# Describing License Information in SPDX

## It’s Easier than you think

Gary O’Neall, Source Auditor Inc.

# Agenda

- What is SPDX, who is using it, and why?
- The complex – examples of SPDX documents
- A simple start – using SPDX license ID’s
  - Overview of the SPDX license list
  - Including license identifiers in your source code
  - Tools to support using license IDs
- A bit more work – SPDX documents for original source
  - Example of an SPDX document
  - Tools to support creating SPDX document
- Advanced SPDX usage – automating your supply chain
- Questions

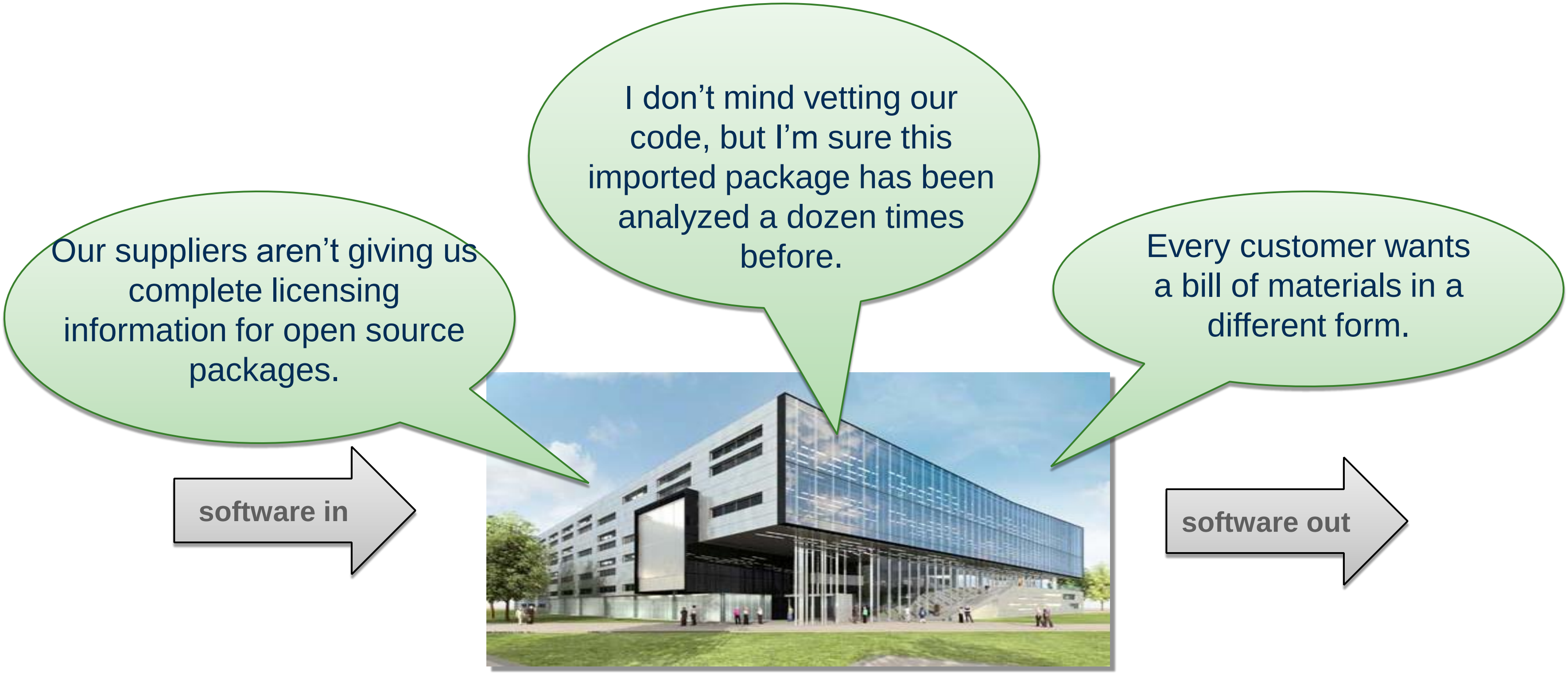
# What is SPDX?

- Standard:
  - A standard format for communicating the components, licenses and copyrights associated with a software package
- Guiding principles:
  - Human and machine readable
  - Focus on capturing facts; avoid interpretations
- Vision:
  - To help reduce redundant work in determining software license information and facilitate compliance

# Who is using SPDX?

- SPDX has over 20 active participants
- Active participation by organizations in the middle of the software supply chain (e.g. TI, HP, Wind River, Samsung)
- Tools providers are incorporating SPDX for import and export of software “Bill of Materials”
- Consultants using the format as a standard output
- Open source projects using the SPDX license identifiers (e.g. Das U-Boot, Ruby projects, GitHub)

# Why SPDX



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.

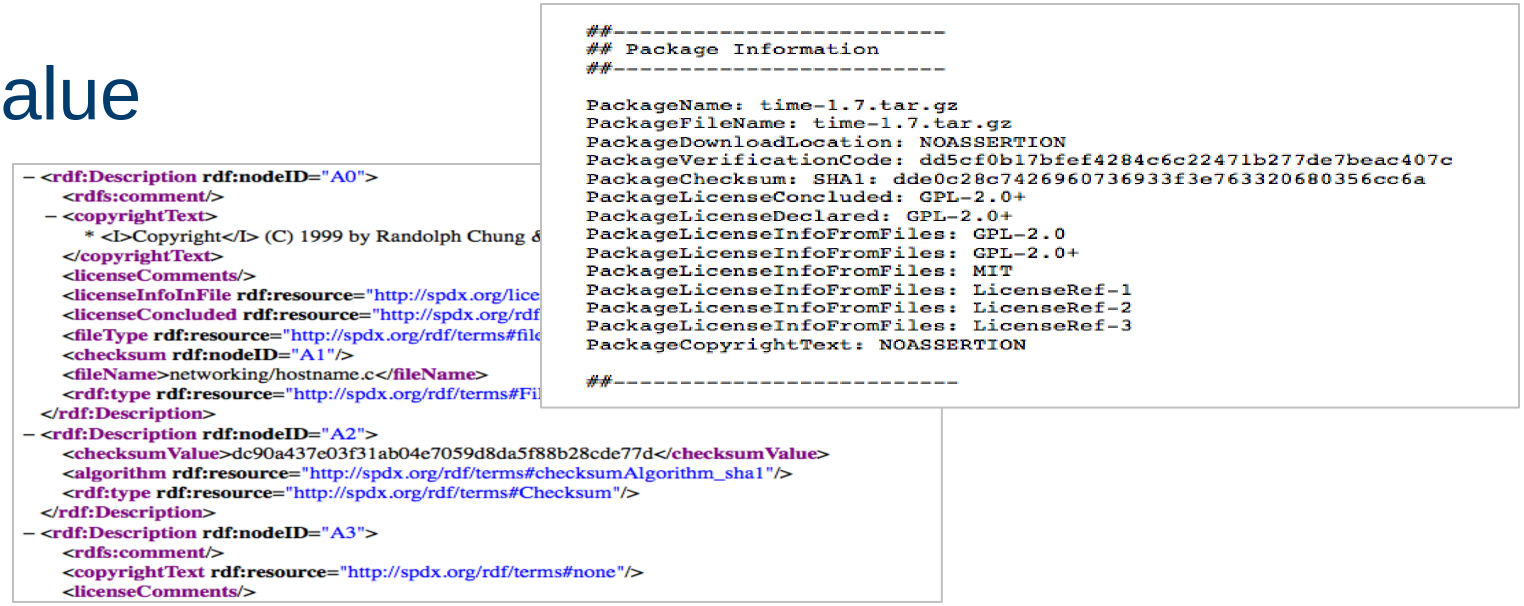
Every customer wants a bill of materials in a different form.

software in

software out

# Example SPDX document Formats

- Tag/Value

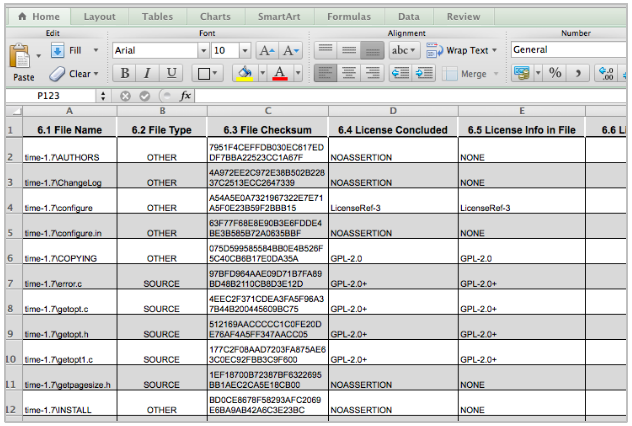


```
##-------------------------
## Package Information
##-------------------------

PackageName: time-1.7.tar.gz
PackageFileName: time-1.7.tar.gz
PackageDownloadLocation: NOASSERTION
PackageVerificationCode: dd5cf0b17bfef4284c6c22471b277de7beac407c
PackageChecksum: SHA1: dde0c28c7426960736933f3e763320680356cc6a
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

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

```
– <rdf:Description rdf:nodeID="A0">
    <rdfs:comment/>
  – <copyrightText>
      * <I>Copyright</I> (C) 1999 by Randolph Chung &
    </copyrightText>
    <licenseComments/>
    <licenseInfoInFile rdf:resource="http://spdx.org/lice
    <licenseConcluded rdf:resource="http://spdx.org/rdf
    <fileType rdf:resource="http://spdx.org/rdf/terms#file
    <checksum rdf:nodeID="A1"/>
    <fileName>networking/hostname.c</fileName>
    <rdf:type rdf:resource="http://spdx.org/rdf/terms#Fil
  </rdf:Description>
– <rdf:Description rdf:nodeID="A2">
    <checksumValue>dc90a437e03f31ab04e7059d8da5f88b28cde77d</checksumValue>
    <algorithm rdf:resource="http://spdx.org/rdf/terms#checksumAlgorithm_sha1"/>
    <rdf:type rdf:resource="http://spdx.org/rdf/terms#Checksum"/>
  </rdf:Description>
– <rdf:Description rdf:nodeID="A3">
    <rdfs:comment/>
    <copyrightText rdf:resource="http://spdx.org/rdf/terms#none"/>
    <licenseComments/>
```

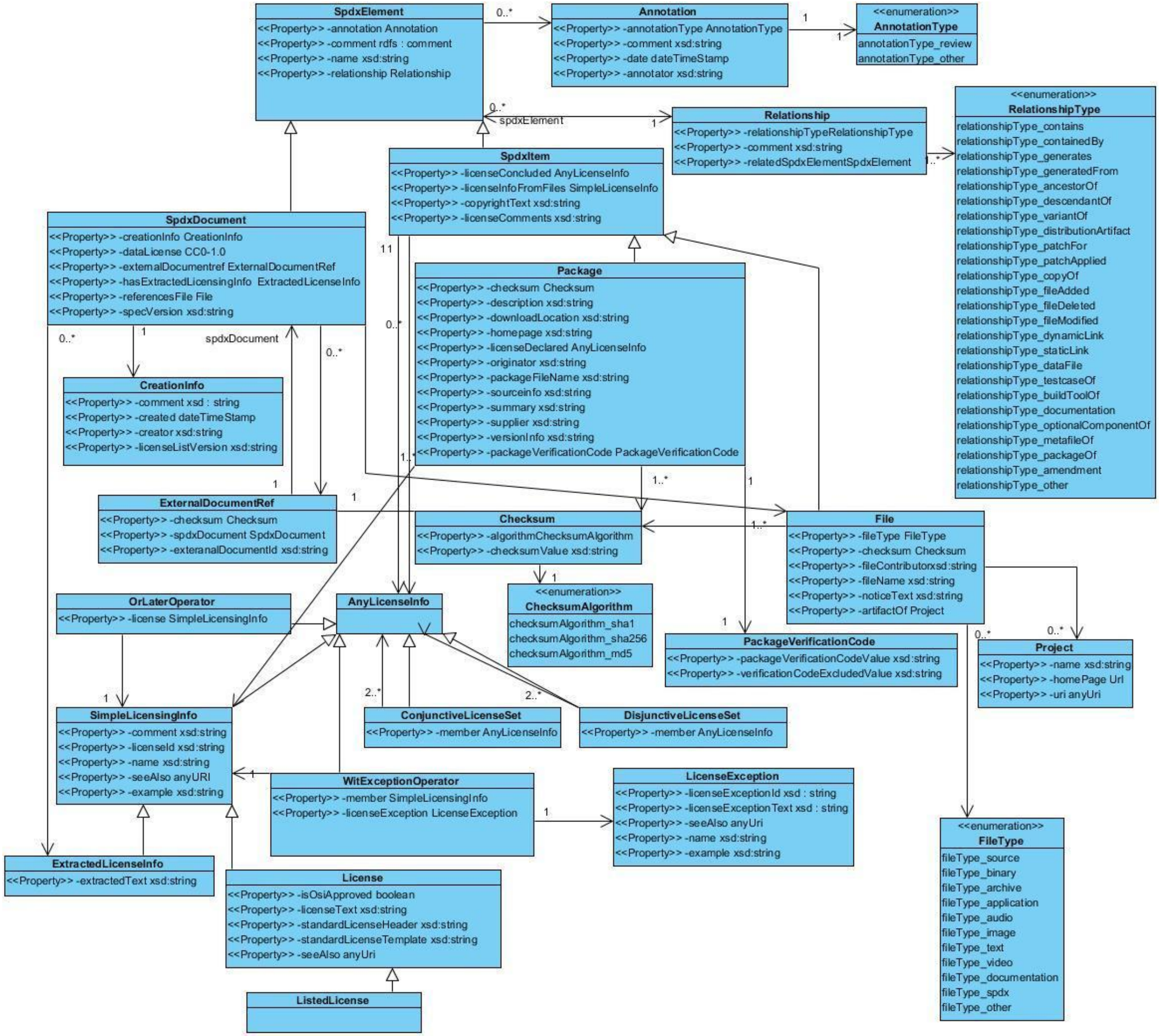
- RDF

- Spreadsheet



| | A | B | C | D | E | |
|---|---|---|---|---|---|---|
| 1 | 6.1 File Name | 6.2 File Type | 6.3 File Checksum | 6.4 License Concluded | 6.5 License Info in File | 6.6 L |
| 2 | time-1.7\AUTHORS | OTHER | 7951F4CEFFDB030EC617ED<br>DF7BBA22523CC1A67F | NOASSERTION | NONE | |
| 3 | time-1.7\ChangeLog | OTHER | 4A972EE2C972E38B502B228<br>37C2513ECC2647339 | NOASSERTION | NONE | |
| 4 | time-1.7\configure | OTHER | A54A5E0A7321967322E7E71<br>A5F0E23B59F2BBB15 | LicenseRef-3 | LicenseRef-3 | |
| 5 | time-1.7\configure.in | OTHER | 63F77F68E8E90B3E6FDDE4<br>BE3B585B72A0635BBF | NOASSERTION | NONE | |
| 6 | time-1.7\COPYING | OTHER | 075D599585584BB0E4B526F<br>5C40CB6B17E0DA35A | GPL-2.0 | GPL-2.0 | |
| 7 | time-1.7\error.c | SOURCE | 97BFD964AAE09D71B7FA89<br>BD48B2110CB8D3E12D | GPL-2.0+ | GPL-2.0+ | |
| 8 | time-1.7\getopt.c | SOURCE | 4EEC2F371CDEA3FA5F96A3<br>7B44B200445609BC75 | GPL-2.0+ | GPL-2.0+ | |
| 9 | time-1.7\getopt.h | SOURCE | 512169AACCCCC1C0FE20D<br>E76AF4A5FF347AACC05 | GPL-2.0+ | GPL-2.0+ | |
| 10 | time-1.7\getopt1.c | SOURCE | 177C2F08AAD7203FA875AE6<br>3C0EC92FBB3C9F600 | GPL-2.0+ | GPL-2.0+ | |
| 11 | time-1.7\getpagesize.h | SOURCE | 1EF18700B72387BF6322695<br>BB1AEC2CA5E18CB00 | NOASSERTION | NONE | |
| 12 | time-1.7\INSTALL | OTHER | BD0CE8678F58293AFC2069<br>E6BA9AB42A6C3E23BC | NOASSERTION | NONE | |

# The Big (and complex) Picture



SpdxElement
<<Property>> -annotation Annotation
<<Property>> -comment rdfs : comment
<<Property>> -name xsd:string
<<Property>> -relationship Relationship

Annotation
<<Property>> -annotationType AnnotationType
<<Property>> -comment xsd:string
<<Property>> -date dateTimeStamp
<<Property>> -annotator xsd:string

<<enumeration>>
AnnotationType
annotationType_review
annotationType_other

Relationship
<<Property>> -relationshipTypeRelationshipType
<<Property>> -comment xsd:string
<<Property>> -relatedSpdxElementSpdxElement

<<enumeration>>
RelationshipType
relationshipType_contains
relationshipType_containedBy
relationshipType_generates
relationshipType_generatedFrom
relationshipType_ancestorOf
relationshipType_descendantOf
relationshipType_variantOf
relationshipType_distributionArtifact
relationshipType_patchFor
relationshipType_patchApplied
relationshipType_copyOf
relationshipType_fileAdded
relationshipType_fileDeleted
relationshipType_fileModified
relationshipType_dynamicLink
relationshipType_staticLink
relationshipType_dataFile
relationshipType_testcaseOf
relationshipType_buildToolOf
relationshipType_documentation
relationshipType_optionalComponentOf
relationshipType_metafileOf
relationshipType_packageOf
relationshipType_amendment
relationshipType_other

SpdxItem
<<Property>> -licenseConcluded AnyLicenseInfo
<<Property>> -licenseInfoFromFiles SimpleLicenseInfo
<<Property>> -copyrightText xsd:string
<<Property>> -licenseComments xsd:string

SpdxDocument
<<Property>> -creationInfo CreationInfo
<<Property>> -dataLicense CC0-1.0
<<Property>> -externalDocumentref ExternalDocumentRef
<<Property>> -hasExtractedLicensingInfo ExtractedLicenseInfo
<<Property>> -referencesFile File
<<Property>> -specVersion xsd:string

Package
<<Property>> -checksum Checksum
<<Property>> -description xsd:string
<<Property>> -downloadLocation xsd:string
<<Property>> -homepage xsd:string
<<Property>> -licenseDeclared AnyLicenseInfo
<<Property>> -originator xsd:string
<<Property>> -packageFileName xsd:string
<<Property>> -sourceinfo xsd:string
<<Property>> -summary xsd:string
<<Property>> -supplier xsd:string
<<Property>> -versionInfo xsd:string
<<Property>> -packageVerificationCode PackageVerificationCode

CreationInfo
<<Property>> -comment xsd : string
<<Property>> -created dateTimeStamp
<<Property>> -creator xsd:string
<<Property>> -licenseListVersion xsd:string

ExternalDocumentRef
<<Property>> -checksum Checksum
<<Property>> -spdxDocument SpdxDocument
<<Property>> -exteranalDocumentId xsd:string

Checksum
<<Property>> -algorithmChecksumAlgorithm
<<Property>> -checksumValue xsd:string

File
<<Property>> -fileType FileType
<<Property>> -checksum Checksum
<<Property>> -fileContributorxsd:string
<<Property>> -fileName xsd:string
<<Property>> -noticeText xsd:string
<<Property>> -artifactOf Project

OrLaterOperator
<<Property>> -license SimpleLicensingInfo

AnyLicenseInfo

<<enumeration>>
ChecksumAlgorithm
checksumAlgorithm_sha1
checksumAlgorithm_sha256
checksumAlgorithm_md5

PackageVerificationCode
<<Property>> -packageVerificationCodeValue xsd:string
<<Property>> -verificationCodeExcludedValue xsd:string

Project
<<Property>> -name xsd:string
<<Property>> -homePage Url
<<Property>> -uri anyUri

SimpleLicensingInfo
<<Property>> -comment xsd:string
<<Property>> -licenseId xsd:string
<<Property>> -name xsd:string
<<Property>> -seeAlso anyURI
<<Property>> -example xsd:string

ConjunctiveLicenseSet
<<Property>> -member AnyLicenseInfo

DisjunctiveLicenseSet
<<Property>> -member AnyLicenseInfo

WitExceptionOperator
<<Property>> -member SimpleLicensingInfo
<<Property>> -licenseException LicenseException

LicenseException
<<Property>> -licenseExceptionId xsd : string
<<Property>> -licenseExceptionText xsd : string
<<Property>> -seeAlso anyUri
<<Property>> -name xsd:string
<<Property>> -example xsd:string

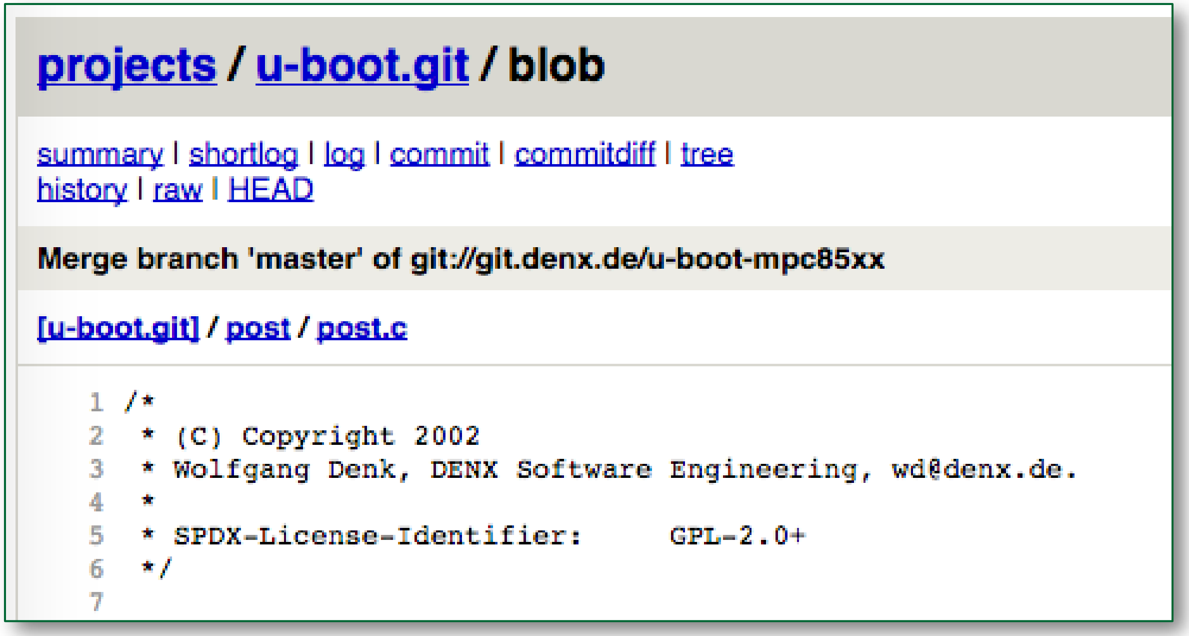
ExtractedLicenseInfo
<<Property>> -extractedText xsd:string

License
<<Property>> -isOsiApproved boolean
<<Property>> -licenseText xsd:string
<<Property>> -standardLicenseHeader xsd:string
<<Property>> -standardLicenseTemplate xsd:string
<<Property>> -seeAlso anyUri

ListedLicense

<<enumeration>>
FileType
fileType_source
fileType_binary
fileType_archive
fileType_application
fileType_audio
fileType_image
fileType_text
fileType_video
fileType_documentation
fileType_spdx
fileType_other

# Starting Simple:
# SPDX License List Identifiers



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

```
/*
 * (C) Copyright 2002
 * Wolfgang Denk, DENX Software Engineering, wd@denx.de.
 *
 * SPDX-License-Identifier:     GPL-2.0+
 */

```

# Advantages to License ID’s

- Reduces effort to determine the actual license used in a source file
- List of (common) open source* licenses
  - Over 300 licenses and over 20 common exceptions
- spdx.org/licenses contains the text, reference URL’s, templates for matching, whether OSI approved and headers
- Backed by an active organization which maintains the license list
- Matching guidelines to help determine if the license text matches the text

# More Info on the License List

- Human and machine readable at http://spdx.org/licenses
- RDFa machine readable access
- JSON file at http://spdx.org/licenses/licenses.json
- For tools support, see the tech report “Accessing SPDX Licenses”: http://spdx.org/publications/tool-documentation/accessing-spdx-licenses
- License ID’s in Source: http://wiki.spdx.org/view/Technical_Team/SPDX_Meta_Tags

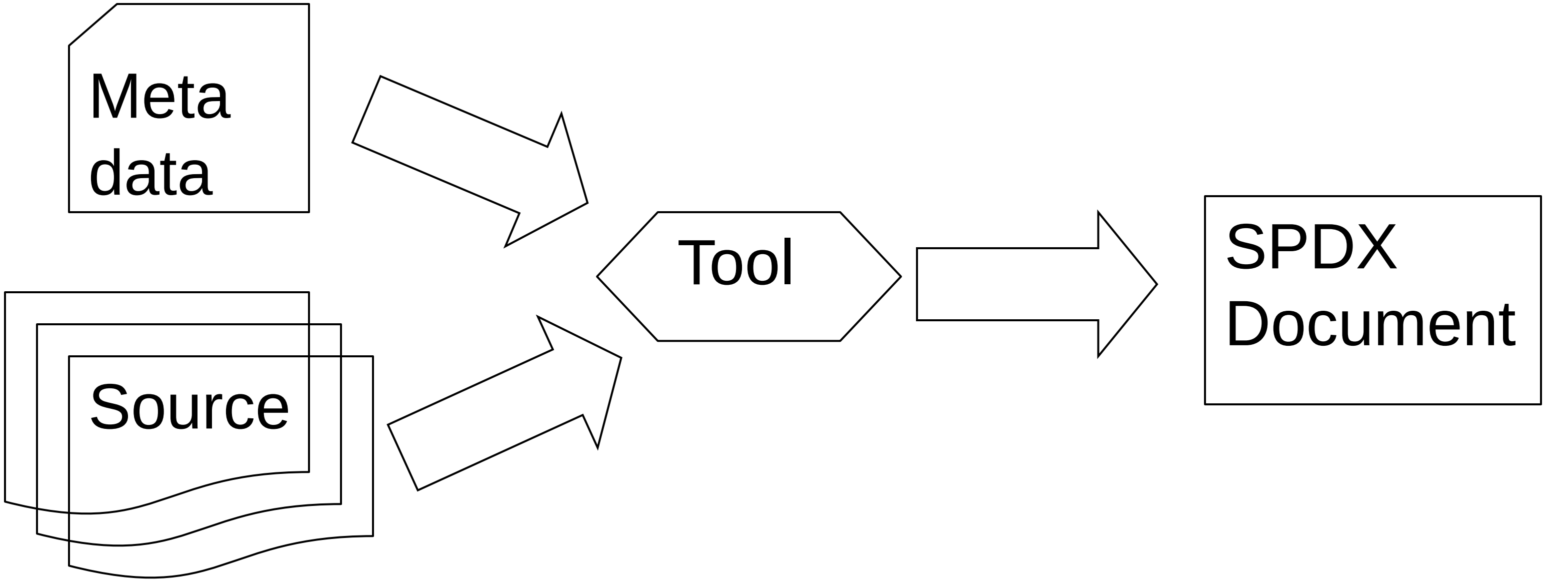
# A bit more work: Using License Expressions

- Expresses a combination of licenses (e.g. “Dual Licensing”)
- AND – Conjunctive licenses
- OR – Disjunctive licenses
- With – Exceptions
- + - Or later versions

# Examples

- Example: GPL-2.0+ OR MIT – Early versions jQuery
- Example: GPL-2.0-with-autoconf-exception AND GPL-3.0+ AND LGPL-2.1+ AND GPL-2.0+
- Example: (GPL-2.0+ OR MIT) AND BSD-3-Clause

# More Initial Effort: SPDX for Original Source



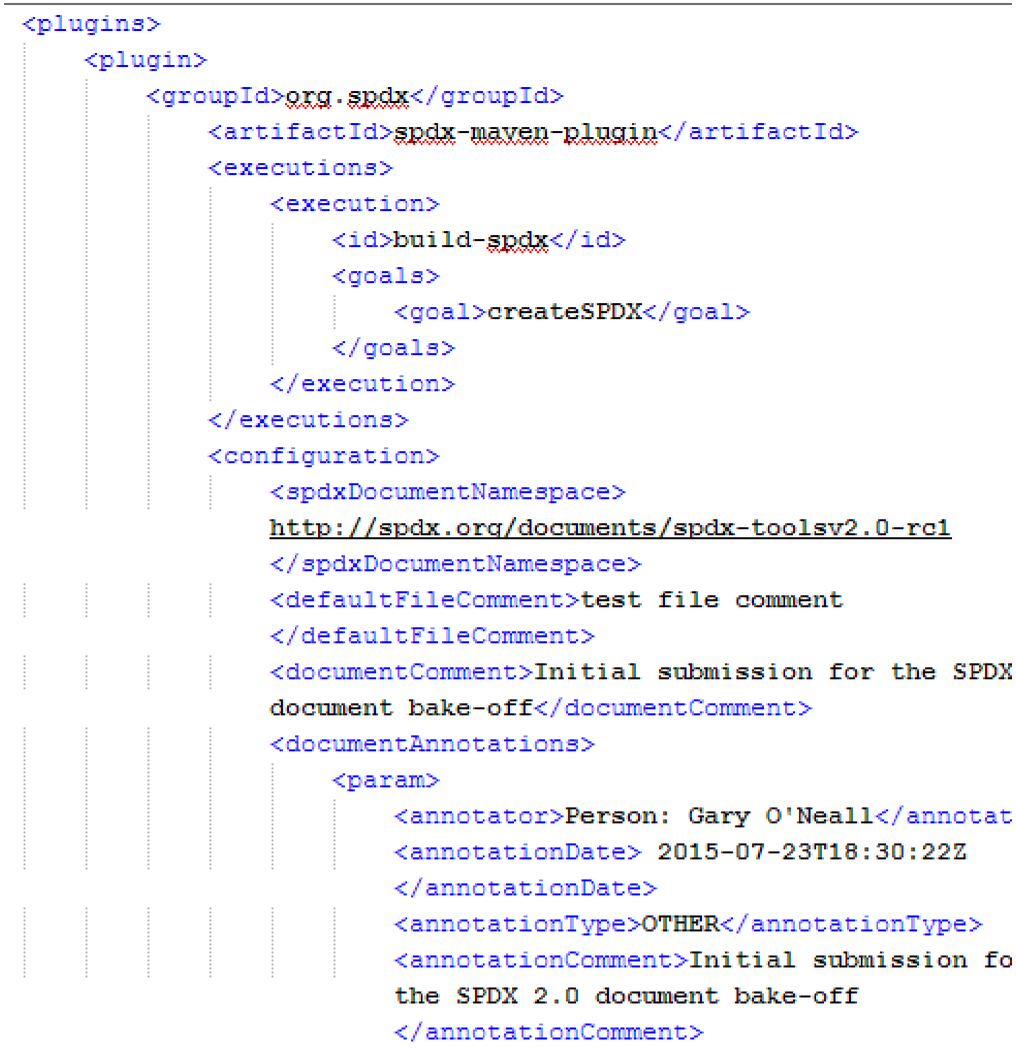
- Requires some tooling since the verification code is generated by checksums

# Tools to Support SPDX Creation

- Wind River website (spdx.windriver.org)
- FOSSology for analyzing licenses (https://fossologyspdx.ist.unomaha.edu/)
- Maven plug-in (https://github.com/goneall/spdx-maven-plugin)
- Yocto – UNO built SPDX extension
- Eclipse Plugin's under development (https://github.com/TCF-30/SPDX_Eclipse_Plugin and https://github.com/goneall/SpdxEclipsePlugin)
- FOSSosology (SPDX support in beta) (http://www.fossology.org/projects/fossology/wiki/WhoUsesFOSSology)
- Others… - See spdx.org/tools

# Example: Maven Plug-in

- Leverages existing meta data
- Additional configuration parameters for SPDX specifics
- Builds relationships based on dependencies
- Can be included in a “parent POM” for a larger open source project



```
<plugins>
    <plugin>
        <groupId>org.spdx</groupId>
            <artifactId>spdx-maven-plugin</artifactId>
            <executions>
                <execution>
                    <id>build-spdx</id>
                    <goals>
                        <goal>createSPDX</goal>
                    </goals>
                </execution>
            </executions>
            <configuration>
                <spdxDocumentNamespace>
                http://spdx.org/documents/spdx-toolsv2.0-rc1
                </spdxDocumentNamespace>
                <defaultFileComment>test file comment
                </defaultFileComment>
                <documentComment>Initial submission for the SPDX
                document bake-off</documentComment>
                <documentAnnotations>
                    <param>
                        <annotator>Person: Gary O'Neall</annotat
                        <annotationDate> 2015-07-23T18:30:22Z
                        </annotationDate>
                        <annotationType>OTHER</annotationType>
                        <annotationComment>Initial submission fo
                        the SPDX 2.0 document bake-off
                        </annotationComment>
```

# Advantages to SPDX Documents

- Can be very descriptive
  - In addition to licenses, contains copyrights, relationships, creation and origin information
- Can be easily translated to human readable form (e.g. a spreadsheet)
- Some verification supported (package verification code, checksums)
- Integrates with various license compliance tools
- REALLY helps the downstream consumers – changes from identification to (maybe) verification

# Tips for Keeping it Simple: Not all fields are required

Document Creation Information

2.1 SPDX Version.
2.2 Data License
2.3 SPDX Identifier
2.4 Document Name
2.5 SPDX Document Namespace
2.8 Creator
2.9 Created

**1 per document**

Package Information

3.1 Package Name
3.2 Package SPDX Identifier
3.7 Package Download Location
3.8 Package Verification Code
3.12 Concluded License
3.13 All Licenses Information from Files.
3.14 Declared License.
3.16 Copyright Text

**1 per package described in document**

File Information

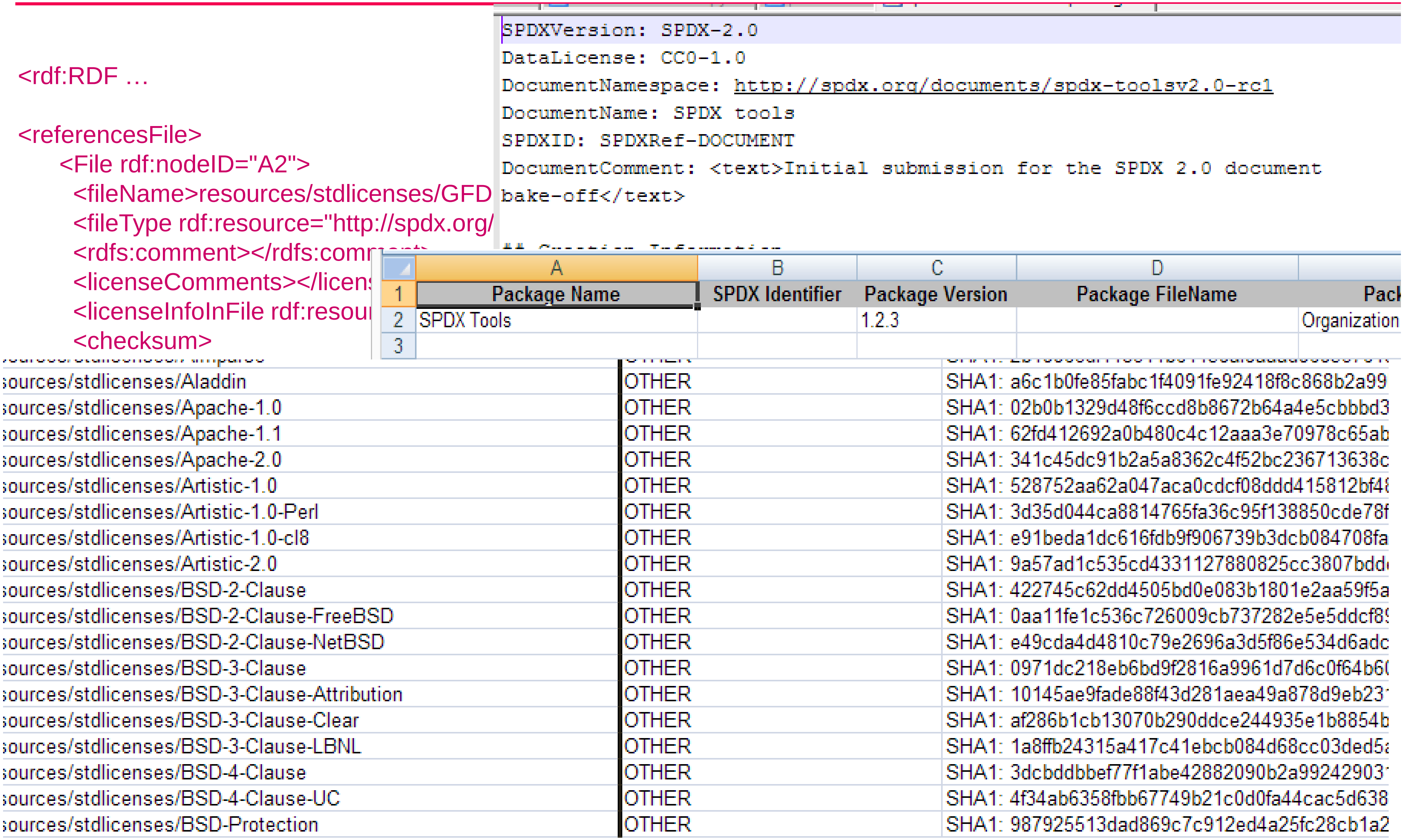
4.1 File Name
4.2 File SPDX Identifier
4.4 File Checksum
4.5 Concluded License
4.6 License Information in File
4.8 Copyright Text

**1 per file in each package**

# Tips for Keeping it Simple

- Beware of over-complicating the relationships
- Refer to best practices: http://wiki.spdx.org/view/Technical_Team/Best_Practices
- Refer to other example SPDX documents, such as the results of the SPDX “bake-off” results
- Monitor the spdx tech mailing lists

# Example – SPDX Tools:



```
<rdf:RDF …

<referencesFile>
    <File rdf:nodeID="A2">
      <fileName>resources/stdlicenses/GFD
      <fileType rdf:resource="http://spdx.org/
      <rdfs:comment></rdfs:comm
      <licenseComments></licen
      <licenseInfoInFile rdf:resou
      <checksum>
```

```
SPDXVersion: SPDX-2.0
DataLicense: CC0-1.0
DocumentNamespace: http://spdx.org/documents/spdx-toolsv2.0-rc1
DocumentName: SPDX tools
SPDXID: SPDXRef-DOCUMENT
DocumentComment: <text>Initial submission for the SPDX 2.0 document
bake-off</text>
```

| | A | B | C | D | |
|---|---|---|---|---|---|
| 1 | Package Name | SPDX Identifier | Package Version | Package FileName | Pack |
| 2 | SPDX Tools | | 1.2.3 | | Organization |
| 3 | | | | | |

| | | |
|---|---|---|
| sources/stdlicenses/Aladdin | OTHER | SHA1: a6c1b0fe85fabc1f4091fe92418f8c868b2a99 |
| sources/stdlicenses/Apache-1.0 | OTHER | SHA1: 02b0b1329d48f6ccd8b8672b64a4e5cbbbd3 |
| sources/stdlicenses/Apache-1.1 | OTHER | SHA1: 62fd412692a0b480c4c12aaa3e70978c65ab |
| sources/stdlicenses/Apache-2.0 | OTHER | SHA1: 341c45dc91b2a5a8362c4f52bc236713638c |
| sources/stdlicenses/Artistic-1.0 | OTHER | SHA1: 528752aa62a047aca0cdcf08ddd415812bf4 |
| sources/stdlicenses/Artistic-1.0-Perl | OTHER | SHA1: 3d35d044ca8814765fa36c95f138850cde78f |
| sources/stdlicenses/Artistic-1.0-cl8 | OTHER | SHA1: e91beda1dc616fdb9f906739b3dcb084708fa |
| sources/stdlicenses/Artistic-2.0 | OTHER | SHA1: 9a57ad1c535cd4331127880825cc3807bdd |
| sources/stdlicenses/BSD-2-Clause | OTHER | SHA1: 422745c62dd4505bd0e083b1801e2aa59f5a |
| sources/stdlicenses/BSD-2-Clause-FreeBSD | OTHER | SHA1: 0aa11fe1c536c726009cb737282e5e5ddcf8 |
| sources/stdlicenses/BSD-2-Clause-NetBSD | OTHER | SHA1: e49cda4d4810c79e2696a3d5f86e534d6adc |
| sources/stdlicenses/BSD-3-Clause | OTHER | SHA1: 0971dc218eb6bd9f2816a9961d7d6c0f64b6 |
| sources/stdlicenses/BSD-3-Clause-Attribution | OTHER | SHA1: 10145ae9fade88f43d281aea49a878d9eb23 |
| sources/stdlicenses/BSD-3-Clause-Clear | OTHER | SHA1: af286b1cb13070b290ddce244935e1b8854b |
| sources/stdlicenses/BSD-3-Clause-LBNL | OTHER | SHA1: 1a8ffb24315a417c41ebcb084d68cc03ded5 |
| sources/stdlicenses/BSD-4-Clause | OTHER | SHA1: 3dcbddbbef77f1abe42882090b2a99242903 |
| sources/stdlicenses/BSD-4-Clause-UC | OTHER | SHA1: 4f34ab6358fbb67749b21c0d0fa44cac5d638 |
| sources/stdlicenses/BSD-Protection | OTHER | SHA1: 987925513dad869c7c912ed4a25fc28cb1a2 |

# Using SPDX in the Software Supply Chain

- Importing upstream SPDX files
- Validating upstream SPDX files
- Scanning and generating SPDX for packages without SPDX files
- Creating output SPDX files

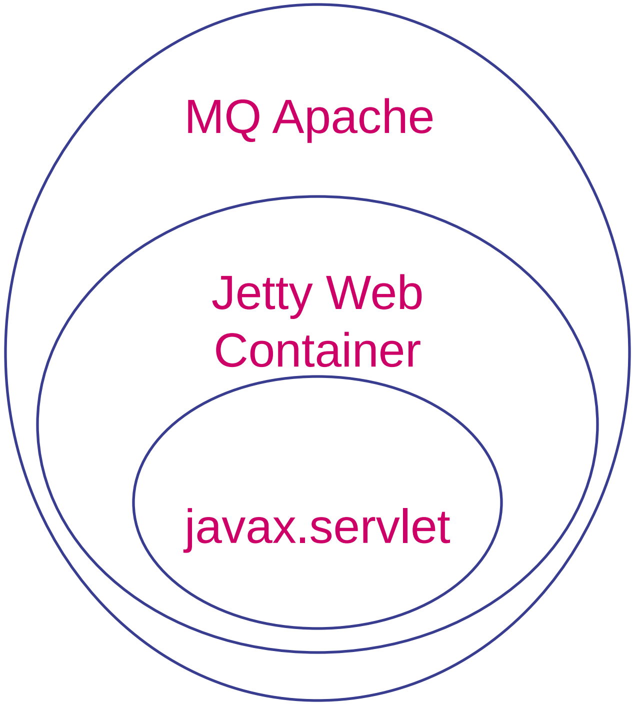
- Will typically involve multiple packages, multiple documents and relationships

# Advantages to using SPDX in the Software Supply Chain

- Maintain fidelity of the licensing data
- Reduce the effort for downstream consumers
- Reduce the effort for suppliers who are using SPDX

# Package Relationships Example

## Package

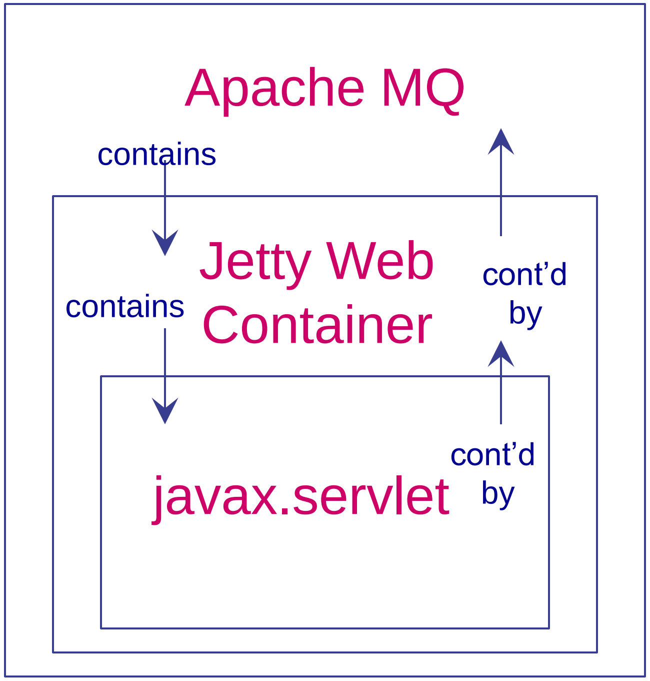


MQ Apache

Jetty Web Container

javax.servlet

## SPDX Doc



Apache MQ

contains

Jetty Web Container

contains

cont'd by

javax.servlet

cont'd by

# Tips on keeping it simple in the supply chain

- Reference existing SPDX documents using external SPDX document relationships
- Choose a common “namespace” for your SPDX documents
- Use relationships and annotations to provide any corrections

# More Information

- spdx.org
  - General information
- SPDX License list: spdx.org/licenses
- SPDX Tools: spdx.org/tools
- wiki.spdx.org
  - Workgroup wiki’s for Technical, Business, and legal teams
  - Contains information on joining the mailing lists and calls

# BACKUPS

# SPDX Tools Library

- Open source (Apache 2.0 licensed) Java code providing access the SPDX Standard Libraries
- Binary .jar files available:
  - http://spdx.org/spdx-tools/tools-from-the-spdx-workgroup
- Source code available:
  - git.spdx.org – spdx-tools project
  - https://github.com/spdx/tools
- Bugs / enhancement ideas can be reported:
  - bugs.linuxfoundation.org – project SPDX/tools
  - Github issues tracking
- Contributions welcome!

# More Information

- See the tech report “Accessing SPDX Licenses”: http://spdx.org/publications/tool-documentation/accessing-spdx-licenses
- Join the spdx-tech mailing list
- Email me at gary@sourceauditor.com