Overview

- Software is everywhere
- How SPDX helps the supply chain
- Black Duck & SPDX case study
- SPDX v2
SOFTWARE IS EVERYWHERE
Open Source Software – Market Trends

“Software is Eating the World.”

Marc Andreessen

“Open Source is ubiquitous...having a policy against open source [use] is impractical and places you at a competitive disadvantage.”

Mark Driver, Gartner
Open Source: the Foundation for Game Changers

Copyright © 2012 Black Duck Software, Inc. All Rights Reserved.
The License Compliance Challenge

Contributors must deliver license compliant code

Platform owner must deliver license compliant platform

OEM must deliver license compliant device

Everyone in the supply chain must implement an effective FOSS Management infrastructure!
How SPDX Can Help!
SPDX™ and Software Bill of Materials

A standard format for communicating a software Bill of Materials across the supply chain.

Benefits:
- Reduced effort
- Reuse analysis
- Improve compliance
SPDX® Group

- A working group of Linux Foundation and a key pillar in Linux Foundation’s

Goal
- 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:
A range of organizations and roles

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

...and others
Status

- Version 1.0 – Released August 2011
- Version 1.1 – Q2 2012
- Version 2.0 – Targeted H2 2012

http://www.spdx.org
What SPDX® Means for You

**Embedded & SW Supply Chains**
- Save Time/Money
- Better Compliance

**Open Source Developers**
- Help Users Comply With Your Licenses

**Consumers of SW & OSS**
- Understand Licensing of the Code You Use
### The SPDX® License List

**SPDX® license repo**

- List of most common licenses (150+)
- Standardized license names
- Exact text of licenses
- Guidelines for matching
- Available on SPDX® website – URLs won’t change
- Short names adopted by OSI

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

- **Document & Creation Info**: SPDX version and SPDX data license. How, when, who.
- **Package Info**: Package identification, copyright and licensing.
- **File Info**: Per-file identification, copyright and licensing.
- **Licensing Info**: Text of licenses that are not in SPDX™ standard list.
- **Review**: Log of 3rd party reviews.

File is in RDF/XML or tag value form; can be converted to/from spreadsheets.
Tools for SPDX®

- **Open Source Tools** (git.spdx.org)
  - Viewer
  - Translate from
    - Spreadsheet to RDF or Tag/Value
    - RDF to Spreadsheet
    - Tag/Value to Spreadsheet
  - License file generator (from Spreadsheet)
  - Spreadsheet template

- **Commercial Tools**
  - Scanning tools to provide SPDX™ support
Black Duck & SPDX Case Study
Open Source in Automotive

- 100+ million lines of code in a premium-class car
- 70% of the code is in the **in-vehicle infotainment (IVI)** sub-systems

Open source can:
- Reduce costs
- Speed time-to-market
- Increase innovation and differentiation
Multi-Tier Automotive Supply Chain
Case Study – GENIVI Ecosystem

- GENIVI is a classic OSS Supply Chain
  - enables a hybrid model for combined proprietary and FOSS

- Three-stage value proposition for Auto ecosystem
  - MontaVista as Platform System Integrator for a Linux-based Next Generation In-Vehicle Infotainment system (IVI)
  - GENIVI creates a baselined BOM for IVI OSS ecosystem
  - With Black Duck, BearingPoint & MontaVista, assist Alliance members with IP compliance using tooling

- Black Duck provides BOM in multiple formats, including SPDX v1.0 standard
Shifting Gears with a Complete GENIVI Solution

OSS Dev. Tools, SDKs, Automotive Tech Platform (ATP) & Services

Embedded Platforms

FOSS License Compliance

BDS Solutions Offerings

Process Analysis and OSS Governance

OSS Strategy Consulting & Implementation

Copyright © 2012 Black Duck Software, Inc. All Rights Reserved.
All supply chain participants required to implement FOSS Management infrastructure!
You Can Help: SPDX v2
Get Involved!

- The SPDX Group is currently working on SPDX v2

- Areas of Focus include
  - Package Hierarchy
  - Composite licensing
  - Signing (provenance)
  - Collecting / codifying shared knowledge
  - Automation / Easier Creation & Consumption

- Use Case driven - http://spdx.org/wiki/spdx-20-use-cases
  - Patch provider
  - Upstream maintainer
  - Intermediate packager
Get Involved!

- See: [http://www.spdx.org](http://www.spdx.org)

- Contact:
  - General - Phil Odence (Chair) - podence@blackducksoftware.com
  - Business team - Jack Manbeck (Co-Chair)- j-manbeck2@ti.com
  - Legal team - Jilayne Lovejoy (Co-Chair) - jilayne.lovejoy@openlogic.com
  - Technical team - Kate Stewart (Chair) - stewart@linux.com
Thank You!

Kirsten Newcomer
knewcomer@blackducksoftware.com