

# How to manage FOSS compliance information in an ecosystem

Nov 17th, 2017

Lei Maohui, Fujitsu

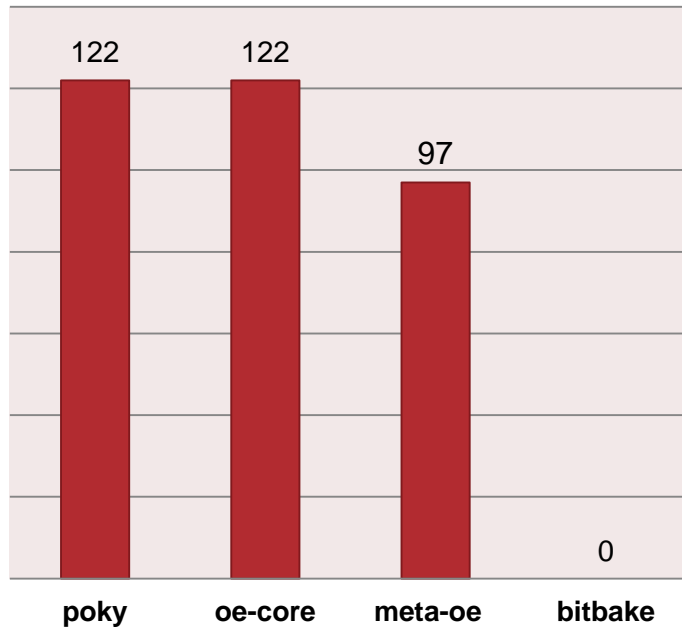
[leimaohui@cn.fujitsu.com](mailto:leimaohui@cn.fujitsu.com)

# Fujitsu's contributions to Yocto community

■ Data comes from yocto (2016-10-31 ~ 2017-11-01)

## Contributions in yocto

■ commits



	Layers	Changesets
1	poky	122
2	oe-core	122
3	meta-oe	97
4	bitbake	0

# Fujitsu's contributions to Yocto community

■ Data comes from yocto (2016-10-31 ~ 2017-11-01)

## Top changeset contributors by employer

No.	employer	Changesets
1	Intel	8454
2	Wind River	1616
3	<b>Fujitsu</b>	<b>343</b>
4	Axis Communications	181
5	simens	130

## Developers with the most changesets

No.	Our Developer	Changesets
<b>poky</b>		
15	Huang Qiyu	81 (0.7%)
38	fan.xin	28 (0.2%)
<b>oe-core</b>		
14	Huang Qiyu	81 (1.1%)
29	fan.xin	28 (0.4%)
<b>Meta-oe</b>		
7	Huang Qiyu	71 (1.7%)
28	fan.xin	12 (0.3%)

## Introduction of SPDX

- Background of SPDX
- What is SPDX
- Who are working for SPDX
- The status of SPDX specification

## meta-spdxscanner in Yocto

- What is Yocto
- SPDX in Yocto
- meta-spdxscanner
- Features in meta-spdxscanner
- How to use meta-spdxscanner

## Manage SPDX files

- SPDX file works in OpenChain
- Manage SPDX files by dnf in your ecosystem
- Future work

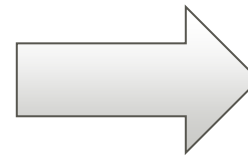
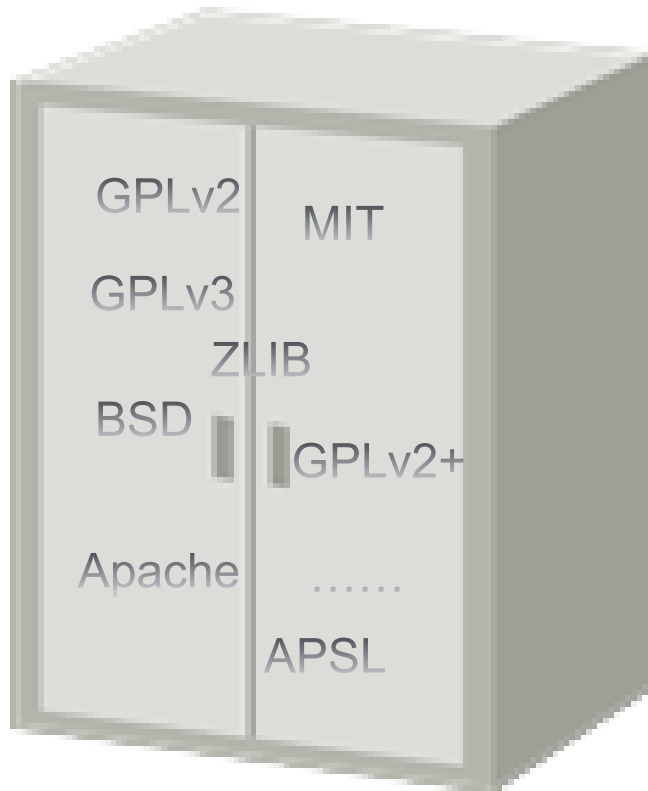
# Introduction of SPDX

- Background of SPDX
- What is SPDX
- Who are working for SPDX
- The status of SPDX specification
- Issues we met



# Background of SPDX

FOSS



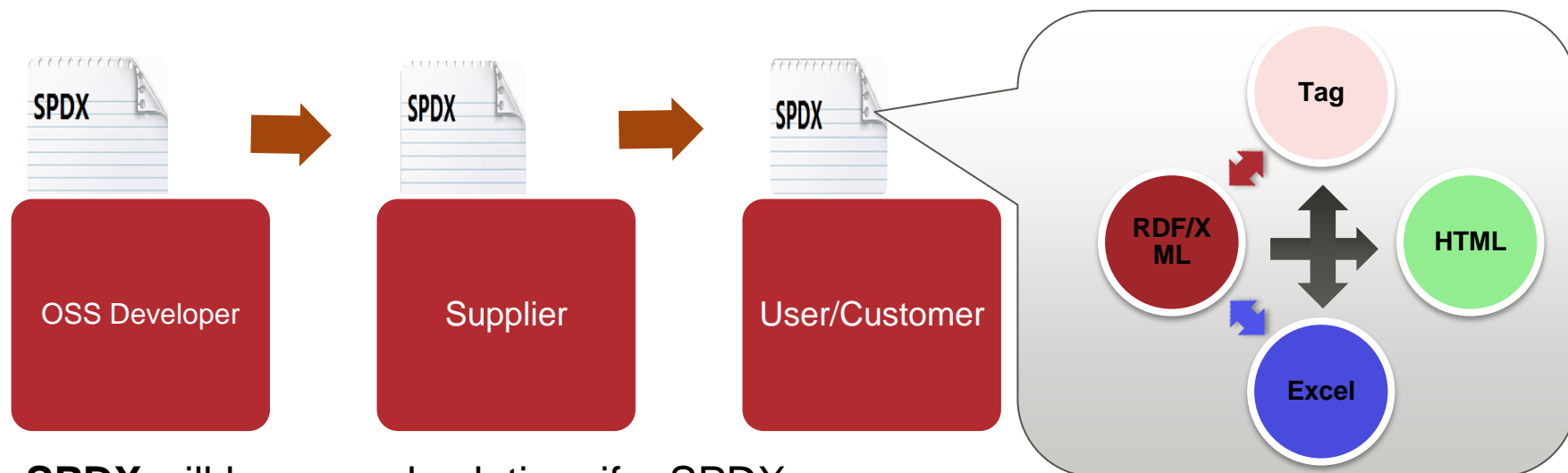
# What is SPDX (1/2)

## What is SPDX

- The full name of SPDX is **S**oftware **P**ackage **D**ata **E**xchange, which is a standard format for communicating the components, licenses and copyrights associated with a software package.

## Vision of SPDX

- achieve license compliance with minimal cost across the supply chain.



**SPDX** will be a good solution, if a SPDX implementation can generate SPDX file including license information automatically.

Obtain details from

- <https://spdx.org/tools>



# What is SPDX (2/2)


## Formats

- Tag:value
- RDF/XML

## Important or useful tags

- SPDXVersion
- DataLicense
- Creator
- PackageName
- PackageOriginator
- PackageVersion
- PackageHomePage
- PackageLicenseDeclared

## A sample of SPDX file



```
SPDXVersion: SPDX-2.0
DataLicense: CC0-1.0
PackageName: Foo
PackageOriginator: David A. Wheeler
PackageHomePage: https://github.com/david-a-wheeler/spdx-tutorial/
PackageLicenseDeclared: MIT
```



# Who are working for SPDX

## Technical Team

- **Primary responsibility**
  - Drafts the specification
  - Develops documentation templates, samples and tools.
- **Delivered**
  - SPDX Spec (2.1, 2.0, 1.2, 1.1, 1.0)
  - Tool (fossology)d
  - Spreadsheet Template
- **Recent**
  - New spec
  - New license list

## Legal Team

- **Primary responsibility**
  - Supports and provides recommendations to the SPDX working groups regarding licensing issues.
  - Maintains the [SPDX License List](#)
  - Promotes the SPDX specification to the legal community at-large
- **Delivered**
  - License Expression Syntax
  - License Inclusion Guidelines (Background))
  - Dealing with Public Domain within SPDX Files
- **Recent**
  - Joint Call with Tech Team
  - License List

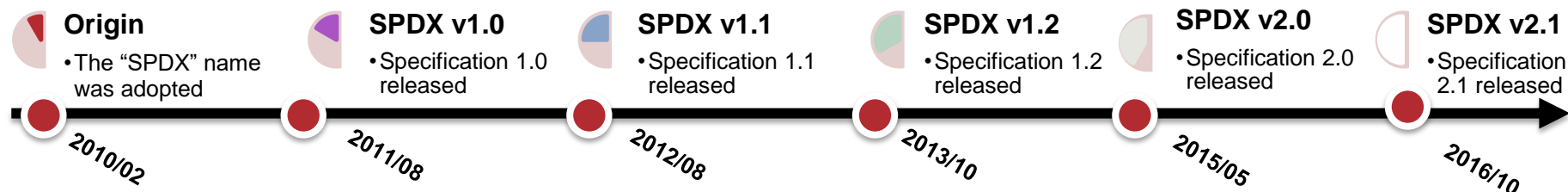
## Outreach Team

- **Primary responsibility**
  - Launch activities for new versions of the SPDX specification.
  - Outreach
  - Participation in events;
  - The SPDX website
- **Delivered**
  - Launch for 1.0 and 1.1
  - Process for Adding to License List (Draft))
  - SPDX Vision & Mission Discussion Document
  - SPDX Vision & Mission Statements (Final Draft))
- **Recent**
  - Working on tool to generate test files for scanners

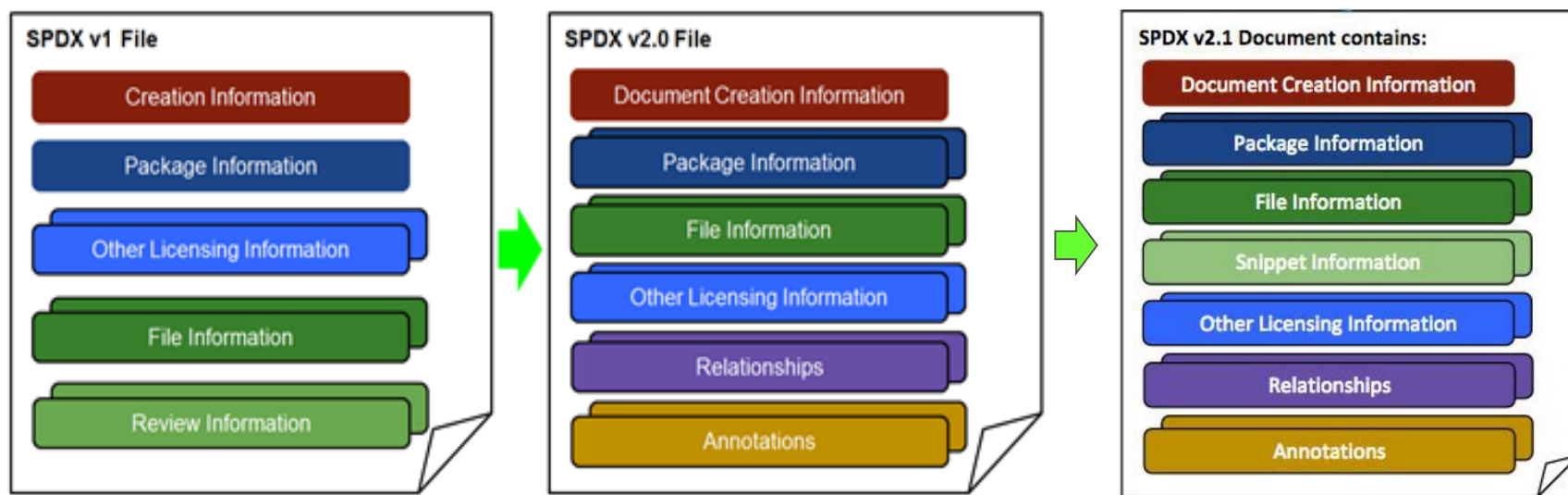
- Obtain details from
  - <http://spdx.org/participate>
  - [http://wiki.spdx.org/view/General\\_Meeting/Minutes](http://wiki.spdx.org/view/General_Meeting/Minutes)

# The status of SPDX Specification(1/2)

## History



## Features in SPDX



# The status of SPDX Specification(2/2)

Kernel v4.14(2017-11-17) added one-liners come from SPDX



The screenshot shows the GitHub interface for the Linux kernel source tree. The URL in the browser is <https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/tree/arch/arm64/kernel>. The page title is "index : kernel/git/torvalds/linux.git" and the subtitle is "Linux kernel source tree". The navigation tabs include "about", "summary", "refs", "log", "tree", "commit", "diff", and "stats". The path shown is "root/arch/arm64/kernel/Makefile". The blob ID is "0029e13adb596a6e470159f8e1682f5e5c7e1917 (plain)". The code content is as follows:

```
1 # SPDX-License-Identifier: GPL-2.0
2 #
3 # Makefile for the linux kernel.
4 #
5
6 CPPFLAGS_vmlinux.lds      := -DTEXT_OFFSET=$(TEXT_OFFSET)
7 AFLAGS_head.o             := -DTEXT_OFFSET=$(TEXT_OFFSET)
8 CFLAGS_armv8_deprecated.o := -I$(src)
9
10 CFLAGS_REMOVE_fttrace.o = -pg
11 CFLAGS_REMOVE_insn.o = -pg
12 CFLAGS_REMOVE_return_address.o = -pg
13
14 CFLAGS_setup.o = -DUTS_MACHINE="$(UTS_MACHINE)"
15
16 # Object file lists.
17 arm64-obj-y      := debug-monitors.o entry.o irq.o fpsimd.o
```

# Issue we met (1/2)

We met such an issue in checking CVE.

CVE-ID	
<b>CVE-2017-6512</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Race condition in the rmtree and remove_tree functions in the <a href="#">File-Path module before 2.13</a> for Perl allows attackers to set the mode on arbitrary files via vectors involving directory-permission loosening logic.	
References	
<b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none"><li>• <a href="http://cpansearch.perl.org/src/JKEENAN/File-Path-2.13/Changes">CONFIRM:http://cpansearch.perl.org/src/JKEENAN/File-Path-2.13/Changes</a></li><li>• <a href="https://rt.cpan.org/Ticket/Display.html?id=121951">CONFIRM:https://rt.cpan.org/Ticket/Display.html?id=121951</a></li></ul>	

But it is difficult to judge the version of perl spdx file.

```
$ grep File-Path perl-5.24.1.spdx
FileName: ./cpan/File-Path/lib/File/Path.pm
FileName: ./cpan/File-Path/t/FilePathTest.pm
FileName: ./cpan/File-Path/t/Path.t
FileName: ./cpan/File-Path/t/Path_root.t
FileName: ./cpan/File-Path/t/Path_win32.t
FileName: ./cpan/File-Path/t/taint.t
```

# Issue we met (2/2)

We met another issue in checking CVE.

CVE-ID	
<b>CVE-2017-11164</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
In PCRE 8.41, the OP_KETRMATCH feature in the match function in <code>pcre_exec.c</code> allows stack exhaustion (uncontrolled recursion) when processing a crafted regular expression.	
References	
<b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none"><li>• <a href="http://openwall.com/lists/oss-security/2017/07/11/3">MISC:http://openwall.com/lists/oss-security/2017/07/11/3</a></li><li>• <a href="#">BID:99575</a></li><li>• <a href="http://www.securityfocus.com/bid/99575">URL:http://www.securityfocus.com/bid/99575</a></li></ul>	
Assigning CNA	
MITRE Corporation	
Date Entry Created	
<b>20170710</b>	Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does

```
$ grep pcre glib-2.0-2.50.3.spdx
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-file-pcre_h-a607-c18ce65f
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-file-pcre_byte_order_c-8b9c-fa7dc829
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-file-pcre_chartables_c-3397-ca3605c6
.....
```

# meta-spdxscanner in Yocto

- What is Yocto
- SPDX in Yocto
  - Status of spdx.bbclass
  - Our team contribution for Yocto-SPDX
- meta-spdxscanner
- Features in meta-spdxscanner
- How to use meta-spdxscanner



# What is Yocto

https://www.yoctoproject.org

LINUX FOUNDATION COLLABORATIVE PROJECTS

yocto PROJECT


ABOUT  
ECOSYSTEM  
DOWNLOADS  
TOOLS + RESOURCES  
DOCUMENTATION

**New to the Project**  
Want to learn more, or just kick the tires? Start here.

START HERE TO LEARN MORE ▼

Introducing the Yocto Project

SEARCH embedded linux Go



**It's not an embedded Linux distribution – it creates a custom one for you**

The Yocto Project is an open source collaboration project that provides templates, tools and methods to help you create custom Linux-based systems for embedded products regardless of the hardware architecture. [Read more](#)

read the **Yocto Project Background** >

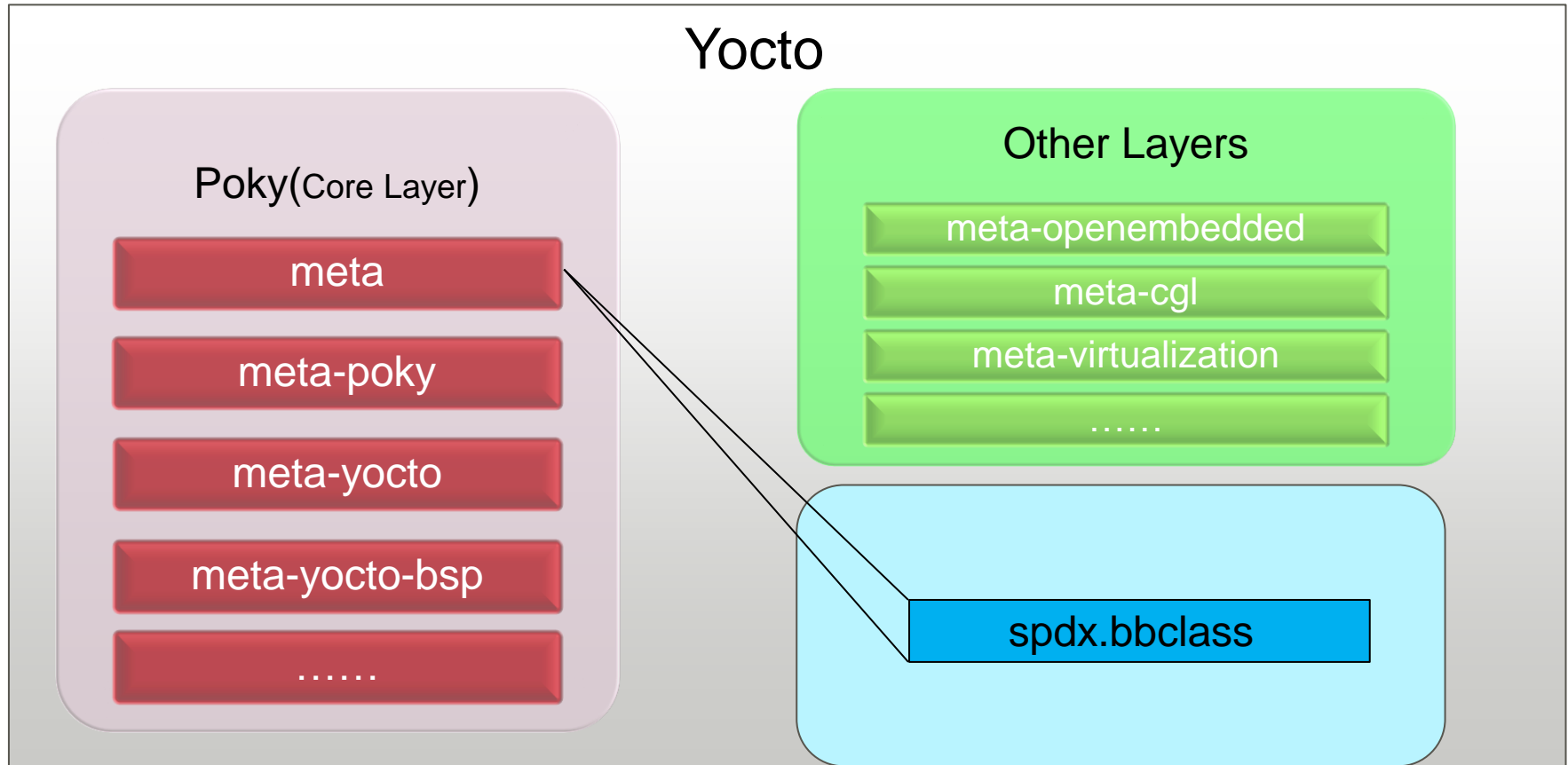
learn about Toaster, the Yocto Project Graphical UI >

register for developer day at ELC in Berlin >

**The Yocto Project is an open source collaboration project that help you create custom Linux-based systems for embedded products**

<https://www.yoctoproject.org/>

# SPDX in Yocto (1/2)



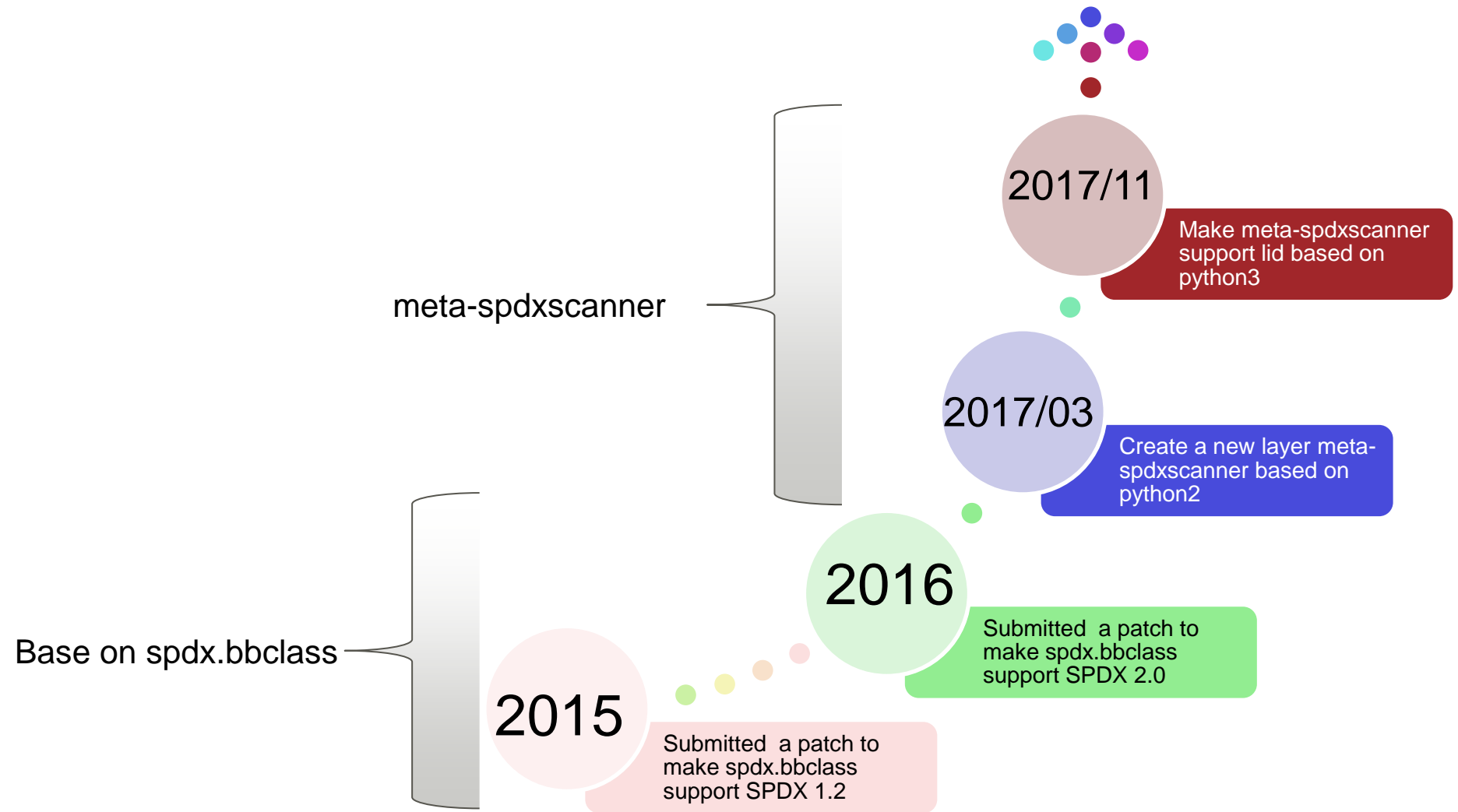
Bitbake taskflow





- Yocto+SPDX is not very compliant with SPDX Specification.
- Can't get package information
- Only support python2
- Only support fossology2.
- Hard to use, you have to set up the fossology2 server.

# Our team contribution for Ycoto-SPDX



# meta-spdxscanner (1/3)

## meta-spdxscanner

- Git Repository: <https://github.com/dl9pf/meta-spdxscanner>
- Our contribution to make Yocto+SPDX support SPDX2.0
- Project Activity: Maintained by our team.

← → ↻ ① layers.openembedded.org/layerindex/branch/master/layers/

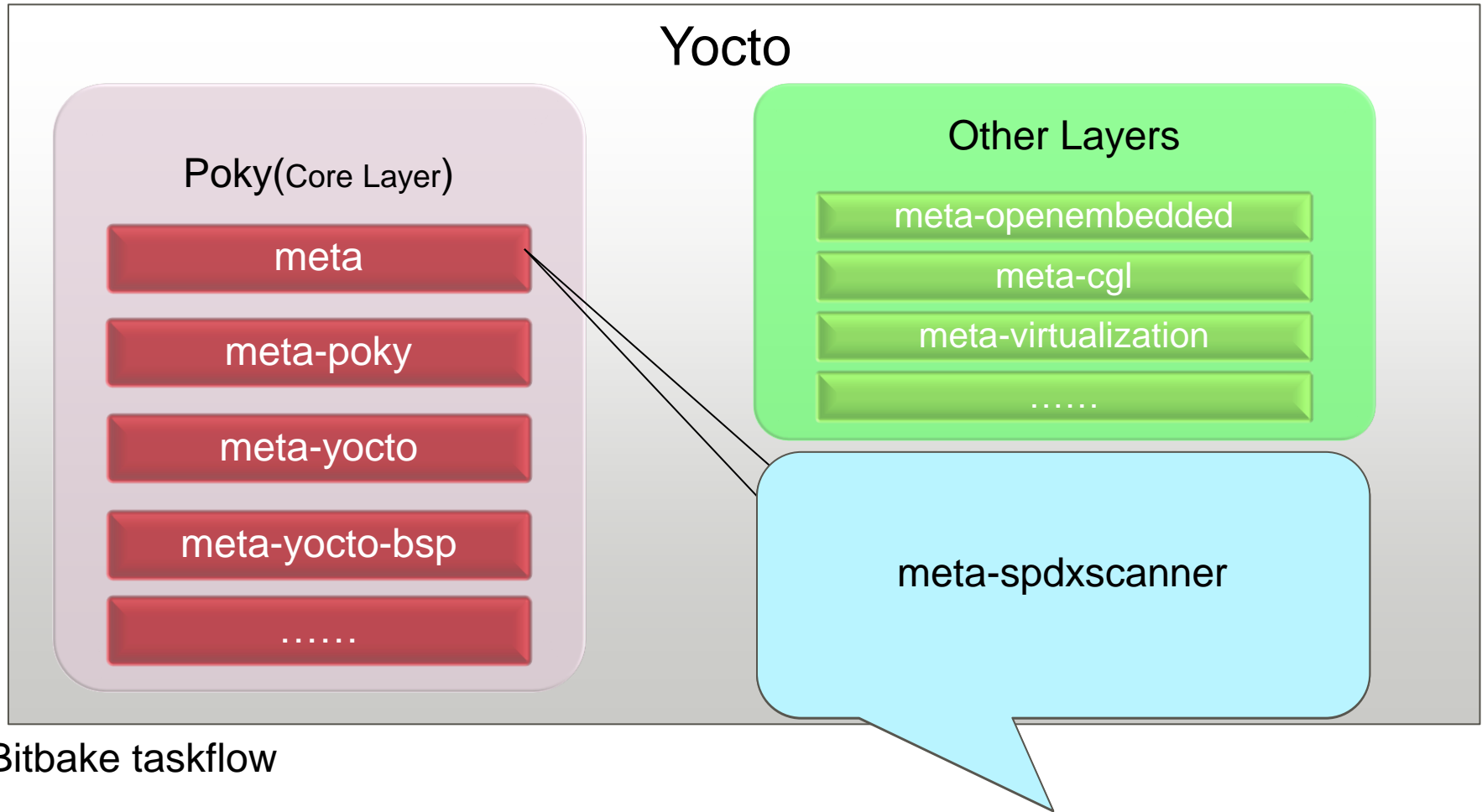
OpenEmbedded Layer Index Submit layer

Branch: master ▾ Layers Recipes Machines Distros

Meta-spdxscanner Filter layers ▾

Layer name	Description	Type	Repository
<a href="#">meta-spdxscanner</a>	spdx support	Distribution	<a href="https://github.com/dl9pf/meta-spdxscanner">https://github.com/dl9pf/meta-spdxscanner</a>

[change history](#) • [about this site](#) • [FAQ](#)

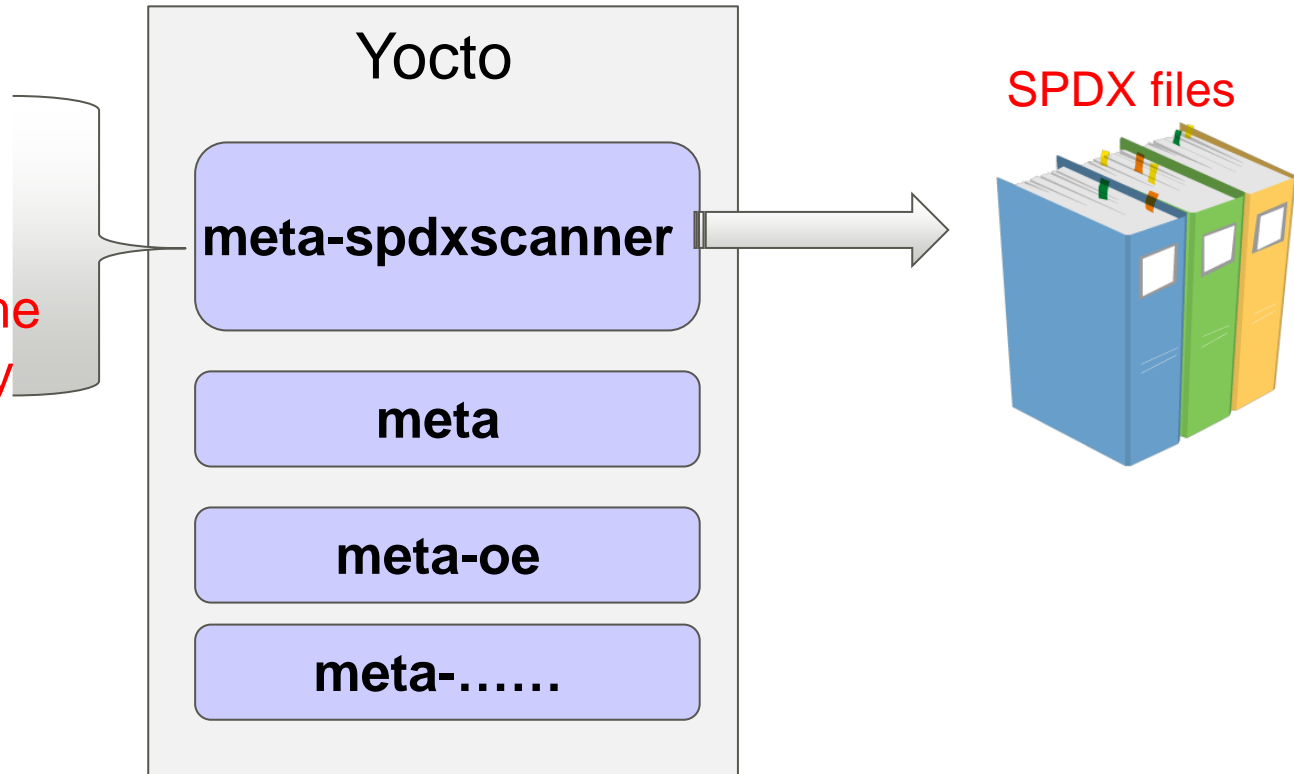


Bitbake taskflow



■ FOSS

□ Patches come from 3<sup>rd</sup> party



## Meta-spxscanner

class

lid-scan.bbclass

dosocs.bbclass

recipes

python3-dosocs2

fossology-nomos

python-lid

.....

bbappend

perl  
glib  
.....

Supports dosocsv2

Supports LiD

Can work with Yocto 2.3

More relationship information

Support SPDX 2.0

## What is DoSOCSv2

- dosocsv2 is a command-line tool for managing SPDX 2.0 documents and data. ([Website](#))
- By default, DoSOCSv2 uses nomos comes from fossology as it's license scanner.

## What is LiD

- Qualcomm OSTG (Open Source Technology Group) **LiD** (License Identifier) tool scans source code and identifies the license and the license text region using a standard set of license templates from sources like SPDX. ([Website](#))

# Dosocsv2 vs LiD (1/3)

## File format

- File created by Dosocsv2 is compliance with SPDX2.0
- File created by LiD isn't compliance with SPDX

```
$ dosocs2 oneshot cpio-2.11
dosocs2: cpio-2.11: package_id: 1
dosocs2: running nomos on package 1
cccccpio-2.11: document_id: 1
```

### SPDXVersion: SPDX-2.0

```
DataLicense: CC0-1.0
DocumentNamespace:
sqlite:///home/leimh/.config/dosocs2/dosocs2.sqlite3/cpio-2.11-fe30375e-3a43-
4d1e-9962-eb24f2dbe8bf
DocumentName: cpio-2.11
SPDXID: SPDXRef-DOCUMENT
DocumentComment: <text></text>
```

#### ## External Document References

#### ## Creation Information

```
Creator: Tool: dosocs2-0.16.1
Created: 2016-07-09T23:18:52Z
CreatorComment: <text></text>
```

### LicenseListVersion: 2.2

#### ## Document Annotations

#### ## Document Relationships

```
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-package-
cpio_2_11-f6eb-4fa85311
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-file-ABOUT-NLS-
b502-579bb6d1
.....
```

```
$ license-identifier -l /home/test/zlib-1.2.11 | less
=== Found 0 results for '/home/test/zlib-1.2.11/CMakeLists.txt':
=== Found 0 results for '/home/test/zlib-1.2.11/ChangeLog':
=== Found 3 results for '/home/test/zlib-1.2.11/FAQ':
```

#### Summary of the analysis

Name of the input file: /home/test/zlib-1.2.11/FAQ

Matched license type is Vim

Score for the match is 0.0513

Rank for the match is ScoreOutOfRange

License text beings at line 343.

License text ends at line 364.

Start byte offset for the license text is 15451.

End byte offset for the license text is 16418.

The found license text has the score of 0.00108

The following text is found to be license text

-----BEGIN-----

41. I'm having a problem with the zip functions in zlib, can you help?

There are no zip functions in zlib. You are probably using minizip by Giles Vollant, which is found in the contrib directory of zlib. It is not part of zlib. In fact none of the stuff in contrib is part of zlib. The files in there are not supported by the zlib authors. You need to contact the authors of the respective contribution for help.

42. The match.asm code in contrib is under the GNU General Public License. Since it's part of zlib, doesn't that mean that all of zlib falls under the GNU GPL?

.....



## License Text Region Identification

- Nomos (the scanner used by default in Dosocsv2) finds snippets
- LiD finds the whole license text

```
$ FileName: ./contrib/iostream2/zstream.h
SPDXID: SPDXRef-file-zstream_h-d034-fcdf1afd
FileType: SOURCE
FileChecksum: SHA256:
d0343e0c57ff58008b6f29643d289c72713aa2d653fe3dcd2e939fc77e7e20b6
LicenseConcluded: NOASSERTION
LicenseInfoInFile: LicenseRef-MIT-style
LicenseComments: <text></text>
.....
```

```
LicenseID: LicenseRef-MIT-style
LicenseName: MIT-style
ExtractedText: <text>b'Permission to use, copy, modify, distribute and sell this
software¥n * and its documentation for any purpose is hereby granted without
fee,¥n * provided that the above copyright notice appear in all copies'</text>
LicenseCrossReference:
LicenseComment: <text>found by nomos</text>
```

```
$ license-identifier -l /home/test/zlib-1.2.11 | less
Name of the input file: /yocto/work001/build/poky/build-poky-dnf/tmp/work/i586-
poky-linux/zlib/1.2.11-r0/zlib-1.2.11/contrib/iostream2/zstream.h
Matched license type is NTP
Score for the match is 0.269
Rank for the match is 3
License text beings at line 2.
License text ends at line 15.
Start byte offset for the license text is 6.
End byte offset for the license text is 642.
The found license text has the score of 0.027The following text is found to be
license text
-----BEGIN-----
* Copyright (c) 1997
* Christian Michelsen Research AS
* Advanced Computing
* Fantoftvegen 38, 5036 BERGEN, Norway
* http://www.cmr.no
*
* Permission to use, copy, modify, distribute and sell this software
* and its documentation for any purpose is hereby granted without fee,
* provided that the above copyright notice appear in all copies and
* that both that copyright notice and this permission notice appear
* in supporting documentation. Christian Michelsen Research AS makes no
* representations about the suitability of this software for any
* purpose. It is provided "as is" without express or implied warranty.
-----END-----
```

# Dosocsv2 vs LiD (3/3)

Item	DoSOCSv2	LiD
License	GPLv2	BSD-3-Clause
Can create SPDX files	SPDX 2.0	-
Include whole license text	-	√
Performance (e.g. zlib-1.2.11)	1min(1st) 5s(2nd)	21min
scanner	Fossology(nomos)	LiD
Project Activity ( <a href="http://www.openhub.net">http://www.openhub.net</a> )	Very Low	Low
GUI	-	-
Command Line	√	√

# Can work with Yocto 2.3

## Build system

~ Yocto 2.2

python-lxml

python-py

python-cryptography

python-...

**Python2**

make

tar

unzip

wget

.....



## Build system

Yocto 2.3 ~

python3-lxml

python3-py

python3-cryptography

python3-...

**Python3**

make

tar

unzip

wget

.....

## Meta-spxscanner

python-dosocs2

python-magic

python-dosocs2

python-...



## Meta-spxscanner

python3-dosocs2

python3-magic

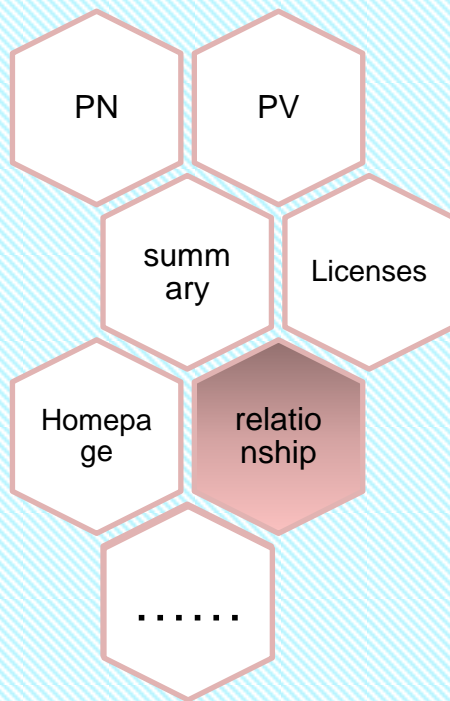
python3-dosocs2

python3-...

# More relationship information (1/2)

More useful relationship informations are add into meta-spdxscanner.

You can get informations such as :



➤ Issue-1 can be resolved

```
$ grep File-Path perl-5.24.1.spdx
Relationship: perl CONTAINS File-Path-2.12
FileName: ./cpan/File-Path/lib/File/Path.pm
FileName: ./cpan/File-Path/t/FilePathTest.pm
FileName: ./cpan/File-Path/t/Path.t
FileName: ./cpan/File-Path/t/Path_root.t
FileName: ./cpan/File-Path/t/Path_win32.t
FileName: ./cpan/File-Path/t/taint.t
```

➤ Issue-2 can be resolved

```
$ grep pcre glib-2.0-2.50.3.spdx
Relationship: glib STATIC_LINK system-pcre
Relationship: SPDXRef-DOCUMENT DESCRIBES
SPDXRef-file-pcre_h-a607-c18ce65f
Relationship: SPDXRef-DOCUMENT DESCRIBES
SPDXRef-file-pcre_byte_order_c-8b9c-fa7dc829
Relationship: SPDXRef-DOCUMENT DESCRIBES
SPDXRef-file-pcre_chartables_c-3397-ca3605c6
.....
```

- Generate SPDX File from Yocto building.

## ④ Start building

- `$ cd [yocto_build_dir]`
- `$ bitbake core-image-minimal`

## ③ Enable dosocs.bbclass

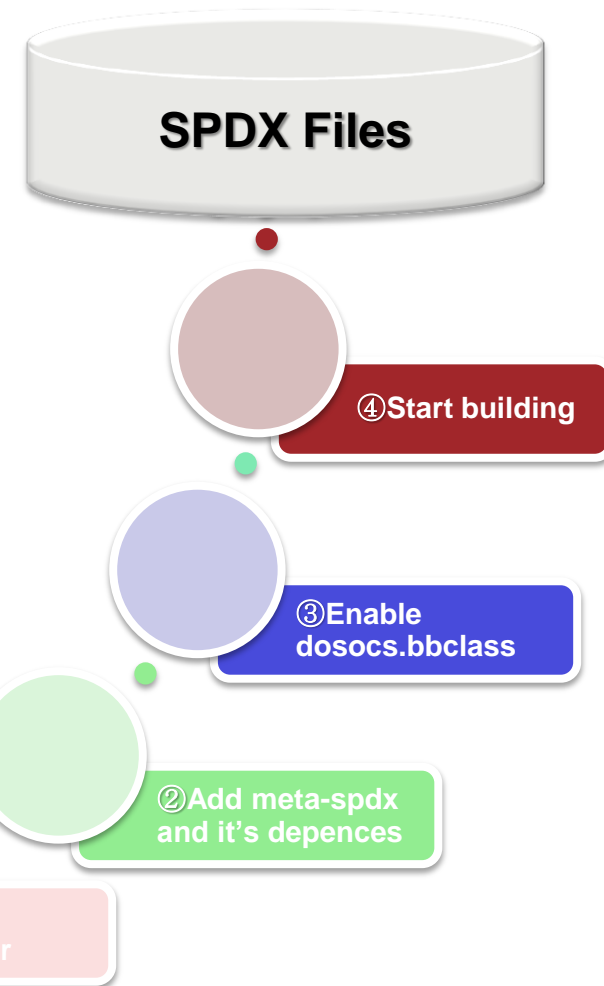
- `$ cd [yocto_build_dir]`
- `$ tail -n 4 conf/local.conf`  
    `INHERIT += "dosocs"`
- `ARCHIVER_MODE[src] = "patched"`
- `SPDX_DEPLOY_DIR = "/yocto/build/poky/build-poky/spdx-out"`

## ② Add meta-spdx and it's depences

- `$ cd [yocto_build_dir]`
- `$ tail -n 3 conf/conf/bblayers.conf`  
    `/yocto/community/meta-spdxscanner ¥`
- `/yocto/community/meta-openembedded/meta-oe ¥`
- `/yocto/community/meta-openembedded/meta-python ¥`

## ① get meta-spdxscanner

- `$ git clone https://github.com/dl9pf/meta-spdxscanner`



# Manage SPDX files

- Manage SPDX files by dnf in your ecosystem
- SPDX file works in OpenChain
  - What is OpenChain
  - Make SPDX files work in OpenChain
- Future work

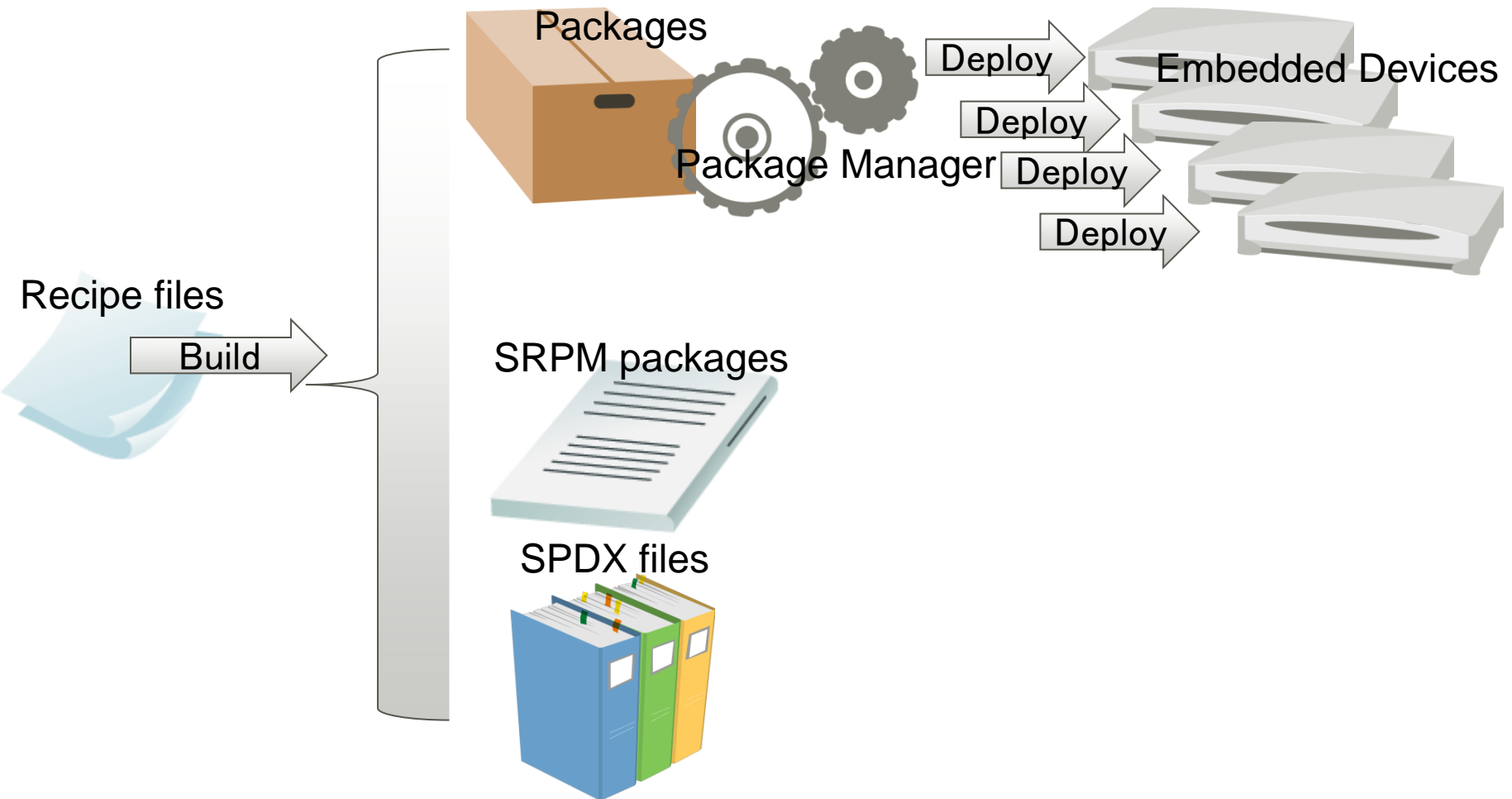
## What is DNF

- **DNF** is a software package manager that installs, updates, and removes [packages](#) on [RPM](#)-based Linux distributions. It automatically computes dependencies and determines the actions required to install packages. DNF also makes it easier to maintain groups of machines, eliminating the need to manually update each one using [rpm](#). Introduced in Fedora 18, it has been the default package manager since Fedora 22.

## Why Yum was forked into DNF

- An undocumented API—this meant more work for developers. In order for developers to do what they needed, it was often necessary to browse through the Yum code base just to be able to write a call. This meant development was very slow.
- Python 3—Fedora was about to make the shift to Python 3 and Yum wouldn't survive this change, whereas DNF can run using either Python 2 or 3.
- Broken dependency solving algorithm—this has been an Achilles heel of the Fedora package manager for a long time. DNF uses a state-of-the-art satisfiability (SAT)-based dependency solver. This is the same type of dependency solver used in SUSE's and openSUSE's Zypper.

# Manage SPDX files by dnf in your ecosystem(1/2)



- Accompanied with the package files and SRPM packages, SPDX files are created to manage license information.



## There is a Demo!

You can reference to:

<https://github.com/ubinux/dnf/tree/dnf-yocto-dev>

## What is OpenChain

- The **OpenChain** Project helps to identify and share the core components of a high quality Free and Open Source Software (FOSS) compliance program. OpenChain builds trust in Open Source by making things simpler, more efficient and more consistent. It is the industry-standard for managing Open Source compliance across the supply chain. ([Website](#))
- OpenChain aims to help companies avoid potential pitfalls in the compliance process:
  1. Intellectual Property (IP) pitfalls
  2. License Compliance pitfalls
  3. Compliance Process pitfalls



# What is OpenChain (2/2)

## OpenChain Conformant Organizations



>\_ ENDOCODE

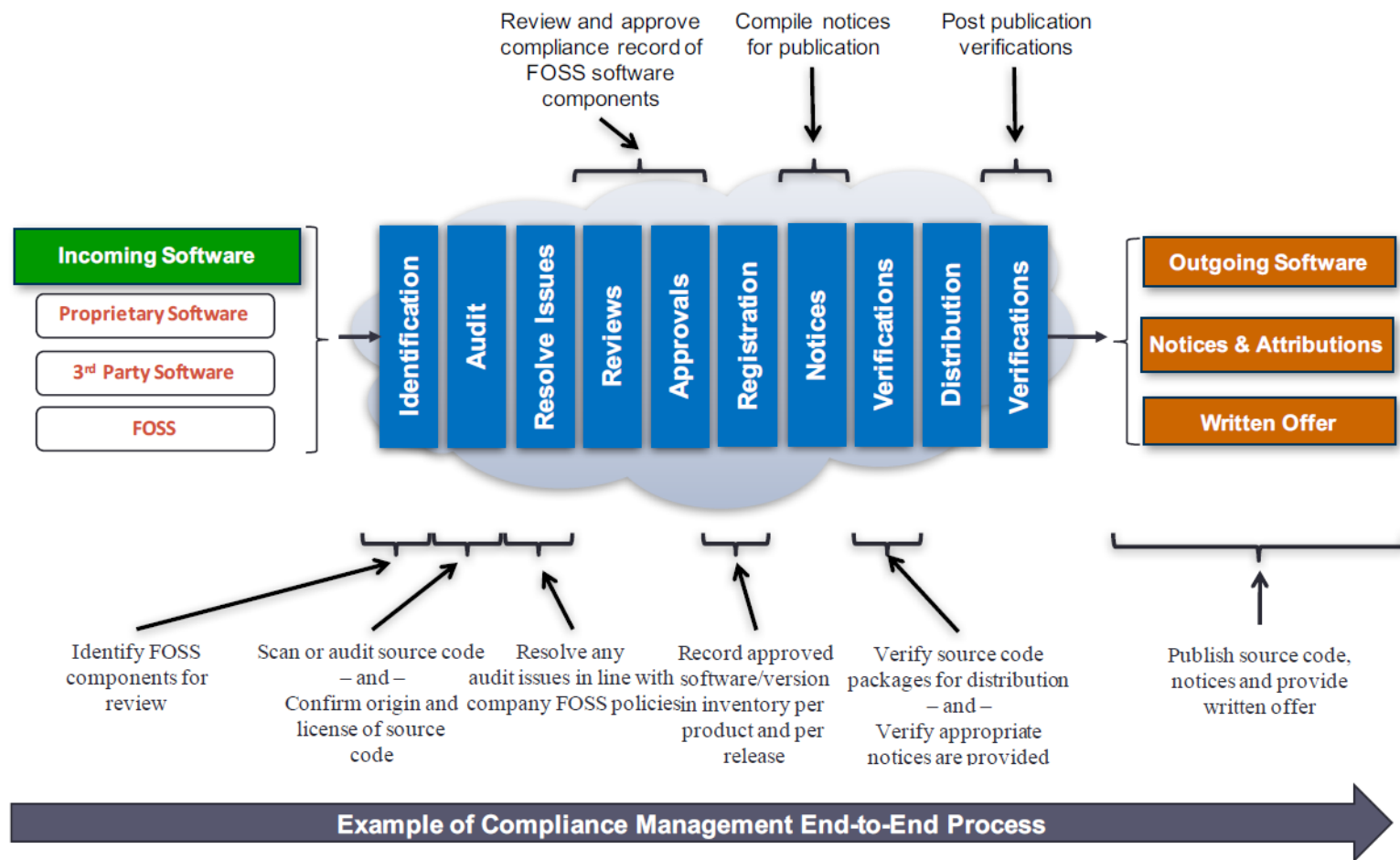


GE Digital



# Make SPDX files work in OpenChain

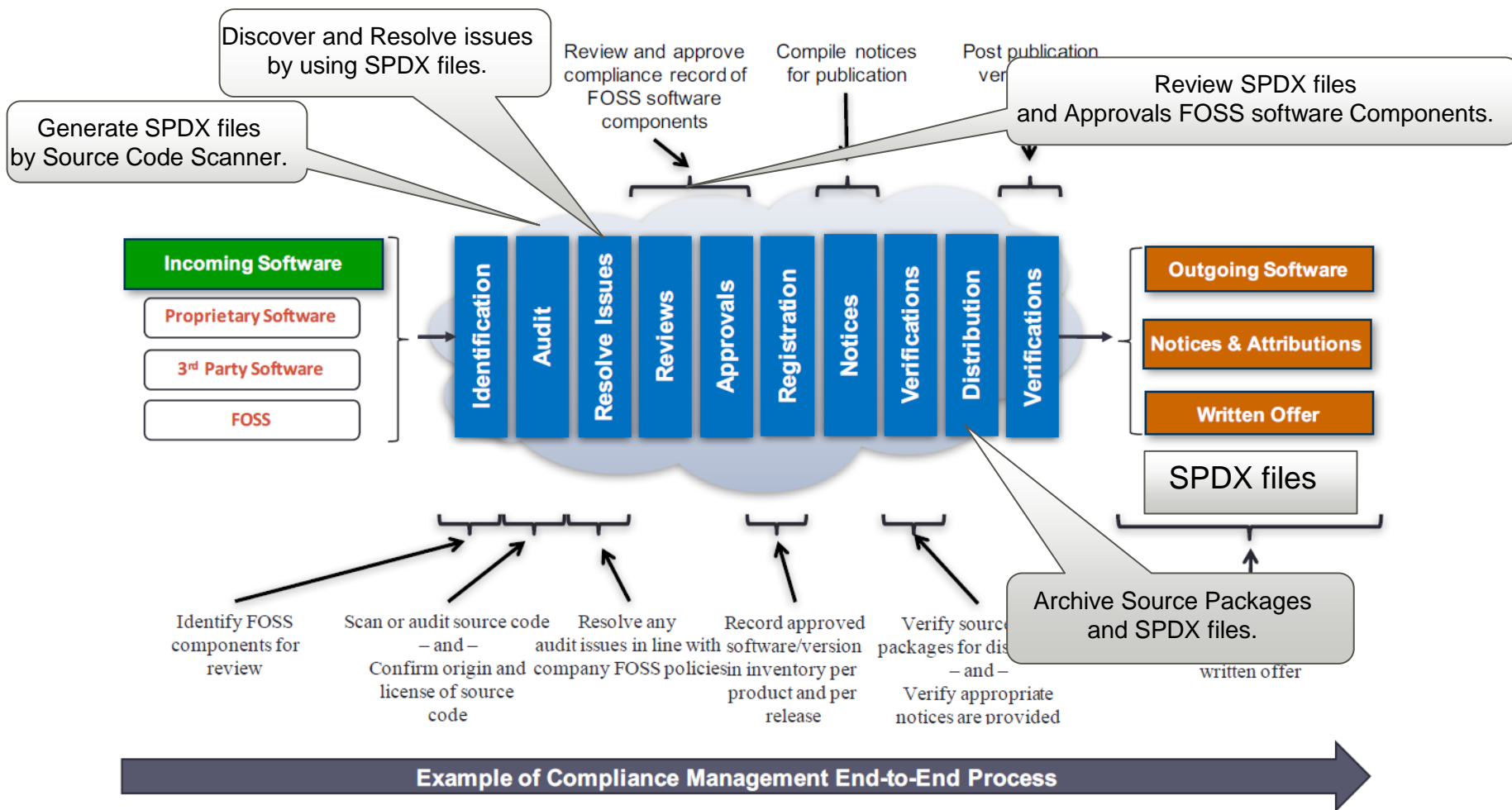
an example of an enterprise process comes from OpenChain



[https://wiki.linuxfoundation.org/\\_media/openchain/openchain-curriculum-for-1-1.pdf](https://wiki.linuxfoundation.org/_media/openchain/openchain-curriculum-for-1-1.pdf)

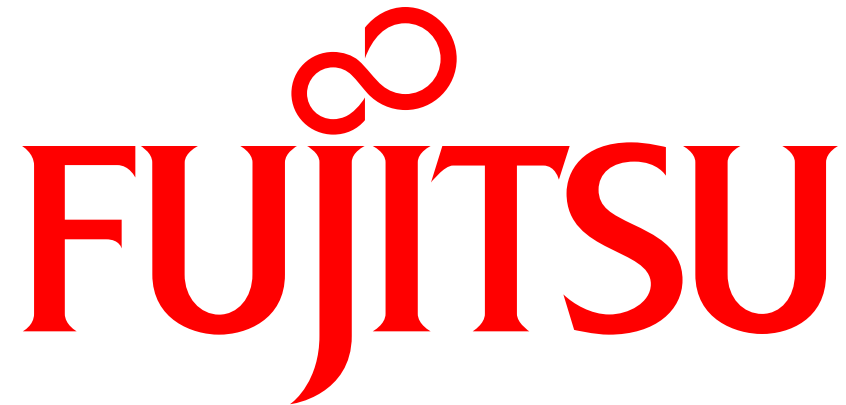
# Make SPDX files work in OpenChain

an example of an enterprise process comes from OpenChain



- Make dnf-host support UI.
- Submit dnf patch to Yocto.
- Add more SPDX sanners into meta-spdxscanner.
- Go on adding useful relationship informations into meta-spdxscanner.
- Release meta-spdxscanner following the step of Yocto.

# Any Questions?



shaping tomorrow with you