



Software Package Data Exchange (SPDX™) Specification

Version: 1.0-rc2



DISCLAIMER

The following is a draft of the Software Package Data Exchange (SDPX) Specification, version 1.0 (“Specification”). Please be advised that in addition to the licensing terms recited below, no reliance should be made regarding this Specification or any content supplied or provided under it, including any reliance that this Specification or any accompanying content supplied or provided under it represents any particular standard for any particular purpose. When the official SPDX specification is released, it will be clearly be labeled "official", and its purpose and recommended use will be clearly stated at that time.

Copyright © 2010-2011 Linux Foundation and its Contributors. All other rights are expressly reserved.

With thanks to Adam Cohn, Andrew Back, Ann Thornton, Bill Schineller, Bruno Corneec, Ciaran Farrell, Daniel German, Debra McGlade, Eran Strod, Eric Thomas, Esteban Rockett, Gary O’Neill, Guillaume Rousseau, Jack Manbeck, Jaime Garcia, Jeff Luszcz, Jilayne Lovejoy, John Ellis, Karen Copenhaver, Kate Stewart, Kim Weins, Kirsten Newcomer, Mark Gisi, Marshall Clow, Martin Michlmayr , Martin von Willebrand, Michael J. Herzog, Michel Ruffin, Peter Williams, Phil Robb, Philip Odencc, Philip Koltun, Scott K Peterson, Shane Coughlan, Steve Cropper, Stuart Hughes, Tom Callaway, and Thomas F. Incorvia for their contributions and assistance.


 This work is licensed under a [Creative Commons Attribution 3.0 Unported License](https://creativecommons.org/licenses/by/3.0/) (reproduced in Appendix III herein).

TABLE OF CONTENTS

1 RATIONALE.....	5
1.1 CHARTER.....	5
1.2 DEFINITION.....	5
1.3 WHY IS A COMMON FORMAT FOR DATA EXCHANGE NEEDED?.....	5
1.4 WHAT DOES THIS SPECIFICATION COVER?.....	5
1.5 WHAT IS NOT COVERED IN THE SPECIFICATION?.....	6
1.6 FORMAT REQUIREMENTS:.....	6
1.7 CONFORMANCE.....	7
2 SPDX DOCUMENT INFORMATION.....	8
2.1 SPDX VERSION	8
2.2 DATA LICENSE	8
3 CREATION INFORMATION.....	10
3.1 CREATOR.....	10
3.2 CREATED.....	10
3.3 CREATOR COMMENT.....	11
4 PACKAGE INFORMATION.....	12
4.1 FORMAL NAME.....	12
4.2 PACKAGE VERSION INFORMATION.....	12
4.3 PACKAGE FILE NAME.....	12
4.4 PACKAGE SUPPLIER.....	13
4.5 PACKAGE ORIGINATOR.....	14
4.6 PACKAGE DOWNLOAD LOCATION.....	14
4.7 PACKAGE VERIFICATION CODE.....	15
4.8 PACKAGE CHECKSUM.....	16
4.9 SOURCE INFORMATION.....	17
4.10 CONCLUDED LICENSE.....	17
4.11 ALL LICENSES INFORMATION FROM FILES.....	18
4.12 DECLARED LICENSE.....	19
4.13 COMMENTS ON LICENSE	20
4.14 COPYRIGHT TEXT.....	21
4.15 PACKAGE SUMMARY DESCRIPTION.....	21
4.16 PACKAGE DETAILED DESCRIPTION.....	22
5 OTHER LICENSING INFORMATION DETECTED.....	23
5.1 IDENTIFIER ASSIGNED.....	23
5.2 EXTRACTED TEXT	23
6 FILE INFORMATION.....	25
6.1 FILE NAME.....	25
6.2 FILE TYPE.....	25
6.3 FILE CHECKSUM.....	26
6.4 CONCLUDED LICENSE.....	26
6.5 LICENSE INFORMATION IN FILE.....	27
6.6 COMMENTS ON LICENSE	28
6.7 COPYRIGHT TEXT.....	29
6.8 ARTIFACT OF PROJECT NAME.....	29

6.9 ARTIFACT OF PROJECT HOMEPAGE..... 30

6.10 ARTIFACT OF PROJECT UNIFORM RESOURCE IDENTIFIER..... 30

7 REVIEW INFORMATION..... 32

7.1 REVIEWER..... 32

7.2 REVIEW DATE..... 32

7.3 REVIEW COMMENTS..... 33

APPENDIX I. STANDARD LICENSE SHORT FORMS..... 34

APPENDIX II. RDF DATA MODEL IMPLEMENTATION 38

OVERVIEW..... 38

VOCABULARY 39

ABSTRACT..... 39

CLASSES..... 39

PROPERTIES..... 45

INDIVIDUALS..... 57

AGENT AND TOOL IDENTIFIERS..... 59

APPENDIX III. CREATIVE COMMONS ATTRIBUTION LICENSE 3.0 UNPORTED..... 61

1 Rationale

1.1 Charter

To create a set of data exchange standards that enable companies and organizations to share license and component information (metadata) for software packages and related content with the aim of facilitating license and other policy compliance.

1.2 Definition

The Software Package Data Exchange (SPDX™) specification is a standard format for communicating the components, licenses and copyrights associated with a software package. An SPDX file is associated with a particular software package and contains information about that package in the SPDX format.

1.3 Why is a common format for data exchange needed?

Companies and organizations (collectively “Organizations”) are widely using and reusing open source and other software packages. Compliance with the associated licenses requires a set of analysis activities and due diligence that each Organization performs independently including: a manual and/or automated scan of software and identification of associated licenses followed by manual verification. Software development teams across the globe use the same open source packages, but little infrastructure exists to facilitate collaboration on the analysis or share the results of these analysis activities. As a result, many groups are performing the same work leading to duplicated efforts and redundant information. The SPDX working group seeks to create a data exchange format so that information about software packages and related content may be collected and shared in a common format with the goal of saving time and improving data accuracy.

1.4 What does this specification cover?

- 1.4.1** SPDX Document Information: Meta data to associate analysis results with a specific version of the SPDX file and license for use.
- 1.4.2** Creation Information: Information about how and when the SPDX file was created.
- 1.4.3** Package Information: Facts that are common properties of the entire package.
- 1.4.4** License Information: A list of common licenses likely to be encountered and a standardized naming convention for referring to these licenses and other licenses also found within an SPDX document. This naming convention will also be the basis for extending this set of common licenses over time.
- 1.4.5** File Information: Facts (e.g. copyrights, licenses) that are specific to each file included in the package.
- 1.4.6** Reviewer Information: Information from those who have reviewed the SPDX file.
- 1.4.7** evolution hooks: A set of mechanisms that permit extending the specification in a structured manner under specific future versions of the specification.

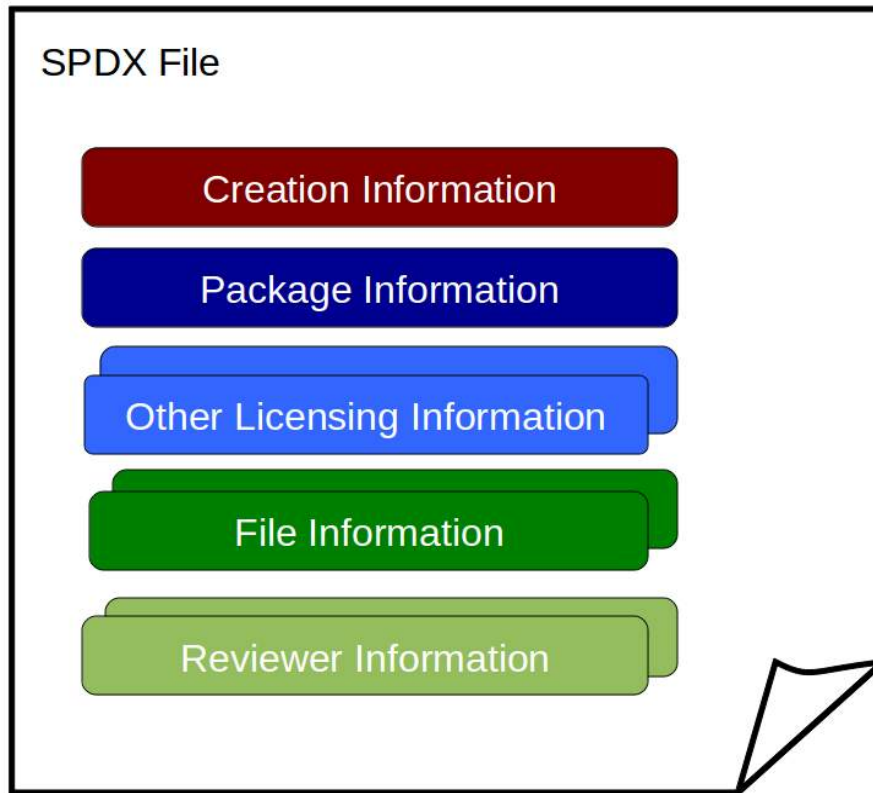


Figure 1. Overview of SPDX file contents.

1.5 What is not covered in the specification?

- 1.5.1** Information that cannot be derived from an inspection (whether manual or using automated tools) of the package to be analyzed.
- 1.5.2** How the data stored in an SPDX file is used by the recipient.
- 1.5.3** Any identification of any patent(s) which may or may not relate to the package.
- 1.5.4** Legal interpretation of the licenses or any compliance actions that might need to be taken.

1.6 Format Requirements:

- 1.6.1** Must be in a human readable form.
- 1.6.2** Must be in a syntax that a software tool can read and write.
- 1.6.3** Must be suitable to be checked for syntactic correctness independent of how it was generated (human or tool).
- 1.6.4** The SPDX file character set must support UTF-8 encoding.

1.6.5 Must permit automated specification syntax validation.

1.6.6 Resource Description Framework (RDF) can be used to represent this information, as can an annotate tag value flat text file.

1.6.7 Interoperability with an annotate tag format and the RDF format will be preserved.

1.7 Conformance

1.7.1 A file can be designated an SPDX file, if it is compliant with the requirements of the SPDX Trademark License (See <http://www.spdx.org/trademark>).

1.7.2 The official copyright notice to be used with any verbatim reproduction and/or distribution of this SPDX Specification 1.0 is:

"Official SPDX Specification 1.0. Copyright © 2010-2011 Linux Foundation and its Contributors. Licensed under the Creative Commons Attribution License 3.0 Unported. All other rights are expressly reserved."

1.7.3 The official copyright notice to be used with any non-verbatim reproduction and/or distribution of this SPDX Specification, including without limitation any partial use or combining this SPDX Specification with another work, is:

"This is not an official SPDX Specification. Portions herein have been reproduced from SPDX Specification 1.0 found at www.spdx.com. These portions are Copyright © 2010-2011 Linux Foundation and its Contributors, and are licensed under the Creative Commons Attribution License 3.0 Unported by the Linux Foundation and its Contributors. All other rights are expressly reserved by Linux Foundation and its Contributors."

2 SPDX Document Information

One instance is required for each SPDX document produced. It provides the necessary information for forward and backward compatibility for the processing tools.

Fields:

2.1 SPDX Version

2.1.1 Purpose: Provide a reference number that can be used to understand how to parse and interpret the rest of the file. It will enable both future changes to the specification and to support backward compatibility. The version number consists of a major and minor version indicator. The major field will be incremented when incompatible changes between versions are made (one or more sections are created, modified or deleted). The minor field will be incremented when backwards compatible changes are made.

2.1.2 Intent: Here, parties exchanging Identification Information in accordance with SPDX specification need to provide 100% transparency as to which SPDX specification such Identification Information is conforming to.

2.1.3 Cardinality: Mandatory, one.

2.1.4 Data Format: "SPDX-M.N"
where: M is major version number, N is minor version number.

2.1.5 Tag: "SPDXVersion:"

Example:

SPDXVersion: SPDX-1.0

2.1.6 RDF: spdx:specVersion

Example:

```
<SpdxDocument rdf:about"<a href="http://www.spdx.org/tools#SPDXANALYSIS">http://www.spdx.org/tools#SPDXANALYSIS">
  <specVersion> SPDX-1.0 </specVersion>
</SpdxDocument>
```

2.2 Data License

2.2.1 Purpose: Designates the license for the SPDX file itself. All content, including any data and any database, that may be in an SPDX file must be licensed under the Open Data Commons Public Domain Dedication and License 1.0 ("PDDL-1.0"). The PDDL-1.0 places data and databases in the public domain to ensure that all have the right to freely re-use the SPDX file without IP restrictions. Nothing in this use of the PDDL-1.0 prevents a supplier of SPDX files from temporarily or permanently limiting, by a separate and independent agreement, their recipients from (i) distribution of the supplier's specific aggregation of SPDX files to others or (ii) disclosing the supplier as the source and/or creator of any specific SPDX file(s).

2.2.2 Intent: This is to alleviate any concern that content (the data or database) in an SPDX file is subject to any form of intellectual property right that could restrict the re-use of the information or the creation of another SPDX file for the same project(s). This approach avoids intellectual property and related restrictions over the SPDX file, however individuals can still contract one to one to restrict release of specific collections of SPDX files (which map to software bill of materials) and the identification of the supplier of SPDX files.

2.2.3 Cardinality: Mandatory, one.

2.2.4 Data Format: "PDDL-1.0"

2.2.5 Tag: "DataLicense:"

Example:

DataLicense: PDDL-1.0

2.2.6 RDF: spdx:dataLicense

Example:

```
<SpdxDocument rdf:about"http://www.spdx.org/tools#SPDXANALYSIS">  
  <dataLicense rdf:resource="http://spdx.org/licenses/PDDL-1.0" />  
</SpdxDocument>
```

3 Creation Information

One instance of the Creation Information field set is required per package instance.

Fields:

3.1 Creator

3.1.1 Purpose: Identify who (or what, in the case of a tool) created the SPDX file. If the SPDX file was created by an individual, indicate the person's name. If the SPDX file was created on behalf of a company or organization, indicate the entity name. If the SPDX file was created using a software tool, the file should indicate an name and version for that tool. If multiple participants or tools were involved, use multiple instances of this field.

3.1.2 Intent: Here, the generation method will assist the reader of the Analysis Information in assessing the general reliability/accuracy of the analysis information provided by this file.

3.1.3 Cardinality: Mandatory, one or more.

3.1.4 Data Format: single line of text with the following keywords.

"Person: person name" and optional "(email)" or
 "Organization: organization" and optional "(email)" or
 "Tool: tool identifier - version".

Person name or organization name may be designated as "ANONYMOUS" if appropriate.

3.1.5 Tag: "Creator:"

Example:

Creator: Person: Jane Doe (jane.doe@example.com)
 Creator: Organization: ExampleCodeInspect (contact@example.com)
 Creator: Tool: LicenseFind-1.0

3.1.6 RDF: property `spdx:creator` in class `spdx:CreationInfo`

Example:

```
<CreationInfo>
  <creator> Person: Jane Doe (jane.doe@example.com) </creator>
  <creator> Organization: ExampleCodeInspect (contact@example.com) </creator>
  <creator> Tool: LicenseFind-1.0 </creator>
</CreationInfo>
```

3.2 Created

3.2.1 Purpose: Identify the date on which the SPDX file was created, which is the later of the date on which the SPDX file is originated or the date of the most recent change or update to the SPDX file (other than a change in accordance with section 7 that is limited to the addition of information regarding the conduct of a review.). This is to be specified according to combined data and time in UTC format as specified in ISO 8601 standard.

3.2.2 Intent: Here, the time stamp can serve as a verification as to whether the analysis needs to be updated.

- 3.2.3 Cardinality:** Mandatory, one.
- 3.2.4 Data Format:** YYYY-MM-DDThh:mm:ssZ
where:
 YYYY is year,
 MM is month with leading zero,
 DD is day with leading zero,
 T is delimiter for time,
 hh is hours with leading zero in 24 hour time,
 mm is minutes with leading zero,
 ss is seconds with leading zero, and
 Z is universal time indicator.
- 3.2.5 Tag:** "Created:"
- Example:**
Created: 2010-01-29T18:30:22Z
- 3.2.6 RDF: property** spdx:created in **class** spdx:CreationInfo
- Example:**
<CreationInfo>
 <created> 2010-01-29T18:30:22Z </created>
</CreationInfo>

3.3 Creator Comment

- 3.3.1 Purpose:** An optional field for creators of the SPDX file to provide general comments to the consumers of the SPDX file content.
- 3.3.2 Intent:** Here, the intent is to provide readers and reviewers with comments by the creator of the SPDX file.
- 3.3.3 Cardinality:** Optional, zero or one.
- 3.3.4 Data Format:** free form text that can span multiple lines.
In tag format this is delimited by <text> .. </text>, in RDF, it is delimited by <rdfs:comment>.
- 3.3.5 Tag:** "CreatorComment:"
- Example:**
CreatorComment: <text>
This package has been shipped in source and binary form.
The binaries were created with gcc 4.5.1 and expect to link to compatible system run time libraries.
</text>
- 3.3.6 RDF: property** rdfs:comment in **class** spdx:CreationInfo
- Example:**
<CreationInfo>
 <rdfs:comment> This package has been shipped in source and binary form.
 The binaries were created with gcc 4.5.1 and expect to link to compatible system run time libraries. </rdfs:comment>
</CreationInfo>

4 Package Information

One instance of the Package Information is required per package being analyzed. A package can contain sub-packages, but the overview is a reference to the entire contents of the package listed.

Fields:

4.1 Formal Name

4.1.1 Purpose: Identify the full name of the package as given by Package Originator.

4.1.2 Intent: Here, the formal name of each package is an important conventional technical identifier to be maintained for each package.

4.1.3 Cardinality: Mandatory, one.

4.1.4 DataFormat: single line of text .

4.1.5 Tag: "PackageName:"

Example:

PackageName: glibc

4.1.6 RDF: property spdx:name in **class** spdx:Package

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <name>glibc 2.11.1</name>
</Package>
```

4.2 Package Version Information

4.2.1 Purpose: Identify the version of the package.

4.2.2 Intent: The versioning of a package is a useful for identification purposes and for indicating later changes for the package version.

4.2.3 Cardinality: Optional, one.

4.2.4 DataFormat: single line text.

4.2.5 Tag: "PackageVersion:"

Example:

PackageVersion: 2.11.1

4.2.6 RDF: property spdx:versionInfo in **class** spdx:Package

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <versionInfo>2.11.1</versionInfo>
</Package>
```

4.3 Package File Name

4.3.1 Purpose: Provide the actual file name of the package. This may include the packaging and compression methods used as part of the file name.

4.3.2 Intent: Here, the actual file name of the compressed file (containing the package) is a significant technical element that needs to be carried with each package's identification information.

4.3.3 Cardinality: Mandatory, one

4.3.4 Data Format: single line of text.

4.3.5 Tag: "PackageFileName:"

Example:

PackageFileName: glibc-2.11.1.tar.gz

4.3.6 RDF: property `spdx:packageFileName` in **class** `spdx:Package`

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <packageFileName>glibc 2.11.1</packageFileName>
</Package>
```

4.4 Package Supplier

4.4.1 Purpose: Identify the actual distribution source for the package identified by the SPDX file. This may or may not be different from the originating distribution source for the package. The name of the Package Supplier must be an organization or recognized author, and not a web site. For example: Sourceforge is a host website, not a supplier, the supplier for `http://sourceforge.net/projects/bridge/` is "The Linux Foundation".

4.4.2 Intent: This field assists with understanding the point of distribution of the code in the package. This field is vital for ensuring that a downstream package distributees can address any ambiguity or concerns that might arise with the information in the SPDX file or the contents of the package it documents. This field can also be used to determine whom to contact for compliance support.

4.4.3 Cardinality: Optional, one.

4.4.4 Data Format: single line of text with the following keywords | "NOASSERTION"

If a single line of text is used it should have the following key words:
 "Person: person name" and optional "(email)" or
 "Organization: organization name" and optional "(email)".

NOASSERTION should be used if

- (i) the creator has attempted to but cannot reach a reasonable objective determination of who the supplier is, or
- (ii) the project is orphaned and was obtained a public web site.

NOASSERTION may be used to indicate that the creator has intentionally left this field blank and no meaning should be implied from the absence of an assertion.

4.4.5 Tag: "PackageSupplier:"

Example:

PackageSupplier: Person: Jane Doe (jane.doe@example.com)

4.4.6 RDF: property spdx:supplier in class spdx:Package

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <supplier>Person: Jane Doe (jane.doe@example.com </supplier>
</Package>
```

4.5 PackageOriginator

4.5.1 Purpose: If the package identified in the SPDX file originated from a different person or organization than identified as Package Supplier (see section 4.4 above), this field identifies from where or whom the package originally came. In some cases a package may be created and originally distributed by a different third party than the Package Supplier of the package. For example, the SPDX file identifies the package glibc, and RedHat as the Package Supplier, but FSF is the Package Originator.

4.5.2 Intent: This field assists with understanding the point of origin of the code in the package. This field is vital for understanding who originally distributed a package and should help in addressing any ambiguity or concerns that might arise with the information in the SPDX file or the contents of the Package it documents.

4.5.3 Cardinality: Optional, one.

4.5.4 Data Format: single line of text with the following keywords | "NOASSERTION"

If a single line of text is used it should have the following keywords:

"Person: person name" and optional "(email)" or

"Organization: organization name" and optional "(email)".

NOASSERTION should be used if

- (i) the creator has attempted to but cannot reach a reasonable objective determination of who can be considered to have originated the package, or
- (ii) the project is orphaned and was obtained from public web site,.

NOASSERTION may be used to indicate that the creator has intentionally left this field blank and no meaning should be implied from the absence of an assertion.

4.5.5 Tag: "PackageOriginator:"

Example:

PackageOriginator: Organization: ExampleCodeInspect (contact@example.com)

4.5.6 RDF: property spdx:originator in class spdx:Package

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <originator>Organization: ExampleCodeInspect (contact@example.com)
  </originator>
</Package>
```

4.6 Package Download Location

4.6.1 Purpose: This field identifies the download Universal Resource Locator (URL) for the package at the time that the SPDX file was created. If there is no public URL, then it is explicitly marked as UNKNOWN.

4.6.2 Intent: Here, where to download the exact package being referenced is a critical verification and tracking datum.

4.6.3 Cardinality: Mandatory, one.

4.6.4 Data Format: uniform resource locator | "UNKNOWN"

4.6.5 Tag: "PackageDownloadLocation:"

Example:

PackageDownloadLocation: http://ftp.gnu.org/gnu/glibc/glibc-2.11.2.tar.gz

4.6.6 RDF: property `spdx:downloadLocation` in class `spdx:Package`

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <downloadLocation>http://ftp.gnu.org/gnu/glibc/ </downloadLocation>
</Package>
```

4.7 Package Verification Code

4.7.1 Purpose: This identifier enables a recipient to determine if any file in the original package that the analysis was done on has been changed, and permits inclusion of an SPDX file as part of a package. This field provides an independently reproducible mechanism that permits unique identification of a specific contents of a package based on the actual files (except the SPDX file itself, if it is included in the package) that make up each package, that correlates to the data in this SPDX file.

4.7.2 Intent: Providing a unique identifier based on the files inside each package, eliminates confusion over which version or modification of a specific package the SPDX file refers to. The SPDX file can be embedded within the package without altering the identifier.

4.7.3 Cardinality: Mandatory, one

4.7.4 Algorithm:

```
verificationcode = 0
filelist = ""
for all files in the package {
  if file is an "excludes" file, skip it /* exclude SPDX analysis file(s) */
  appended filelist with "SHA1(file)" || "normalized_filename(file)\n"
}
sort filelist in ascending order by SHA1 value
verificationcode = SHA1(filelist)
```

Where `SHA1(file)` applies a SHA1 algorithm on the contents of file and returns the result in lowercase hexadecimal digits.

Where `normalized_filename(file)` normalized file name is a relative file uri transformed

to remove all `.` and `.` path elements removed. For example, `normalized("./foo.c") => "foo.c"` and `normalized("foo/./bar/./important.c") => "foo/important.c"`.

4.7.5 Data Format: single line of text with 160 bit binary represented as 40 hexadecimal digits

4.7.6 Tag: "PackageVerificationCode:" (and optionally "(excludes: normalized_filename)")

Example:

PackageVerificationCode: d6a770ba38583ed4bb4525bd96e50461655d2758 (excludes: package.spdx)

4.7.7 RDF: spdx:packageVerificationCodeValue, spdx:packageVerificationCodeExcludedFile in **class** spdx:PackageVerificationCode

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <packageVerificationCode>
    <PackageVerificationCode>
      <packageVerificationCodeValue>d6a770ba38583ed4bb4525bd96e50461655d2758
      </packageVerificationCodeValue>
      <packageVerificationCodeExcludedFile> package.spdx
      </packageVerificationCodeExcludesFile>
    </PackageVerificationCode>
  </packageVerificationCode>
</Package>
```

4.8 Package Checksum

4.8.1 Purpose: This field provides an independently reproducible mechanism that permits unique identification of a specific package that correlates to the data in this SPDX file. This identifier enables a recipient to determine if any file in the original package has been changed. The SHA-1 algorithm will be used to provide the checksum by default.

4.8.2 Intent: Here, by providing a unique identifier of each the package, confusion over which version or modification of a specific package the SPDX file references should be eliminated.

4.8.3 Cardinality: Optional, zero or one.

4.8.4 Algorithm: **SHA1** (<http://tools.ietf.org/html/rfc3174>) is to be used on on the package.

4.8.5 Data Format: There are two components, an algorithm identifier("SHA1") and a 160 bit value represented as 40 lowercase hexadecimal digits.

4.8.6 Tag: "PackageChecksum:"

Example:

PackageChecksum: SHA1: d6a770ba38583ed4bb4525bd96e50461655d2758

4.8.7 RDF: properties spdx:algorithm, spdx:checksumValue in **class** spdx:checksum

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <checksum>
    <Checksum>
      <algorithm rdf:resource="checksumAlgorithm_sha1"/>
      <checksumValue> d6a770ba38583ed4bb4525bd96e50461655d2758
      </checksumValue>
    </Checksum>
  </checksum>
</Package>
```



```

    </checksum>
  </Package>

```

4.9 Source Information

4.9.1 Purpose: This field provides a place for the SPDX file creator to record any relevant background information or additional comments about the origin of the package. For instance, this field might include comments indicating whether the package been pulled from a source code management system or has been repackaged.

4.9.2 Intent: Here, by providing a freeform field, the SPDX file creator can provide additional information to describe any anomalies, or discoveries, in the determination of the origin of the package.

4.9.3 Cardinality: Optional, one

4.9.4 Data Format: free form text that can span multiple lines. In tag format this is delimited by `<text> .. </text>`.

4.9.5 Tag: "PackageSourceInfo:"

Example:

PackageSourceInfo: uses glibc-2_11-branch from git://sourceware.org/git/glibc.git.

4.9.6 RDF: spdx:sourceInfo

Example:

```

<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <sourceInfo>uses glibc-2_11-branch from git://sourceware.org/git/glibc.git.
</sourceInfo>
</Package>

```

4.10 Concluded License

4.10.1 Purpose: This field contains the license the SPDX file creator has concluded as governing the package or alternative values, if the governing license cannot be determined. The options to populate this field are limited to:

- (a) the SPDX License List short form identifier; if the concluded license is on the SPDX License List;
- (b) a reference to the license text denoted by the LicenseRef-#, if the concluded license is not on the SPDX License List;
- (c) NOASSERTION; should be used if;
 - (i) the SPDX file creator has attempted to but cannot reach a reasonable objective determination of the Concluded License,
 - (ii) the SPDX file creator is uncomfortable concluding a license, despite some license information being available;
 - (iii) the SPDX file creator has made no attempt to determine a Concluded License, or
 - (iv) there is no licensing information from which to conclude a license for the package.

NOASSERTION may be used to indicate that the creator has intentionally left this field blank and no meaning should be implied from the absence of an assertion.

With respect to (a) and (b) above, if there is more than one concluded license, all should be included. If the package recipient has a choice of multiple licenses, then each of the choices should be recited as a "disjunctive" license. If the Concluded License is not the same as the Declared License, a written explanation should be provided in the Comments on License field (section 4.13). With respect to (c), a written explanation in the Comments on License field (section 4.13) is preferred.

4.10.2 Intent: Here, the intent is for the SPDX file creator to analyze the license information in package, and other objective information, e.g., COPYING.txt file etc., together with the results from any scanning tools, to arrive at a reasonably objective conclusion as to what license governs the package.

4.10.3 Cardinality: Mandatory, one

4.10.4 Data Format: <short form identifier in Appendix I> | "LicenseRef"-N | "NOASSERTION" | "NONE" | <license set>

4.10.5 Tag: "PackageLicenseConcluded:"
For a license set, when there is a choice between licenses ("disjunctive license"), they should be separated with "or" and enclosed in parentheses. When multiple licenses apply ("conjunctive license"), they should be separated with an "and" and enclosed in parentheses.

Example:
PackageLicenseConcluded: LGPL-2.0

Example:
PackageLicenseConcluded: (LGPL-2.0 or LicenseRef-3)

4.10.6 RDF: property spdx:licenseConcluded in **class** spdx:Package

Example:
<Package rdf:about="<http://www.spdx.org/tools#SPDXANALYSIS?package>">
 <licenseConcluded> rdf:resource="<http://spdx.org/licenses/LGPL-2.0>" />
</Package>

Example:
<Package rdf:about="<http://www.spdx.org/tools#SPDXANALYSIS?package>">
 <licenseConcluded>
 <DisjunctiveLicenseSet>
 <member rdf:resource="<http://spdx.org/licenses/LGPL-2.0>" />
 <member rdf:resource="_:licenseRef-3" />
 </DisjunctiveLicenseSet>
 </licenseConcluded>
</Package>

4.11 All Licenses Information from Files

4.11.1 Purpose: This field is to contain a list of all licenses found in the package. The options to populate this list are limited to:

- (a) the SPDX License List short form identifier, if a detected license is on the SPDX License List;
- (b) a reference to the license, denoted by LicenseRef-#, if the detected license is not on the SPDX License List;
- (c) NONE, if no license information is detected in any of the files; or

(d)NOASSERTION, if the SPDX file creator has not examined the contents of the actual files or if the SPDX file creator has intentionally left this field blank (no meaning should be implied by doing so).

Note: The relationship between licenses (conjunctive, disjunctive) is not specified in this field – it is simply a listing of all licenses found.

4.11.2 Intent: Here, we intend to capture all license information detected in the actual files.

4.11.3 Cardinality: Mandatory, one or many.

4.11.4 Data Format: <short form identifier in Appendix I> | "LicenseRef"-N | "NONE" | "NOASSERTION"

4.11.5 Tag: "PackageLicenseInfoFromFiles:"

Example:

```
PackageLicenseInfoFromFiles: GPL-2.0
PackageLicenseInfoFromFiles: LicenseRef-1
PackageLicenseInfoFromFiles: LicenseRef-2
```

4.11.6 RDF: property spdx:licenseInfoFromFiles in **class** spdx:Package

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <licenseInfoFromFiles rdf:resource="http://spdx.org/licenses/GPL-2.0" />
  <licenseInfoFromFiles rdf:resource="_.licenseRef-1" />
  <licenseInfoFromFiles rdf:resource="_.licenseRef-2" />
</Package>
```

4.12 Declared License

4.12.1 Purpose: This field lists the licenses that have been declared by the authors of the package. Any license information that does not originate from the package authors, e.g. license information from a third party repository, should not be included in this field. The options to populate this field are limited to:

- (a) the SPDX License List short form identifier; if the license is on the SPDX License List;
- (b) a reference to the license, denoted by LicenseRef-#, if the declared license is not on the SPDX License List;
- (c) NONE, if no license information is detected in any of the files
- (d) NOASSERTION, if the SPDX file creator has not examined the contents of the package or if the SPDX file creator has intentionally left this field blank (no meaning should be implied by doing so).

With respect to "a" and "b" above, if license information for more than one license is contained in the file, all should be reflected in this field. If the license information offers the recipient a choice of licenses, then each of the choices should be recited as a "disjunctive" licenses.

4.12.2 Intent: This is simply the license identified in text in one or more files (for example COPYING file) in the source code package. This field is not intended to capture license information obtained from an external source, such as the package website. Such information can be included in 4.7 Concluded License. This field may have multiple declared licenses, if multiple licenses are declared at the package level.

4.12.3 Cardinality: Mandatory, one.

4.12.4 Data Format: <short form identifier in Appendix I> | "LicenseRef"-N | "NONE" | "NOASSERTION" | <license set>

4.12.5 Tag: "PackageLicenseDeclared:"
For a license set, when there is a choice between licenses ("disjunctive license"), they should be separated with a "or" and enclosed in brackets. Similarly, when multiple licenses need to be applied ("conjunctive license"), they should be separated with an "and" and enclosed in brackets.

Example:

PackageLicenseDeclared: LGPL-2.0

Example:

PackageLicenseDeclared: (LGPL-2.0 and LicenseRef-3)

4.12.6 RDF: property spdx:licenseDeclared in **class** spdx:Package

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <licenseDeclared rdf:resource="http://spdx.org/licenses/LGPL-2.0" />
</Package>
```

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <licenseDeclared>
    <DisjunctiveLicenseSet>
      <member rdf:resource="http://spdx.org/licenses/LGPL-2.0" />
      <member rdf:resource="_.licenseRef-3" />
    </DisjunctiveLicenseSet>
  </licenseDeclared>
</Package>
```

4.13 Comments on License

4.13.1 Purpose: This field provides a place for the SPDX file creator to record any relevant background information or analysis that went in to arriving at the Concluded License for a package. If the Concluded License does not match the Declared License or License Information from Files, this should be explained by the SPDX file creator. Its is also preferable to include an explanation here when the Concluded License is NOASSERTION.

4.13.2 Intent: Here, the intent is to provide the reader with a detailed explanation of how the Concluded License(s) was determined if it does not match the License Information from the files or the source code package, is marked NOASSERTION, or other helpful information for the reader relevant to determining the license of the package.

4.13.3 Cardinality: Optional, one

4.13.4 Data Format: free form text that can span multiple lines. In tag format this is delimited by `<text> .. </text>`, in RDF, it is delimited by `<rdfs:comment>`.

4.13.5 Tag: "PackageLicenseComments:"

Example:

PackageLicenseComments: `<text>`

The license for this project changed with the release of version x.y. The version of the project included here post-dates the license change.
`</text>`

4.13.6 RDF: property `spdx:licenseComments` in **class** `spdx:Package`

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <licenseComments>
    This package has been shipped in source and binary form.
    The binaries were created with gcc 4.5.1 and expect to link to
    compatible system run time libraries.
  </licenseComments>
</Package>
```

4.14 Copyright Text

4.14.1 Purpose: Identify the copyright holders of the package, as well as any dates present. This will be a free form text field extracted from the package information files. The options to populate this field are limited to:

- (a) any text related to a copyright notice, even if not complete;
- (b) "NONE" if the package contains no license information whatsoever; or
- (c) NOASSERTION, if the SPDX file creator has not examined the contents of the package or if the SPDX file creator has intentionally left this field blank (no meaning should be implied by doing so).

4.14.2 Intent: Record any copyright notices for the package.

4.14.3 Cardinality: Mandatory, one.

4.14.4 Data Format: delimited multiple lines of free form text | "NOASSERTION" | "NONE"

4.14.5 Tag: "PackageCopyrightText:"
In tag format multiple lines are delimited by `<text> .. </text>`.

Example:

PackageCopyrightText: `<text>`
Copyright 2008-2010 John Smith
`</text>`

4.14.6 RDF: property `spdx:copyrightText` in **class** `spdx:Package`

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <copyrightText>
    Copyright 2008-2010 John Smith
  </copyrightText>
</Package>
```

4.15 Package Summary Description

4.15.1 Purpose: This field is a short description of the package

4.15.2 Intent: Here, the intent is to allow a reader/reviewer of this field to quickly understand the function/use of the package, at a high level, without having to parse the source code of the actual package.

4.15.3 Cardinality: Optional, one.

4.15.4 Data Format: delimited free form text that can span multiple lines.

4.15.5 Tag: "PackageSummary:"
In tag format multiple lines are delimited by <text> .. </text>.

Example:

PackageSummary: <text> gnu c library </text>

4.15.6 RDF: property spdx:summary in **class** spdx:Package

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <summary> gnu c library </summary>
</Package>
```

4.16 Package Detailed Description

4.16.1 Purpose: This field is a more detailed description of the package, and can be used for any comments on license discrepancies. It may also be extracted from the packages itself.

4.16.2 Intent: Here, the intent is to provide technical readers/reviewers with a detailed technical explanation of the functionality, anticipated use, and anticipated implementation of the package. This field may also include a description of improvements over prior version of the package, where applicable.

4.16.3 Cardinality: Optional, one.

4.16.4 Data Format: delimited free form text than can span multiple lines.

4.16.5 Tag: "PackageDescription:"
In tag format multiple lines are delimited by <text> .. </text>.

Example:

PackageDescription: <text>
This package provides the gnu c library,
</text>

4.16.6 RDF: property spdx:description in **class** spdx:Package

Example:

```
<Package rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?package">
  <description>
    This package provides the gnu c library, ....
  </description>
</Package>
```

5 Other Licensing Information Detected

This section is used for any detected, declared or concluded licenses that are NOT on the SPDX License List. For the most up-to-date version of the list see: <http://spdx.org/licenses/>. The SPDX License List can also be found here in Appendix I.

One instance should be created for every unique license or licensing information reference detected in package that does not match one of the licenses on the SPDX License List. Each license instance should have the following fields.

Fields:

5.1 Identifier Assigned

5.1.1 Purpose: Provide a unique identifier to refer to licenses that are not found on the SPDX License List. This unique identifier can then be used in the packages and files sections of the SPDX file (sections 4 and 6, respectively).

5.1.2 Intent: Create a short form license identifier for license not on the SPDX License List..

5.1.3 Cardinality: Conditional(mandatory, one) if license is not on SPDX License List.

5.1.4 Data Format: "LicenseRef-"N where N is a unique numeric value.

5.1.5 Tag: "LicenseID:"

Example:

LicenseID: LicenseRef-1

5.1.6 RDF: property spdx:licenseID in **class** spdx:ExtractedLicensingInfo

Example:

```
<ExtractedLicensingInfo rdf:about="" _:licenseRef-1>
  <licenseID> LicenseRef-1 </licenseID>
</ExtractedLicensingInfo>
```

5.2 Extracted Text

5.2.1 Purpose: Provide a copy of the actual text of the license reference extracted from the package that is associated with the License ID to aid in future analysis.

5.2.2 Intent: Provide the license reference text as found in the package or file that is not on the SPDX License List.

5.2.3 Cardinality: Conditional(Mandatory, one) if license is not on SPDX License List.

5.2.4 Data Format: delimited free form text field that may span multiple lines.

5.2.5 Tag: "ExtractedText:"
In tag format multiple lines are delimited by <text> .. </text>.

Example:

```
ExtractedText: <text>"THE BEER-WARE LICENSE" (Revision 42):
<phk@FreeBSD.ORG> wrote this file. As long as you retain this notice you
can do whatever you want with this stuff. If we meet some day, and you think this stuff
is worth it, you can buy me a beer in return Poul-Henning Kamp
```

</text>

5.2.6 RDF: property `spdx:extractedText` in class `spdx:ExtractedLicensingInfo`

Example:

```
<ExtractedLicensingInfo rdf:about=" :licenseRef-1>
  <licenseId> LicenseRef-1 </licenseId>
  <extractedText> "THE BEER-WARE LICENSE" (Revision 42):
  <phk@FreeBSD.ORG> wrote this file. As long as you retain this notice you
  can do whatever you want with this stuff. If we meet some day, and you think
  this stuff is worth it, you can buy me a beer in return Poul-Henning Kamp
  </extractedText>
</ExtractedLicensingInfo>
```


6 File Information

This section is used to list information for the files in the package. Each file in the package should have a set of the following fields.

Fields:

6.1 File Name

6.1.1 Purpose: Identify path to file that corresponds to this information.

6.1.2 Intent: To aid finding the correct file which corresponds to the file information grouped together.

6.1.3 Cardinality: Mandatory, one.

6.1.4 Data Format: A relative file URL(<http://tools.ietf.org/html/rfc1738>) from the root of the package archive or directory.

6.1.5 Tag: "FileName:"

Example:

FileName: ./package/foo.c

6.1.6 RDF: property spdx:fileName in **class** spdx:File

Example:

```
<File rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?file">
  <fileName>./package/foo.c</fileName>
</File>
```

6.2 File Type

6.2.1 Purpose: This field identifies common types of files where there may be different treatment of copyright and license information: source, binary, machine generated, etc. "SOURCE" should be used when the file is of human readable source code (.c, .html, etc.). "BINARY" should be used, when the file is a compiled object (.o, .a, etc.). "ARCHIVE" should be used when the file contains an archive (.tar, .jar, etc.). "OTHER" should be used for those files that don't fit into the above categories (pictures, audio, data files, etc.)

6.2.2 Intent: Here, this field is basically the "best available" summary of the format field, from a developer perspective.

6.2.3 Cardinality: Optional, one.

6.2.4 Data Format: "SOURCE" | "BINARY" | "ARCHIVE" | "OTHER"

6.2.5 Tag: "FileType:"

Example:

FileType: BINARY

6.2.6 RDF: property spdx:fileType in **class** spdx:File

Example:

```
<File rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?file">
```

```

    <fileType rdf:resource="fileType_binary" />
  </File>

```

6.3 File Checksum

6.3.1 Purpose: Provide a unique identifier to match analysis information on specific files of a package.

6.3.2 Intent: Here, by providing a unique identifier of each file, confusion over which version/modification of a specific file the Identification Information references should be eliminated.

6.3.3 Cardinality: Mandatory, one.

6.3.4 Algorithm: SHA1 (<http://tools.ietf.org/html/rfc3174>) is to be used on the file.

6.3.5 Data Format: There are two components, an algorithm identifier (SHA-1), a separator (":") and a 160 bit value represented as 40 hexadecimal digits.

6.3.6 Tag: "FileChecksum:"

Example:

FileChecksum: SHA1: d6a770ba38583ed4bb4525bd96e50461655d2758

6.3.7 RDF: property spdx:Checksum in **class** spdx:File

Example:

```

<File rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?file">
  <checksum>
    <Checksum>
      <algorithm>SHA1</algorithm>
      <checksumValue>d6a770ba38583ed4bb4525bd96e50461655d2758
    </checksumValue>
    </Checksum>
  </checksum>
</File>

```

6.4 Concluded License

6.4.1 Purpose: This field contains the license the SPDX file creator has concluded as governing the file, or alternative values if the governing license cannot be determined. The options to populate this field are limited to:

- (a) the SPDX standardized license short form identifier; if the concluded license is on the SPDX License List;
- (b) a reference to the licenses, denoted by LicenseRef-#, if the concluded license is not on the SPDX License List;
- (c) NOASSERTION; should be used
 - (i) if the SPDX file creator has attempted to but cannot reach a reasonable objective determination of the concluded license, or
 - (ii) if the SPDX file creator is uncomfortable concluding a license, despite some license information being available; or
 - (iii) if the SPDX file creator has made no attempt to arrive at a concluded license; or
 - (iv) there is no license information from which to conclude a license for the file.

With respect to “a” and “b” above, if there is more than one concluded license, all should be included. If the package recipient has a choice of multiple licenses, then each of the choices should be recited as a “disjunctive” license. If the Concluded License(s) is not the same as the License Information in File, a written explanation should be provided in the Comments on License field (section 6.6). With respect to (c), a written explanation in the Comments on License field is preferred.

6.4.2 Intent: Here, the intent is for the SPDX file creator to analyze the License Information in File (section 6.5) and other objective information, e.g., “COPYING FILE”, etc., together with the results from any scanning tools, to arrive at a reasonably objective conclusion as to what license is governing the file.

6.4.3 Cardinality: Mandatory, one.

6.4.4 Data Format: <short form identifier in Appendix I> | “LicenseRef”-N | “NOASSERTION” | “NONE” | <license set>

6.4.5 Tag: “LicenseConcluded:”
For a license set, when there is a choice between licenses (“disjunctive license”), they should be separated with “or” and enclosed in brackets. Similarly when multiple licenses need to be applied (“conjunctive license”), they should be separated with an “and” and enclosed in brackets.

Example:

LicenseConcluded: LGPL-2.0

Example:

LicenseConcluded: (LGPL-2.0 or LicenseRef-2)

6.4.6 RDF: property `spdx:licenseConcluded` in **class** `spdx:File`

Example:

```
<File rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?file">
  <licenseConcluded> LGPL-2.0 </licenseConcluded>
</File>
```

Example:

```
<File rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?file">
  <licenseConcluded>
    <ConjunctiveLicenseSet>

      <member rdf:resource="http://spdx.org/licenses/LGPL-2.0"/>
      <member rdf:nodeID="LicenseRef-2"/>

    </ConjunctiveLicenseSet>
  </licenseConcluded>
</File>
```

6.5 License Information in File

6.5.1 Purpose: This field contains the license information actually found in the file, if any. Any license information not actually in the file, e.g., “COPYING.txt” file in a toplevel directory, etc., should not be reflected in this field. This information is most commonly found in the header of the file, although it may be in other areas of the actual file. The options to populate this field are limited to:

- (a) the SPDX License List short form identifier; if the license is on the SPDX License List;
- (b) a reference to the license, denoted by LicenseRef-#, if the found license is not on the SPDX License List;
- (c) NONE; if the actual file contains no license information whatsoever; or
- (d) NOASSERTION, if the SPDX file creator has not examined the contents of the actual file or the SPDX file creator has intentionally left this field blank (no meaning should be implied by doing so).

With respect to “a” and “b” above, if license information for more than one license is contained in the file, all should be reflected in this field. If the license information offers the package recipient a choice of licenses, then each of the choices should be listed as a separate License Information in File entry.

6.5.2 Intent: Here, the intent is to provide the license information actually in the file, as compared to the Concluded License field.

6.5.3 Cardinality: Mandatory, one or many

6.5.4 Data Format: <short form identifier in Appendix I> | "LicenseRef"-N | "NONE" | "NOASSERTION"

6.5.5 Tag: “LicenseInfoInFile:”

Example:

LicenseInfoInFile: GPL-2.0
LicenseInfoInFile: LicenseRef-2

6.5.6 RDF: property spdx:licenseInfoInFile in **class** spdx:File

Example:

```
<File rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?file">
  <licenseInfoInFile rdf:resource="http://spdx.org/licenses/GPL-2.0" />
  <licenseInfoInFile rdf:resource="_.licenseRef-2" />
</File>
```

6.6 Comments on License

6.6.1 Purpose: This field provides a place for the SPDX file creator to record any relevant background references or analysis that went in to arriving at the Concluded License(s) for a file. If the Concluded License(s) does not match the License Information in File, this should be explained by the SPDX filecreator. It is also preferable to include an explanation here when the Concluded License is NOASSERTION.

6.6.2 Intent: Here, the intent is to provide the reader with a detailed explanation of how the Concluded License(s) was determined if it does not match the License Information in File, is marked NOASSERTION, or other helpful information for the reader relevant to determining the license of the file.

6.6.3 Cardinality: Optional, one

6.6.4 Data Format: delimited free form text that can span multiple lines

6.6.5 Tag: “LicenseComments:”
In tag format multiple lines are delimited by <text> .. </text>.

Example:

LicenseComments: <text>

The concluded license was taken from the package level that the file was included in. This information was found in the COPYING.txt file in the xyz directory.

</text>

6.6.6 RDF: property spdx:licenseComments in **class** spdx:File**Example:**

<File:about="http://www.spdx.org/tools#SPDXANALYSIS?file">

<licenseComments>

The concluded license was taken from the package level that the file was included in. This information was found in the COPYING.txt file in the xyz directory. This package has been shipped in source and binary form.

</licenseComments>

</File>

6.7 Copyright Text

6.7.1 Purpose: Identify the copyright holder of the file, as well as any dates present. This will be a freeform text field extracted from the actual file. The options to populate this field are limited to:

(a) any text relating to a copyright notice, even if not complete;

(b) NONE; if the file contains no license information whatsoever; or

(c) NOASSERTION; if the SPDX creator has not examined the contents of the

actual file. NOASSERTION may be used to indicate that the creator

has

intentionally left this field blank (no meaning should be implied from the absence of an assertion).

6.7.2 Intent: Record any copyright notice for the package.**6.7.3 Cardinality:** Mandatory, one.**6.7.4 Data Format:** delimited free form text that can span multiple lines | "NONE" | "NOASSERTION"**6.7.5 Tag:** "FileCopyrightText:"

In tag format multiple lines are delimited by <text> .. </text>.

Example:

FileCopyrightText: <text> Copyright 2008-2010 John Smith </text>

6.7.6 RDF: property spdx:copyrightText in **class** spdx:File**Example:**

<File rdf:about="http://www.spdx.org/tools#SPDXANALYSIS?file">

<copyrightText>

Copyright 2008-2010 John Smith

</copyrightText>

</File>

6.8 Artifact of Project Name

- 6.8.1 Purpose:** To indicate that a file has been derived from a specific project.
- 6.8.2 Intent:** To make it easier for consumers of the report to determine the original source of the file.
- 6.8.3 Cardinality:** Optional, one.
- 6.8.4 Data Format:** single free form line of text
- 6.8.5 Tag:** "ArtifactOfProjectName:"

Example:

ArtifactOfProjectName: Jena

- 6.8.6 RDF:** property `spdx:artifactOf/doap:Project/doap:name`

Example:

```
<File>
  <artifactOf>
    <doap:Project>
      <doap:name>Jena</doap:name>
    </doap:Project>
  </artifactOf>
</File>
```

6.9 Artifact of Project Homepage

- 6.9.1 Purpose:** To indicate the location of the project from which the file has been derived.
- 6.9.2 Intent:** To make it easier for consumers of the report to determine the original source of the file.
- 6.9.3 Cardinality:** Optional, one.
- 6.9.4 Data Format:** uniform resource locator | "UNKNOWN"
- 6.9.5 Tag:** "ArtifactOfProjectHomePage:"

Example:ArtifactOfProjectHomePage: <http://www.openjena.org/>

- 6.9.6 RDF:** `spdx:artifactOf/doap:Project/doap:homepage`

Example:

```
<File>
  <artifactOf>
    <doap:Project>
      <doap:homepage rdf:resource="http://www.openjena.org/" />
    </doap:Project>
  </artifactOf>
</File>
```

6.10 Artifact of Project Uniform Resource Identifier

6.10.1 Purpose: To provide a linkage to the project resource in the doap document and permit interoperability between the different formats supported.

6.10.2 Intent: To make it easier for consumers of the report to determine the original source of the file.

6.10.3 Cardinality: Optional, one.

6.10.4 Data Format: URI specifier

6.10.5 Tag: "ArtifactOfProjectURI:"

Example:

ArtifactOfProjectURI: <http://svn.apache.org/repos/asf/httpd/site/trunk/docs/doap.rdf>

6.10.6 RDF: spdx:artifactOf/doap

Example:

```
<File>
  <artifactOf
    rdf:resoure="http://svn.apache.org/repos/asf/httpd/site/trunk/docs/doap.rdf" />
</File>
```

7 Review Information

Review information can optionally be added after the initial SPDX file has been created. The Created date should not be modified as a result of the addition of information regarding the conduct of a review. The presence of this information is optional, and separate instances can be added. Once a Reviewer entry is added though, the ReviewDate is mandatory to be associated with the Reviewer. A specific ReviewComment is optional.

Fields:

7.1 Reviewer

7.1.1 Purpose: Record of a person, organization or tool that has reviewed the SPDX file and the date of that review. Note that there is no requirement for a particular reviewer to add their name to the file, however it may be important for participants in the software supply chain to validate whether upstream providers have reviewed the SPDX file. This can be considered as an equivalent to “signed off” or “reviewed by”. Additional reviewers can be added after the original version of the SPDX file is created and be appended append to the original file.

7.1.2 Intent: Here, as time progresses certain reviewers will begin to gain credibility as reliable. This field intends to make such information transparent.

7.1.3 Cardinality: Optional, one.

7.1.4 Data Format: single line of text with the following keywords.
 ”Person: person name” and optional “(email)” or
 ”Organization: organization” and optional “(email)” or
 ”Tool: tool identifier - version”.

7.1.5 Tag: “Reviewer:”

Example:

Reviewer: Person: Jane Doe (jane.doe@example.com)

7.1.6 RDF: property spdx:reviewer in **class** spdx:Review

Example:

```
<Review>
  <reviewer> Person: Jane Doe (jane@example.com) </reviewer>
</Review>
```

7.2 Review Date

7.2.1 Purpose: Identify when the review was done. This is to be specified according to the combined date and time in the UTC format, as specified in the ISO 8601 standard.

7.2.2 Intent: Here, the ReviewDate can serve as a verification as to when the actual review was done.

7.2.3 Cardinality: Conditional(Mandatory, one), if there is a Reviewer.

7.2.4 Data Format: YYYY-MM-DDThh:mm:ssZ
 where:

YYYY is year,
 MM is month with leading zero,

DD is day with leading zero,
T is delimiter for time,
hh is hours with leading zero in 24 hour time,
mm is minutes with leading zero,
ss is seconds with leading zero, and
Z is universal time indicator.

7.2.5 Tag: "ReviewDate:"

Example:

ReviewDate: 2010-01-29T18:30:22Z

7.2.6 RDF: property spdx:reviewDate in **class** spdx:Review

Example:

```
<Review>
  <reviewDate> 2010-01-29T18:30:22Z </reviewDate>
</Review>
```

7.3 Review Comments

7.3.1 Purpose: This optional free form multiline text field permits the reviewer to provide commentary on the analysis.

7.3.2 Intent: This allows the reviewer to provide independent assessment and note any points where there is disagreement with the analysis.

7.3.3 Cardinality: Optional, one.

7.3.4 Data Format: delimited free form text that can span multiple lines.

7.3.5 Tag: "ReviewComments:"
 In tag format multiple lines are delimited by <text> .. </text>.

Example:

```
ReviewComments: <text>
All of the licenses seen in the file, are matching what was seen during manual
inspection. There are some terms that can influence the concluded license, and some
alternatives may be possible, but the concluded license is one of the options.
</text>
```

7.3.6 RDF: property spdx:comment in **class** spdx:Review

Example:

```
<Review>
  <rdfs:comment>
    All of the licenses seen in the file, are matching what was seen during manual
    inspection. There are some terms that can influence the concluded license, and
    some alternatives may be possible, but the concluded license is one of the options.
  </rdfs:comment>
</Review>
```

Appendix I. Standard License Short Forms

The following table contains the licenses with standardized short forms that should be recognized by programs which comply to this version of the specification. The short forms have been derived from common usage identifiers, followed by the version number when known. The identifier and version should be separated by a “-”.

Additional license may be added in subsequent versions of the SPDX Specification by following the process at: <http://www.spdx.org/addlicense>. For the most up to date list, please see <http://www.spdx.org/licenses>.

Exact match, of the formal license is expected unless indicated otherwise on the SPDX.org web site.

License Identifier	Full name of License
AFL-1.1	Academic Free License v1.1
AFL-1.2	Academic Free License v1.2
AFL-2.0	Academic Free License v2.0
AFL-2.1	Academic Free License v2.1
AFL-3.0	Academic Free License v3.0
APL-1.0	Adaptive Public License 1.0
ANTLR-PD	ANTLR Software Rights Notice
Apache-1.0	Apache License 1.0
Apache-1.1	Apache License 1.1
Apache-2.0	Apache License 2.0
APSL-1.0	Apple Public Source License 1.0
APSL-1.1	Apple Public Source License 1.1
APSL-1.2	Apple Public Source License 1.2
APSL-2.0	Apple Public Source License 2.0
Artistic-1.0	Artistic License 1.0
Artistic-2.0	Artistic License 2.0
AAL	Attribution Assurance License
BSL-1.0	Boost Software License 1.0
BSD-2-Clause	BSD 2-clause "Simplified" or "FreeBSD" License
BSD-3-Clause	BSD 3-clause "New" or "Revised" License
BSD-4-Clause	BSD 4-clause "Original" or "Old" License
CECILL-1.0	CeCILL Free Software License Agreement v1.0
CECILL-1.1	CeCILL Free Software License Agreement v1.1
CECILL-2.0	CeCILL Free Software License Agreement v2.0
CECILL-B	CeCILL-B Free Software License Agreement
CECILL-C	CeCILL-C Free Software License Agreement
CIArtistic	Clarified Artistic License
CDDL-1.0	Common Development and Distribution License 1.0
CPAL-1.0	Common Public Attribution License 1.0
CPL-1.0	Common Public 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-2.0	Creative Commons Attribution 2.0
CC-BY-2.5	Creative Commons Attribution 2.5

CC-BY-3.0	Creative Commons Attribution 3.0
CC-BY-ND-1.0	Creative Commons Attribution No Derivatives 1.0
CC-BY-ND-2.0	Creative Commons Attribution No Derivatives 2.0
CC-BY-ND-2.5	Creative Commons Attribution No Derivatives 2.5
CC-BY-ND-3.0	Creative Commons Attribution No Derivatives 3.0
CC-BY-NC-1.0	Creative Commons Attribution Non Commercial 1.0
CC-BY-NC-2.0	Creative Commons Attribution Non Commercial 2.0
CC-BY-NC-2.5	Creative Commons Attribution Non Commercial 2.5
CC-BY-NC-3.0	Creative Commons Attribution Non Commercial 3.0
CC-BY-NC-ND-	Creative Commons Attribution Non Commercial No Derivatives 1.0
CC-BY-NC-ND-2.0	Creative Commons Attribution Non Commercial No Derivatives 2.0
CC-BY-NC-ND-2.5	Creative Commons Attribution Non Commercial No Derivatives 2.5
CC-BY-NC-ND-3.0	Creative Commons Attribution Non Commercial No Derivatives 3.0
CC-BY-NC-SA-1.0	Creative Commons Attribution Non Commercial Share Alike 1.0
CC-BY-NC-SA-2.0	Creative Commons Attribution Non Commercial Share Alike 2.0
CC-BY-NC-SA-2.5	Creative Commons Attribution Non Commercial Share Alike 2.5
CC-BY-NC-SA-3.0	Creative Commons Attribution Non Commercial Share Alike 3.0
CC-BY-SA-1.0	Creative Commons Attribution Share Alike 1.0
CC-BY-SA-2.0	Creative Commons Attribution Share Alike 2.0
CC-BY-SA-2.5	Creative Commons Attribution Share Alike 2.5
CC-BY-SA-3.0	Creative Commons Attribution Share Alike 3.0
CC0-1.0	Creative Commons Zero v1.0 Universal
CUA-OPL-1.0	CUA Office Public License v1.0
EPL-1.0	Eclipse Public License 1.0
eCos-2.0	eCos license version 2.0
ECL-1.0	Educational Community License v1.0
ECL-2.0	Educational Community License v2.0
EFL-1.0	Eiffel Forum License v1.0
EFL-2.0	Eiffel Forum License v2.0
Entessa	Entessa Public License
ErlPL-1.1	Erlang Public License v1.1
EUDatagrid	EU DataGrid Software License
EUPL-1.0	European Union Public License 1.0
EUPL-1.1	European Union Public License 1.1
Fair	Fair License
Frameworkx-1.0	Frameworkx Open License 1.0
AGPL-3.0	GNU Affero General Public License v3
GFDL-1.1	GNU Free Documentation License v1.1
GFDL-1.2	GNU Free Documentation License v1.2
GFDL-1.3	GNU Free Documentation License v1.3
GPL-1.0	GNU General Public License v1.0 only
GPL-1.0+	GNU General Public License v1.0 or later
GPL-2.0	GNU General Public License v2.0 only
GPL-2.0+	GNU General Public License v2.0 or later
GPL-2.0-with-autoconf-exception	GNU General Public License v2.0 w/Autoconf exception
GPL-2-with-bison-exception	GNU General Public License v2.0 w/Bison exception
GPL-2.0-with-classpath-exception	GNU General Public License v2.0 w/Classpath exception

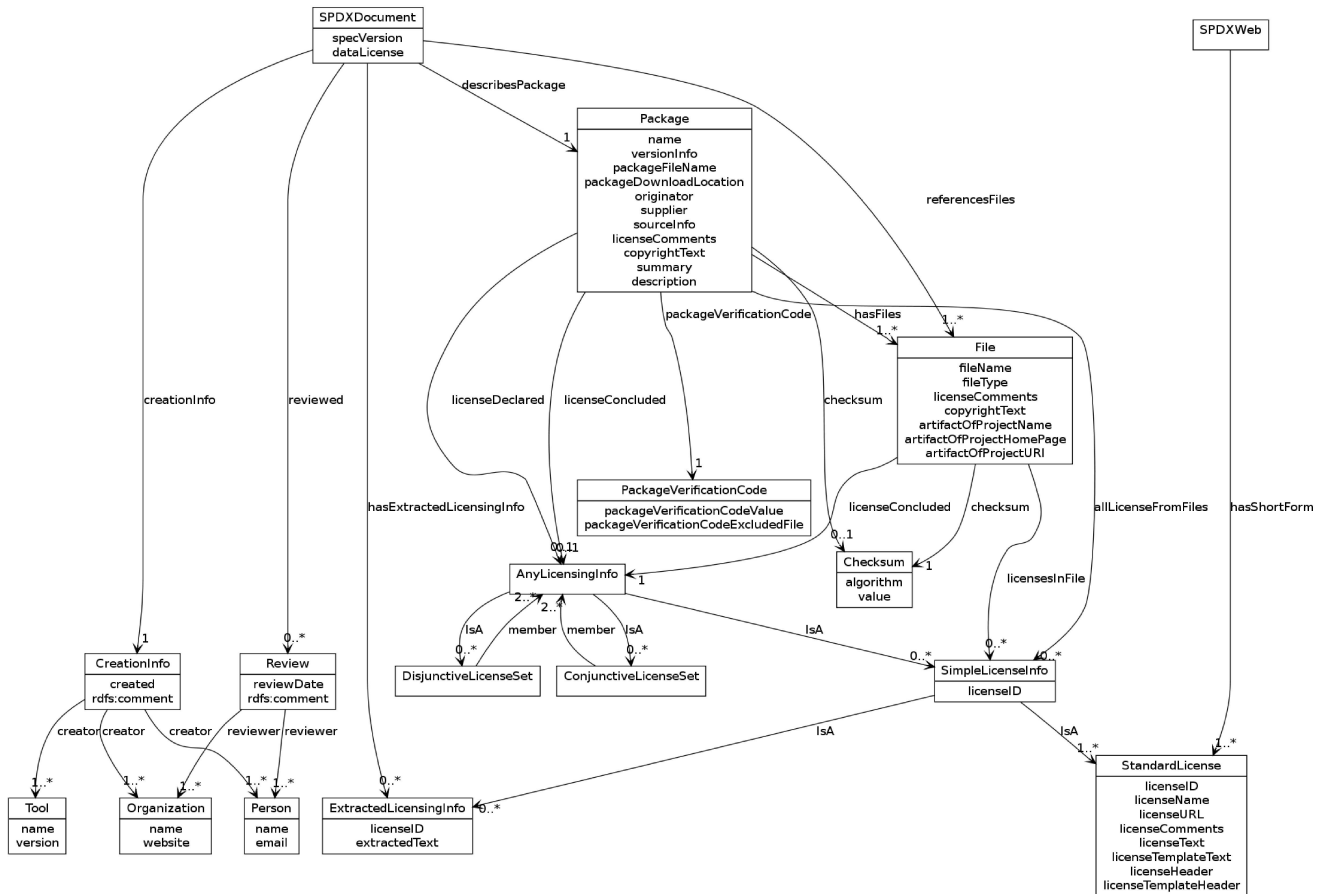
GPL-2.0-with-font-exception	GNU General Public License v2.0 w/Font exception
GPL-2.0-with-GCC-exception	GNU General Public License v2.0 w/GCC Runtime Library exception
GPL-3.0	GNU General Public License v3.0 only
GPL-3.0+	GNU General Public License v3.0 or later
GPL-3.0-with-autoconf-exception	GNU General Public License v3.0 w/Autoconf exception
GPL-3.0-with-GCC-exception	GNU General Public License v3.0 w/GCC Runtime Library exception
LGPL-2.1	GNU Lesser General Public License v2.1 only
LGPL-2.1+	GNU Lesser General Public License v2.1 or later
LGPL-3.0	GNU Lesser General Public License v3.0 only
LGPL-3.0+	GNU Lesser General Public License v3.0 or later
LGPL-2.0	GNU Library General Public License v2 only
LGPL-2.0+	GNU Library General Public License v2 or later
gSOAP-1.3b	gSOAP Public License v1.b
HPND	Historic Permission Notice and Disclaimer
IPL-1.0	IBM Public License v1.0
IPA	IPA Font License
ISC	ISC License (Bind, DHCP Server)
LPPL-1.0	LaTeX Project Public License v1.0
LPPL-1.1	LaTeX Project Public License v1.1
LPPL-1.2	LaTeX Project Public License v1.2
LPPL-1.3c	LaTeX Project Public License v1.3c
Libpng	libpng License
LPL-1.02	Lucent Public License v1.02 (Plan9)
MS-PL	Microsoft Public License
MS-RL	Microsoft Reciprocal License
MirOS	MirOS Licence
MIT	MIT license (also X11)
Motosoto	Motosoto License
MPL-1.0	Mozilla Public License 1.0
MPL-1.1	Mozilla Public License 1.1
Multics	Multics License
NASA-1.3	NASA Open Source Agreement 1.3
Nauman	Naumen Public License
NGPL	Nethack General Public License
Nokia	Nokia Open Source License
NPOSL-3.0	Non-Profit Open Software License 3.0
NTP	NTP License
OCLC-2.0	OCLC Research Public License 2.0
ODbL-1.0	ODC Open Database License v1.0
PDDL-1.0	ODC Public Domain Dedication & License 1.0
OGTSL	Open Group Test Suite License
OSL-1.0	Open Software License 1.0
OSL-2.0	Open Software License 2.0
OSL-3.0	Open Software License 3.0
OLDAP-2.8	OpenLDAP Public License v2.8
OpenSSL	OpenSSL License
PHP-3.01	PHP License v3.01

PostgreSQL	PostgreSQL License
Python-2.0	Python License 2.0
QPL-1.0	Q Public License 1.0
RPSL-1.0	RealNetworks Public Source License v1.0
RPL-1.5	Reciprocal Public License 1.5
RHeCos-1.1	Red Hat eCos Public License v1.1
RSCPL	Ricoh Source Code Public License
Ruby	Ruby License
SAX-PD	Sax Public Domain Notice
OFL-1.1	SIL Open Font License 1.1
SimPL-2.0	Simple Public License 2.0
Sleepycat	Sleepycat License
SugarCRM-1.1.3	SugarCRM Public License v1.1.3
SPL-1.0	Sun Public License v1.0
Watcom-1.0	Sybase Open Watcom Public License 1.0
NCSA	University of Illinois/NCSA Open Source License
VSL-1.0	Vovida Software License v1.0
W3C	W3C Software and Notice License
WXwindows	wxWindows Library License
Xnet	X.Net License
XFree86-1.1	XFree86 License 1.1
YPL-1.1	Yahoo! Public License v1.1
Zimbra-1.3	Zimbra Public License v1.3
Zlib	zlib License
ZPL-1.1	Zope Public License 1.1
ZPL-2.0	Zope Public License 2.0
ZPL-2.1	Zope Public License 2.1

Appendix II. RDF Data Model Implementation

Overview

The following diagram is provided to illustrate the RDF Vocabulary and provide context for relationship between the classes and properties.



Vocabulary

Version:

DRAFT (12 Aug 2011 13:37 UTC master dcea7a **with corrections**)

Latest Version:

<http://spdx.org/rdf/terms>

Copyright © 2010-2011 Linux Foundation and its Contributors. All other rights are expressly reserved.

Licensed under the [Creative Commons Attribution License 3.0 unported](#).

Abstract

This specification describes the SPDX language, defined as a dictionary of named properties and classes using W3C's RDF Technology.

SPDX is a designed to allow the exchange of data about software package. This information includes general information about the package, licensing information about the package as a whole, a manifest of files contained in the package and licensing information related to the contained files.

The `spdx` prefix used in this document expands to `http://spdx.org/rdf/terms#`. Any terms in this document without an explicit prefix may be assumed to be in the `spdx` namespace.

Other vocabularies used by this one are: [DOAP](#)

Classes

- [SpdxDocument](#)
- [CreationInfo](#)
- [Package](#)
- [ExtractedLicensingInfo](#)
- [Checksum](#)
- [PackageVerificationCode](#)
- [File](#)
- [Review](#)
- [License](#)
- [ConjunctiveLicenseSet](#)
- [DisjunctiveLicenseSet](#)
- [AnyLicenseInfo](#)
- [SimpleLicenseInfo](#)

Class: SpdxDocument

An `SdpxDocument` is a summary of the contents, provenance, ownership and licensing analysis of a specific software package. This is, effectively, the top level of SPDX information.

Status:

testing

Properties:

- [specVersion](#)
Cardinality: Mandatory, one
- [dataLicense](#)
Cardinality: Mandatory, one
- [creationInfo](#)
Cardinality: Mandatory, one
- [describesPackage](#)
Cardinality: Mandatory, one
- [hasExtractedLicensingInfo](#)
Cardinality: Optional, zero or more
- [referencesFile](#)
Cardinality: Mandatory, one or more
- [reviewed](#)
Cardinality: Optional, zero or more.

Class: CreationInfo

A CreationInfo provides information about the individuals, organizations and tools involved in the creation of an [SpdxDocument](#).

Status:

testing

Properties:

- [creator](#)
Cardinality: Mandatory, one or more
- [created](#)
Cardinality: Mandatory, one
- [rdfs:comment](#)
Cardinality: Optional, zero or one

Class: Package

A Package represents a collection of software files that are delivered as a single functional component.

Status:

testing

Properties:

- [name](#)
Cardinality: Mandatory, one

- [versionInfo](#)
Cardinality: Optional, zero or one
- [packageFileName](#)
Cardinality: Mandatory, one
- [supplier](#)
Cardinality: Optional, zero or one
- [originator](#)
Cardinality: Optional, zero or one
- [downloadLocation](#)
Cardinality: Mandatory, one
- [packageVerificationCode](#)
Cardinality: Mandatory, one
- [checksum](#)
Cardinality: Optional, zero or one
- [sourceInfo](#)
Cardinality: Optional, zero or one
- [licenseConcluded](#)
Cardinality: Mandatory, one
- [licenseInfoFromFiles](#)
Cardinality: Mandatory, one or more
- [licenseDeclared](#)
Cardinality: Mandatory, one
- [licenseComments](#)
Cardinality: Optional, zero or one
- [copyrightText](#)
Cardinality: Mandatory, one
- [summary](#)
Cardinality: Optional, zero or one
- [description](#)
Cardinality: Optional, zero or one
- [hasFile](#)
Cardinality: Mandatory, one or more

Class: ExtractedLicensingInfo

An ExtractedLicensingInfo represents a license or licensing notice that was found in the package. Any license text that is recognized as a license may be represented as a [License](#) rather than an ExtractedLicensingInfo.

Status:

testing

Properties:

- [licenseId](#)
Cardinality: Mandatory, one
- [extractedText](#)
Cardinality: Mandatory, one

Class: File

A File represents a named sequence of information that is contained in a software package.

Status:

testing

Properties:

- [fileName](#)
Cardinality: Mandatory, one
- [fileType](#)
Cardinality: Optional, zero or one
- [checksum](#)
Cardinality: Mandatory, one
- [licenseConcluded](#)
Cardinality: Mandatory, one
- [licenseInfoInFile](#)
Cardinality: Mandatory, one or more
- [licenseComments](#)
Cardinality: Optional, zero or one
- [copyrightText](#)
Cardinality: Mandatory, one
- [artifactOf](#)
Cardinality: Optional, zero or one

Class: Review

A Review represents an audit and signoff by an individual, organization or tool on the information in an [SpdxDocument](#).

Status:

testing

Properties:

- [reviewer](#)
Cardinality: Mandatory, one
- [reviewDate](#)
Cardinality: Mandatory, one
- [rdfs:comment](#)
Cardinality: Optional, zero or one

Class: License

A License represents a software copyright license. This class is used by the SPDX license list to represent standard licenses.

Status:

testing

Properties:

- [licenseId](#)
Cardinality: Mandatory, one
- [licenseText](#)
Cardinality: Mandatory, one

Class: Checksum

A Checksum is simple value that allows the contents of a file to be authenticated. Even small changes to the content of the file will change it's checksum value.

Status:

testing

Properties:

- [algorithm](#)
Cardinality: Mandatory, one
- [checksumValue](#)
Cardinality: Mandatory, one

Class: PackageVerificationCode

A PackageVerificationCode is a value that allows authentication of the package. This differs from the [Checksum](#) in that it uses an algorithm that allows the SPDX file to be embedded in the package. This verification code is produced using a cryptographic hash algorithm applied to a manifest of the package. Some files in the package (e.g. the SPDX files) are explicitly excluded from the verification code. This allows those excluded files to not impact the verification code.

Status:

testing

Properties:

- [packageVerificationCodeExcludedFile](#)
Cardinality: Optional, zero or more
- [packageVerificationCodeValue](#)
Cardinality: Mandatory, one

Class: ConjunctiveLicenseSet

A ConjunctiveLicenseSet represents a set of [licensing information](#) all of which apply.

This class refines [rdfs:Container](#).

Status:

testing

Properties:

- [member](#)
Cardinality: Mandatory, two or more.

Class: DisjunctiveLicenseSet

A DisjunctiveLicenseSet represents a set of [licensing information](#) where only one license applies at a time. This class implies that the recipient gets to choose one of these licenses they would prefer to use.

This class refines [rdfs:Container](#).

Status:

testing

Properties:

- [member](#)
Cardinality: Mandatory, two or more.

Class: AnyLicenseInfo

The AnyLicenseInfo class includes all resources that represent licensing information.

Status:

testing

Members

All resources in any of the following classes:

- [License](#)
- [ExtractedLicensingInfo](#)
- [ConjunctiveLicenseSet](#)
- [DisjunctiveLicenseSet](#)

Class: SimpleLicenseInfo

The SimpleLicenseInfo class includes all resources that represent simple, atomic, licensing information.

Status:

testing

Members

All resources in any of the following classes:

- [License](#)
- [ExtractedLicensingInfo](#)

Properties

- [algorithm](#)
- [artifactOf](#)
- [checksum](#)
- [checksumValue](#)
- [copyrightText](#)
- [created](#)
- [creationInfo](#)
- [creator](#)
- [dataLicense](#)
- [describesPackage](#)
- [description](#)
- [downloadLocation](#)
- [extractedText](#)
- [fileName](#)
- [fileType](#)
- [hasExtractedLicensingInfo](#)
- [hasFile](#)
- [licenseComments](#)
- [licenseConcluded](#)
- [licenseDeclared](#)
- [licenseId](#)
- [licenseText](#)
- [licenseInfoFromFiles](#)
- [licenseInfoInFile](#)
- [member](#)
- [name](#)

- [originator](#)
- [packageFileName](#)
- [packageVerificationCode](#)
- [packageVerificationCodeExcludedFile](#)
- [packageVerificationCodeValue](#)
- [referencesFile](#)
- [reviewDate](#)
- [reviewed](#)
- [reviewer](#)
- [sourceInfo](#)
- [specVersion](#)
- [summary](#)
- [supplier](#)
- [versionInfo](#)

Property: `algorithm`

Identifies the algorithm used to produce the subject [checksum](#).

Currently, [SHA-1](#) is the only supported algorithm. It is anticipated that other algorithms will be supported at a later time.

Status:

testing

Domain:

[Checksum](#)

Range:

[spdx:checksumAlgorithm_sha1](#)

Property: `artifactOf`

Indicates the project in which the file originated.

Tools must preserve `doap:homepage` and `doap:name` properties and the URI (if one is known) of `doap:Project` resources that are values of this property. All other properties of `doap:Projects` are not directly supported by SPDX and may be dropped when translating to or from some SPDX formats.

Status:

testing

Domain:

[File](#)

Range:

[doap:Project](#)

Property: checksum

The checksum property provides a mechanism that can be used to verify that the contents of a [File](#) or [Package](#) have not changed.

Status:

testing

Domain:

Any of:

- [Package](#)
- [File](#)

Range:

[Checksum](#)

Property: checksumValue

The checksumValue property provides a lower case hexadecimal encoded digest value produced using a specific algorithm.

Status:

testing

Domain:

[Checksum](#)

Range:

[xsd:hexBinary](#)

Property: created

The date and time at which the [SpdxDocument](#) was created. This value must in UTC and have 'Z' as its timezone indicator.

Status:

testing

Domain:

[CreationInfo](#)

Range:

[xsd:dateTime](#)

Property: copyrightText

The text of copyright declarations recited in the [Package](#) or [File](#).

Status:

testing

Domain:

Any of:

- [Package](#)
- [File](#)

Range:

Any of:

- [rdfs:Literal](#)
- [spdx:none](#)
- [spdx:noassertion](#)

Property: creationInfo

The creationInfo property relates an [SpdxDocument](#) to a set of information about the creation of the [SpdxDocument](#).

Status:

testing

Domain:

[SpdxDocument](#)

Range:

[CreationInfo](#)

Property: creator

The name and, optionally, contact information of a person, organization or tool that created, or was used to create, the [SpdxDocument](#).

Status:

testing

Domain:

[CreationInfo](#)

Range:

[xsd:string](#)

Property: dataLicense

The licensing under which the [creator](#) of this SPDX document allows related data to be reproduced.

The only valid value for this property is <http://spdx.org/licenses/PDDL-1.0>. This is to alleviate any concern that content (the data) in an SPDX file is subject to any form of intellectual property right that could restrict the re-use of the information or the creation of another SPDX file for the same project(s). This approach avoids intellectual property and related restrictions over the SPDX file, however individuals can still contract one to one to restrict release of specific collections of SPDX files (which map to software bill of materials) and the identification of the supplier of SPDX files.

Status:

testing

Domain:

[SpdxDocument](#)

Range:

[AnyLicenseInfo](#)

Property: `describesPackage`

The `describesPackage` property relates an `SpdxDocument` to the package which it describes.

Status:

testing

Domain:

[SpdxDocument](#)

Range:

[Package](#)

Property: `description`

Provides a detailed description of the [package](#).

Status:

testing

Domain:

[Package](#)

Range:

[xsd:string](#)

Property: `downloadLocation`

The URI at which this package is available for download. Private (i.e., not publicly reachable) URIs are acceptable as values of this property.

The values <http://spdx.org/rdf/terms#none> and <http://spdx.org/rdf/terms#noassertion> may be used to specify that the package is not downloadable or that no attempt was made to determine its download location, respectively.

Status:

testing

Domain:

[Package](#)

Range:

[xsd:anyURI](#)

Property: `extractedText`

Verbatim license or licensing notice text that was discovered.

Status:

testing

Domain:

[ExtractedLicensingInfo](#)

Range:

[xsd:string](#)

Property: fileName

The name of the file relative to the root of the package.

Status:

testing

Domain:

[File](#)

Range:

[xsd:string](#)

Property: fileType

The type of the file.

Status:

testing

Domain:

[File](#)

Range:

One of:

- [spdx:fileType_source](#)

Indicates the file is a source code file.

- [spdx:fileType_archive](#)

Indicates the file is an archive file.

- [spdx:fileType_binary](#)

Indicates the file is not a text file. `filetype_archive` is preferred for archive files even though they are binary.

- [spdx:fileType_other](#)

Indicates the file did not fall into any of the other categories.

Property: hasExtractedLicensingInfo

Indicates that a particular [ExtractedLicensingInfo](#) was defined in the subject [SpxDocument](#).

Status:

testing

Domain:

[SpdxDocument](#)

Range:

[ExtractedLicensingInfo](#)

Property: **hasFile**

Indicates that a particular [file](#) belongs to a [package](#).

Status:

testing

Domain:

[Package](#)

Range:

[File](#)

Property: **licenseComments**

The `licenseComments` property allows the preparer of the SPDX document to describe why the licensing in [spdx:licenseConcluded](#) was chosen.

Status:

testing

Domain:

Any of:

- [Package](#)
- [File](#)

Range:

[xsd:string](#)

Property: **licenseConcluded**

The licensing that the preparer of this SPDX document has concluded, based on the evidence, actually applies to the package.

Status:

testing

Domain:

Any of:

- [Package](#)
- [File](#)

Range:

Any of:

- [AnyLicenseInfo](#)
- [spdx:none](#)
- [spdx:noassertion](#)

Property: licenseDeclared

The licensing that is declared by the authors of the package.

Status:

testing

Domain:

[Package](#)

Range:

Any of:

- [AnyLicenseInfo](#)
- [spdx:none](#)
- [spdx:noassertion](#)

Property: licenseId

A short name for the license that is at least 3 characters long and made up of the characters from the set 'a'-z', 'A'-Z', '0'-9', '+', '_', '.', and '-'. Formally, all `licenseId` values must match the regular expression: `[-+_ .a-zA-Z0-9]{3,}`

Status:

testing

Domain:

- [License](#)
- [ExtractedLicensingInfo](#)

Range:

[xsd:string](#)

Property: licenseText

The full text of the license.

Status:

testing

Domain:

[License](#)

Range:

[xsd:string](#)

Property: licenseInfoFromFiles

The licensing information that was discovered directly within the package. There will be an instance of this property for each distinct value of all [licenseInfoInFile](#) properties of all the files contained in the package.

Status:

testing

Domain:

[Package](#)

Range:

Any of:

- [SimpleLicenseInfo](#)
- [spdx:none](#)
- [spdx:noassertion](#)

Property: **licenseInfoInFile**

Licensing information that was discovered directly in the subject [File](#).

Status:

testing

Domain:

[File](#)

Range:

Any of:

- [SimpleLicenseInfo](#)
- [spdx:none](#)
- [spdx:noassertion](#)

Property: **member**

A [license](#), or other licensing information, that is a member of the subject license set.

Status:

testing

Domain:

Any of:

- [ConjunctiveLicenseSet](#)
- [DisjunctiveLicenseSet](#)

Range:

[AnyLicenseInfo](#)

Refines:

[rdfs:member](#)

Property: **name**

The full name of the package including version information.

Status:

testing

Domain:

[Package](#)

Range:

[xsd:string](#)

Property: packageFileName

The base name of the package file name. For example, `zlib-1.2.5.tar.gz`.

Status:

testing

Domain:

[Package](#)

Range:

[xsd:string](#)

Property: packageVerificationCode

A manifest based **verification code** (the algorithm is defined in section 4.7 of the full specification) of the package. This allows consumers of this **data and/or database** to determine if a package they have in hand is identical to the package from which the data was produced. This algorithm works even if the SPDX document is included in the package. This algorithm is described in detail in the SPDX **specification**.

Status:

testing

Domain:

[Package](#)

Range:

[PackageVerificationCode](#)

Property: packageVerificationCodeExcludedFile

A file that was excluded when calculating the package verification code. This is usually a file containing SPDX data regarding the package. If a package contains more than one SPDX file, all SPDX files must be excluded from the package verification code. If this is not done each recalculation of the package verification code in one file will require the other to be recalculated to be valid which will require the original which will require the original file's be recalculated **recursively**.

Status:

testing

Domain:

[PackageVerificationCode](#)

Range:

[xsd:string](#)

Property: packageVerificationCodeValue

The actual package verification code as a hex encoded value.

Status:

testing

Domain:

[PackageVerificationCode](#)

Range:

[xsd:hexBinary](#)

Property: originator

The name and, optionally, contact information of the person or organization that originally created the package.

Status:

testing

Domain:

[Package](#)

Range:

Any of:

- [xsd:string](#)
- [spdx:noassertion](#)

Property: referencesFile

Indicates that a particular file belongs as part of the set of analyzed files in [SpdxDocument](#).

Status:

testing

Domain:

[SpdxDocument](#)

Range:

[File](#)

Property: reviewDate

The date and time at which the [SpdxDocument](#) was reviewed. This value must be in UTC and have 'Z' as its timezone indicator.

Status:

testing

Domain:

[Review](#)

Range:

[xsd:dateTime](#)

Property: reviewed

The review property relates a SpdxDocument to the review history.

Status:
testing
Domain:
[SpdxDocument](#)
Range:
[Review](#)

Property: reviewer

The name and, optionally, contact information of the person who performed the review.

Status:
testing
Domain:
[Review](#)
Range:
[xsd:string](#)

Property: sourceInfo

Allows the producer(s) of the SPDX document to describe how the package was acquired and/or changed from the original source.

Status:
testing
Domain:
[Package](#)
Range:
[xsd:string](#)

Property: specVersion

Identifies the version of this specification that was used to produce this SPDX document. Currently the only supported value is `SPDX-1.0`.

Status:
testing
Domain:
[SpdxDocument](#)
Range:
[xsd:string](#)

Property: summary

Provides a short description of the [package](#).

Status:
testing
Domain:
[Package](#)
Range:
[xsd:string](#)

Property: **supplier**

The name, and optionally the contact information, of the person or organization who was the immediate supplier of the package to the distributee.

Values of this property must conform to the [agent and tool syntax](#).

Status:
testing
Domain:
[Package](#)
Range:
Any of:

- [xsd:string](#)
- [spdx:noassertion](#)

Property: **versionInfo**

Provides an indication of the version of the package that is described by this [SpdxDocument](#).

Status:
testing
Domain:
[Package](#)
Range:
[xsd:string](#)

Individuals

- [checksumAlgorithm_sha1](#)
- [fileType_archive](#)
- [fileType_binary](#)
- [fileType_other](#)
- [fileType_source](#)
- [noassertion](#)
- [none](#)

Individual: checksumAlgorithm_sha1

Indicates the algorithm used was [SHA-1](#)

Status:
testing

Individual: fileType_archive

Indicates the file is an archive file.

Status:
testing

Individual: fileType_binary

Indicates the file is not a text file. [spdx:filetype_archive](#) is preferred for archive files even though they are binary.

Status:
testing

Individual: fileType_other

Indicates the file is not a [source](#), [archive](#) or [binary](#) file.

Status:
testing

Individual: fileType_source

Indicates the file is a source code file.

Status:
testing

Individual: none

When this value is used as the object of a property it indicates that the preparer of the [SpdxDocument](#) believes that there is no value for the property. This value should only be used if there is sufficient evidence to support this assertion.

Status:
testing

Individual: noassertion

Indicates that the preparer of the SPDX document is not making any assertion regarding the value of this field.

Status:
testing

Agent and Tool Identifiers

Fields that identify entities that have acted in relation to the SPDX file are single line of text which name the agent or tool and, optionally, provide contact information. For example, "Person: Jane Doe (jane.doe@example.com)", "Organization: ExampleCodeInspect (contact@example.com)" and "Tool: LicenseFind - 1.0". The exact syntax of agent and tool identifications is described below in [ABNF](#).

For example,
"Person: Jane Doe ([jane.doe@example.com](#))",
"Organization: ExampleCodeInspect ([contact@example.com](#))" and
"Tool: LicenseFind – 1.0".

The syntax of agent and tool identifications is described below in ABNF[1].

```

Agent           = person / organization

person          = "Person: " name 0*1contact-info
organization    = "Organization: " name 0*1contact-info
name            = 1*( unreserved ) / U+0022 1*( vchar-sans-quote ) U+0022
contact-info   = " (" email-addr ")"
email-addr     = *( atext / "." ) atext "@" ldh-str 1*( "." ldh-str )

tool           = "Tool: " name 0*1( " " dash " " version)
version        = 1*vchar-sans-quote

dash           = U+2010 / U+2212 / ; hyphen, minus,
                U+2013 / U+2014 ; em dash and en dash

unreserved     = U+0020-U+0027 / ; visible unicode characters
                U+0029-U+0080 / ; except '(' and dashes
                U+00A0-U+200F /
                U+2011-U+2027 /
                U+202A-U+2211 /

```

U+2213-U+E01EF

vchar-sans-quote = U+0020-U+0021 / ; visible unicode characters
 U+0023-U+0080 / ; except quotation mark
 U+00a0-U+E01EF

atext = ALPHA / DIGIT /; Printable US-ASCII
 "!" / "#" / ; characters not including
 "\$" / "%" / ; specials. Used for atoms.
 "&" / "'" /
 "*" / "+" /
 "-" / "/" /
 "=" / "?" /
 "^" / " " /
 "`" / "{" /
 "|" / "}" /
 "~"

ldh-str = ALPHA / DIGIT / "-"

Appendix III. Creative Commons Attribution License 3.0 Unported

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. Definitions

- a. **"Adaptation"** means a work based upon the Work, or upon the Work and other pre-existing works, such as a translation, adaptation, derivative work, arrangement of music or other alterations of a literary or artistic work, or phonogram or performance and includes cinematographic adaptations or any other form in which the Work may be recast, transformed, or adapted including in any form recognizably derived from the original, except that a work that constitutes a Collection will not be considered an Adaptation for the purpose of this License. For the avoidance of doubt, where the Work is a musical work, performance or phonogram, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered an Adaptation for the purpose of this License.
- b. **"Collection"** means a collection of literary or artistic works, such as encyclopedias and anthologies, or performances, phonograms or broadcasts, or other works or subject matter other than works listed in Section 1(f) below, which, by reason of the selection and arrangement of their contents, constitute intellectual creations, in which the Work is included in its entirety in unmodified form along with one or more other contributions, each constituting separate and independent works in themselves, which together are assembled into a collective whole. A work that constitutes a Collection will not be considered an Adaptation (as defined above) for the purposes of this License.
- c. **"Distribute"** means to make available to the public the original and copies of the Work or Adaptation, as appropriate, through sale or other transfer of ownership.
- d. **"Licensor"** means the individual, individuals, entity or entities that offer(s) the Work under the terms of this License.
- e. **"Original Author"** means, in the case of a literary or artistic work, the individual, individuals, entity or entities who created the Work or if no individual or entity can be identified, the publisher; and in addition (i) in the case of a performance the actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, interpret or otherwise perform literary or artistic works or expressions of folklore; (ii) in the case of a phonogram the producer being the person or legal entity who first fixes the sounds of a performance or other sounds; and, (iii) in the case of broadcasts, the organization that transmits the broadcast.
- f. **"Work"** means the literary and/or artistic work offered under the terms of this License including without limitation any production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression including digital form, such as a book, pamphlet and other writing; a lecture, address, sermon or other work of the same nature; a dramatic or dramatico-musical work; a choreographic work or entertainment in dumb show; a musical composition with or without words; a cinematographic work to which are assimilated works expressed by a process analogous to cinematography; a work of drawing, painting, architecture, sculpture, engraving or lithography; a photographic work to which are assimilated works expressed by a process analogous to photography; a work of applied art; an illustration, map, plan, sketch or three-dimensional work relative to geography, topography, architecture or science; a performance; a broadcast; a phonogram; a compilation of data to the extent it is protected as a copyrightable work; or a work performed by a variety or circus performer to the extent it is not otherwise considered a literary or artistic work.
- g. **"You"** means an individual or entity exercising rights under this License who has not previously violated

the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

- h. **"Publicly Perform"** means to perform public recitations of the Work and to communicate to the public those public recitations, by any means or process, including by wire or wireless means or public digital performances; to make available to the public Works in such a way that members of the public may access these Works from a place and at a place individually chosen by them; to perform the Work to the public by any means or process and the communication to the public of the performances of the Work, including by public digital performance; to broadcast and rebroadcast the Work by any means including signs, sounds or images.
- i. **"Reproduce"** means to make copies of the Work by any means including without limitation by sound or visual recordings and the right of fixation and reproducing fixations of the Work, including storage of a protected performance or phonogram in digital form or other electronic medium.

2. Fair Dealing Rights. Nothing in this License is intended to reduce, limit, or restrict any uses free from copyright or rights arising from limitations or exceptions that are provided for in connection with the copyright protection under copyright law or other applicable laws.

3. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

- a. to Reproduce the Work, to incorporate the Work into one or more Collections, and to Reproduce the Work as incorporated in the Collections;
- b. to create and Reproduce Adaptations provided that any such Adaptation, including any translation in any medium, takes reasonable steps to clearly label, demarcate or otherwise identify that changes were made to the original Work. For example, a translation could be marked "The original work was translated from English to Spanish," or a modification could indicate "The original work has been modified.";
- c. to Distribute and Publicly Perform the Work including as incorporated in Collections; and,
- d. to Distribute and Publicly Perform Adaptations.
- e. For the avoidance of doubt:
 - i. **Non-waivable Compulsory License Schemes.** In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme cannot be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License;
 - ii. **Waivable Compulsory License Schemes.** In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme can be waived, the Licensor waives the exclusive right to collect such royalties for any exercise by You of the rights granted under this License; and,
 - iii. **Voluntary License Schemes.** The Licensor waives the right to collect royalties, whether individually or, in the event that the Licensor is a member of a collecting society that administers voluntary licensing schemes, via that society, from any exercise by You of the rights granted under this License.

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. Subject to Section 8(f), all rights not expressly granted by Licensor are hereby reserved.

4. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

- a. You may Distribute or Publicly Perform the Work only under the terms of this License. You must include a copy of, or the Uniform Resource Identifier (URI) for, this License with every copy of the Work You

Distribute or Publicly Perform. You may not offer or impose any terms on the Work that restrict the terms of this License or the ability of the recipient of the Work to exercise the rights granted to that recipient under the terms of the License. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties with every copy of the Work You Distribute or Publicly Perform. When You Distribute or Publicly Perform the Work, You may not impose any effective technological measures on the Work that restrict the ability of a recipient of the Work from You to exercise the rights granted to that recipient under the terms of the License. This Section 4(a) applies to the Work as incorporated in a Collection, but this does not require the Collection apart from the Work itself to be made subject to the terms of this License. If You create a Collection, upon notice from any Licensor You must, to the extent practicable, remove from the Collection any credit as required by Section 4(b), as requested. If You create an Adaptation, upon notice from any Licensor You must, to the extent practicable, remove from the Adaptation any credit as required by Section 4(b), as requested.

- b. If You Distribute, or Publicly Perform the Work or any Adaptations or Collections, You must, unless a request has been made pursuant to Section 4(a), keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or if the Original Author and/or Licensor designate another party or parties (e.g., a sponsor institute, publishing entity, journal) for attribution ("Attribution Parties") in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; (ii) the title of the Work if supplied; (iii) to the extent reasonably practicable, the URI, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work; and (iv) , consistent with Section 3(b), in the case of an Adaptation, a credit identifying the use of the Work in the Adaptation (e.g., "French translation of the Work by Original Author," or "Screenplay based on original Work by Original Author"). The credit required by this Section 4 (b) may be implemented in any reasonable manner; provided, however, that in the case of a Adaptation or Collection, at a minimum such credit will appear, if a credit for all contributing authors of the Adaptation or Collection appears, then as part of these credits and in a manner at least as prominent as the credits for the other contributing authors. For the avoidance of doubt, You may only use the credit required by this Section for the purpose of attribution in the manner set out above and, by exercising Your rights under this License, You may not implicitly or explicitly assert or imply any connection with, sponsorship or endorsement by the Original Author, Licensor and/or Attribution Parties, as appropriate, of You or Your use of the Work, without the separate, express prior written permission of the Original Author, Licensor and/or Attribution Parties.
- c. Except as otherwise agreed in writing by the Licensor or as may be otherwise permitted by applicable law, if You Reproduce, Distribute or Publicly Perform the Work either by itself or as part of any Adaptations or Collections, You must not distort, mutilate, modify or take other derogatory action in relation to the Work which would be prejudicial to the Original Author's honor or reputation. Licensor agrees that in those jurisdictions (e.g. Japan), in which any exercise of the right granted in Section 3(b) of this License (the right to make Adaptations) would be deemed to be a distortion, mutilation, modification or other derogatory action prejudicial to the Original Author's honor and reputation, the Licensor will waive or not assert, as appropriate, this Section, to the fullest extent permitted by the applicable national law, to enable You to reasonably exercise Your right under Section 3(b) of this License (right to make Adaptations) but not otherwise.

5. Representations, Warranties and Disclaimer

UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT

WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

- a. This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Adaptations or Collections from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.
- b. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous

- a. Each time You Distribute or Publicly Perform the Work or a Collection, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.
- b. Each time You Distribute or Publicly Perform an Adaptation, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.
- c. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.
- d. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.
- e. This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.
- f. The rights granted under, and the subject matter referenced, in this License were drafted utilizing the terminology of the Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979), the Rome Convention of 1961, the WIPO Copyright Treaty of 1996, the WIPO Performances and Phonograms Treaty of 1996 and the Universal Copyright Convention (as revised on July 24, 1971). These rights and subject matter take effect in the relevant jurisdiction in which the License terms are sought to be enforced according to the corresponding provisions of the implementation of those treaty provisions in the applicable national law. If the standard suite of rights granted under applicable copyright law includes additional rights not granted under this License, such additional rights are deemed to be included in the License; this License is not intended to restrict the license of any rights under applicable law.