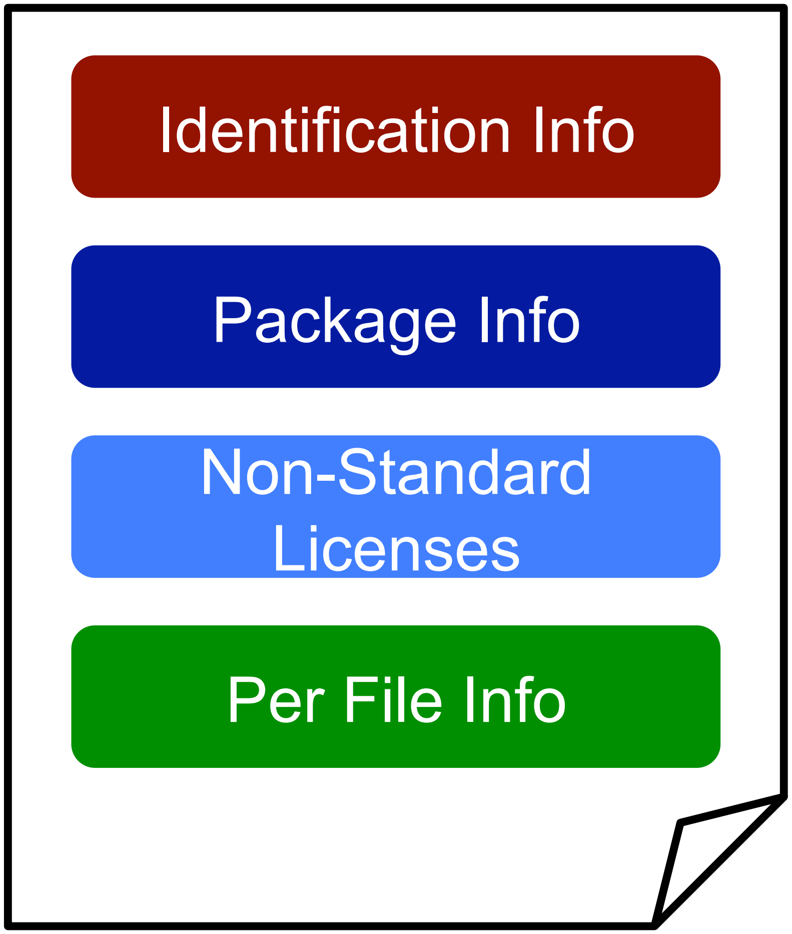
4. Index of Non Standard License(s) Detected

5. File Specific Information

6. Definitions

Appendix I: Standard License Short Forms

The SPDX™ File



Identification Info

Package Info

Non-Standard Licenses

Per File Info

Source of this SPDX™ file

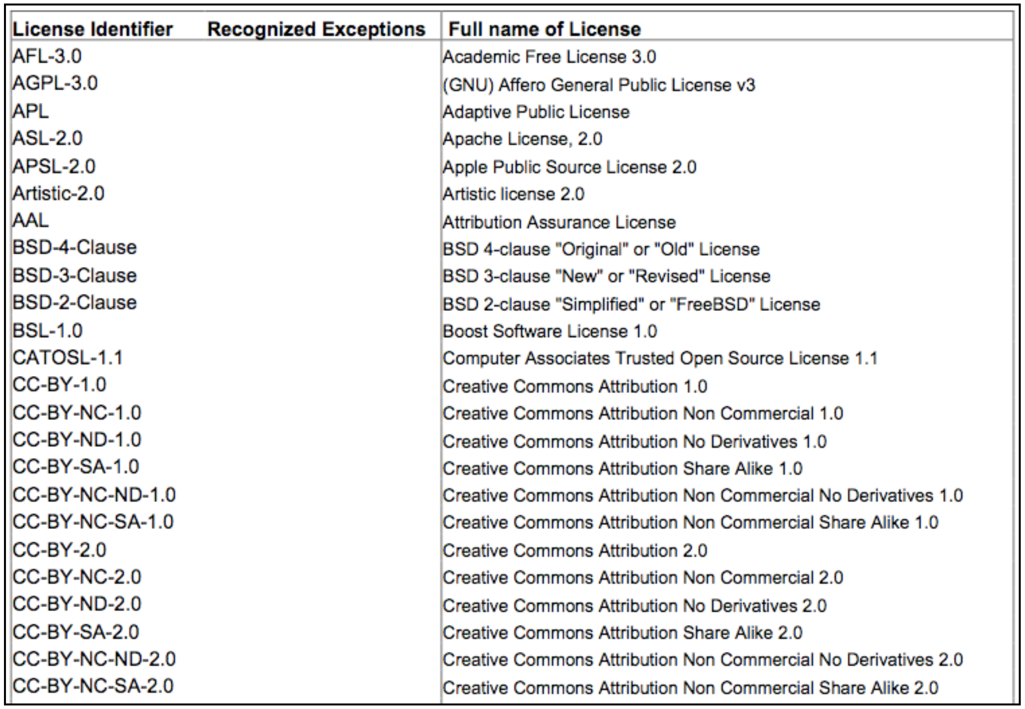
Associates an SPDX™ file with a software package (tarball, zip, archive)

Text of licenses that are not in the SPDX™ standard list

License associated with each file

SPDX™ Standard Licenses

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

Standardized license names

Exact text of licenses available on SPDX™ website – URLs won't change

Tools for SPDX™

- Tools Needed
  - Viewers
  - Validators
  - Create SPDX™ file
  - Read SPDX™ file
- Open Source Tools
  - “Pretty Print” viewer for SPDX™
  - License scanning tools (Fossology, Ninka)
  - More to come…
- Commercial Tools
  - Scanning tools expected to provide SPDX™ support

What it Means to You

Embedded & SW Supply Chains	Save Time/Money Better Compliance
Open Source Developers	Help Users Comply With Your Licenses
Consumers of SW & OSS	Understand the Licenses of the Code You Use

Get Involved

- Read the Spec
- Join the SPDX™ Group
- Provide Feedback
- Try it Out
- Become a Beta Site
- Contribute
  - We need Business, Marketing, Technical, Legal people to help
- Talk to Others
  - Your Company, Supply Chain Partners, Community Members

Contact Info

- See:
  - http://www.spdx.org

- Contact Me:
  - Kim Weins kim.weins@openlogic.com

- Other SPDX™ Contacts:
  - Phil Odence (co-chair) podence@blackducksoftware.com
  - Kate Stewart (co-chair) stewart@linux.com
  - Martin Michlmayr (FOSSBazaar liason) tbm@hp.com

QUESTIONS?

Thank you!