INTERNATIONAL STANDARD

ISO/IEC 5962

First edition
2021-08

Information technology — SPDX® Specification V2.2.1

Technologies de l'information — Spécification SPDX® V2.2.1

Reference number
ISO/IEC 5962:2021(E)

Documents
Document Sharing Hub
© ISO/IEC 2021

Full document details: ISO_IEC 5962_2021

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC 5962_2021

Contents

Foreword ... xiii
Introduction ... xiii
1 Scope ... 1
2 Normative references ... 1
3 Terms and definitions ... 2
4 Conformance ... 3
4.1 SPDX Current and Previous Versions ... 3
4.2 Obsolete features ... 3
4.3 Alternate notation for some conformance requirements ... 3
4.4 Standard data format requirements ... 4
4.5 Trademark Compliance ... 5
4.6 The SPDX Lite profile ... 5
5 Composition of an SPDX document ... 6
5.1 What this specification covers ... 6
5.2 Sections ... 7
5.2.1 SPDX document creation information section ... 7
5.2.2 Package information section ... 7
5.2.3 File information section ... 8
5.2.4 Snippet information section ... 8
5.2.5 Other licensing information detected section ... 9
5.2.6 Relationships between SPDX elements information section ... 9
5.2.7 Annotations information section ... 9
5.2.8 Review information section ... 9
5.3 What this specification does not cover ... 10
6 SPDX document creation information section ... 10
6.1 SPDX version field ... 10
6.1.1 Description ... 10
6.1.2 Intent ... 10
6.1.3 Examples ... 10
6.2 Data license field ... 11
6.2.1 Description ... 11
6.2.2 Intent ... 11
6.2.3 Examples ... 11
6.3 SPDX identifier field ... 12
6.3.1 Description ... 12
6.3.2 Intent ... 12
6.3.3 Examples ... 12
6.4 Document name field ... 12
6.4.1 Description ... 12
6.4.2 Intent ... 13
6.4.3 Examples ... 13
6.5 SPDX document namespace field ... 13
6.5.1 Description ... 13
6.5.2 Intent ... 14
6.5.3 Examples ... 15
6.6 External document references field ... 15
6.6.1 Description ... 15
6.6.2 Intent ... 15

© ISO/IEC 2021 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

6.6.3 Examples 16
6.7 License list version field 16
6.7.1 Description 16
6.7.2 Intent 17
6.7.3 Examples 17
6.8 Creator field 17
6.8.1 Description 17
6.8.2 Intent 18
6.8.3 Examples 18
6.9 Created field 18
6.9.1 Description 18
6.9.2 Intent 19
6.9.3 Examples 19
6.10 Creator comment field 19
6.10.1 Description 19
6.10.2 Intent 20
6.10.3 Examples 20
6.11 Document comment field 20
6.11.1 Description 20
6.11.2 Intent 21
6.11.3 Examples 21

7 Package information section 21
7.1 Package name field 21
7.1.1 Description 21
7.1.2 Intent 21
7.1.3 Examples 21
7.2 Package SPDX identifier field 22
7.2.1 Description 22
7.2.2 Intent 22
7.2.3 Examples 22
7.3 Package version field 23
7.3.1 Description 23
7.3.2 Intent 23
7.3.3 Examples 23
7.4 Package file name field 23
7.4.1 Description 23
7.4.2 Intent 24
7.4.3 Examples 24
7.5 Package supplier field 24
7.5.1 Description 24
7.5.2 Intent 25
7.5.3 Examples 25
7.6 Package originator field 25
7.6.1 Description 25
7.6.2 Intent 26
7.6.3 Examples 26
7.7 Package download location field 27
7.7.1 Description 27
7.7.2 Intent 28
7.7.3 Examples 28
7.8 Files analyzed field 32
7.8.1 Description 32
7.8.2 Intent 32
7.8.3 Examples 33

AVA Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: ISO_IEC 5962_2021

7.9 Package verification code field ... 33
7.9.1 Description ... 33
7.9.2 Intent ... 34
7.9.3 Examples ... 34
7.10 Package checksum field ... 35
7.10.1 Description ... 35
7.10.2 Intent ... 35
7.10.3 Examples ... 35
7.11 Package home page field ... 36
7.11.1 Description ... 36
7.11.2 Intent ... 37
7.11.3 Examples ... 37
7.12 Source information field ... 37
7.12.1 Description ... 37
7.12.2 Intent ... 38
7.12.3 Examples ... 38
7.13 Concluded license field ... 38
7.13.1 Description ... 38
7.13.2 Intent ... 39
7.13.3 Examples ... 39
7.14 All licenses information from files field ... 40
7.14.1 Description ... 40
7.14.2 Intent ... 40
7.14.3 Examples ... 41
7.15 Declared license field ... 41
7.15.1 Description ... 41
7.15.2 Intent ... 42
7.15.3 Examples ... 42
7.16 Comments on license field ... 43
7.16.1 Description ... 43
7.16.2 Intent ... 43
7.16.3 Examples ... 43
7.17 Copyright text field ... 44
7.17.1 Description ... 44
7.17.2 Intent ... 44
7.17.3 Examples ... 44
7.18 Package summary description field ... 45
7.18.1 Description ... 45
7.18.2 Intent ... 45
7.18.3 Examples ... 45
7.19 Package detailed description field ... 45
7.19.1 Description ... 45
7.19.2 Intent ... 46
7.19.3 Examples ... 46
7.20 Package comment field ... 46
7.20.1 Description ... 46
7.20.2 Intent ... 47
7.20.3 Examples ... 47
7.21 External reference field ... 47
7.21.1 Description ... 47
7.21.2 Intent ... 48
7.21.3 Examples ... 48
7.22 External reference comment field ... 49
7.22.1 Description ... 49

Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: ISO_IEC 5962_2021

7.22.2 Intent 49
7.22.3 Examples 50
7.23 Package attribution text field 50
7.23.1 Description 50
7.23.2 Intent 51
7.23.3 Examples 51

8 File information section 51
8.1 File name field 51
8.1.1 Description 51
8.1.2 Intent 52
8.1.3 Examples 52
8.2 File SPDX identifier field 52
8.2.1 Description 52
8.2.2 Intent 52
8.2.3 Examples 52
8.3 File type field 53
8.3.1 Description 53
8.3.2 Intent 54
8.3.3 Examples 54
8.4 File checksum field 54
8.4.1 Description 54
8.4.2 Intent 55
8.4.3 Examples 55
8.5 Concluded license field 56
8.5.1 Description 56
8.5.2 Intent 56
8.5.3 Examples 56
8.6 License information in file field 57
8.6.1 Description 57
8.6.2 Intent 58
8.6.3 Examples 58
8.7 Comments on license field 58
8.7.1 Description 58
8.7.2 Intent 59
8.7.3 Examples 59
8.8 Copyright text field 59
8.8.1 Description 59
8.8.2 Intent 60
8.8.3 Examples 60
8.9 Artifact of project name field (deprecated) 60
8.9.1 Description 60
8.9.2 Intent 61
8.9.3 Examples 61
8.10 Artifact of project homepage field (deprecated) 61
8.10.1 Description 61
8.10.2 Intent 61
8.10.3 Examples 61
8.11 Artifact of project uniform resource identifier field (deprecated) 62
8.11.1 Description 62
8.11.2 Intent 62
8.11.3 Examples 62
8.12 File comment field 63
8.12.1 Description 63
8.12.2 Intent 63

AVA Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: ISO_IEC 5962_2021

8.12.3 Examples ... 63
8.13 File notice field ... 63
8.13.1 Description ... 63
8.13.2 Intent ... 64
8.13.3 Examples ... 64
8.14 File contributor field ... 64
8.14.1 Description ... 64
8.14.2 Intent ... 64
8.14.3 Examples ... 65
8.15 File attribution text field ... 65
8.15.1 Description ... 65
8.15.2 Intent ... 65
8.15.3 Examples ... 66
8.16 File dependencies field (deprecated) ... 66
8.16.1 Description ... 66
8.16.2 Intent ... 66
8.16.3 Examples ... 67

9 Snippet information section ... 67
9.1 Snippet SPDX identifier field ... 67
9.1.1 Description ... 67
9.1.2 Intent ... 68
9.1.3 Examples ... 68
9.2 Snippet from file SPDX identifier field ... 68
9.2.1 Description ... 68
9.2.2 Intent ... 69
9.2.3 Examples ... 69
9.3 Snippet byte range field ... 70
9.3.1 Description ... 70
9.3.2 Intent ... 70
9.3.3 Examples ... 70
9.4 Snippet line range field ... 71
9.4.1 Description ... 71
9.4.2 Intent ... 71
9.4.3 Examples ... 71
9.5 Snippet concluded license field ... 72
9.5.1 Description ... 72
9.5.2 Intent ... 73
9.5.3 Examples ... 73
9.6 License information in snippet field ... 74
9.6.1 Description ... 74
9.6.2 Intent ... 75
9.6.3 Examples ... 75
9.7 Snippet comments on license field ... 75
9.7.1 Description ... 75
9.7.2 Intent ... 75
9.7.3 Examples ... 75
9.8 Snippet copyright text field ... 76
9.8.1 Description ... 76
9.8.2 Intent ... 76
9.8.3 Examples ... 76
9.9 Snippet comment field ... 77
9.9.1 Description ... 77
9.9.2 Intent ... 77
9.9.3 Examples ... 77

AVA Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: ISO_IEC 5962_2021

9.10 Snippet name field 78
9.10.1 Description 78
9.10.2 Intent 78
9.10.3 Examples 78
9.11 Snippet attribution text field 78
9.11.1 Description 78
9.11.2 Intent 79
9.11.3 Examples 79

10 Other licensing information detected section 79
10.1 License identifier field 79
10.1.1 Description 79
10.1.2 Intent 80
10.1.3 Examples 80
10.2 Extracted text field 80
10.2.1 Description 80
10.2.2 Intent 81
10.2.3 Examples 81
10.3 License name field 82
10.3.1 Description 82
10.3.2 Intent 82
10.3.3 Examples 82
10.4 License cross reference field 82
10.4.1 Description 82
10.4.2 Intent 83
10.4.3 Examples 83
10.5 License comment field 83
10.5.1 Description 83
10.5.2 Intent 83
10.5.3 Examples 83

11 Relationships between SPDX elements information section 84
11.1 Relationship field 84
11.1.1 Description 84
11.1.2 Intent 89
11.1.3 Examples 89
11.2 Relationship comment field 90
11.2.1 Description 90
11.2.2 Intent 90
11.2.3 Examples 90

12 Annotations information section 91
12.1 Annotator field 91
12.1.1 Description 91
12.1.2 Intent 91
12.1.3 Examples 91
12.2 Annotation date field 92
12.2.1 Description 92
12.2.2 Intent 92
12.2.3 Examples 92
12.3 Annotation type field 93
12.3.1 Description 93
12.3.2 Intent 93
12.3.3 Examples 93
12.4 SPDX identifier reference field 93
12.4.1 Description 93

AVA Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: ISO_IEC 5962_2021

12.4.2 Intent ... 94
12.4.3 Examples ... 94
12.5 Annotation comment field ... 94
12.5.1 Description ... 94
12.5.2 Intent ... 95
12.5.3 Examples ... 95

13 Review information section (deprecated) ... 95
13.1 Reviewer field (deprecated) ... 95
13.1.1 Description ... 95
13.1.2 Intent ... 96
13.1.3 Examples ... 96
13.2 Review date field (deprecated) ... 96
13.2.1 Description ... 96
13.2.2 Intent ... 97
13.2.3 Examples ... 97
13.3 Review comment field (deprecated) ... 97
13.3.1 Description ... 97
13.3.2 Intent ... 98
13.3.3 Examples ... 98

Annex A (Informative) SPDX license list ... 99

A.1 Licenses with short identifiers ... 99

A.2 Exceptions list ... 114

A.3 Deprecated licenses ... 116

Annex B (Informative) License matching guidelines and templates ... 118

B.1 SPDX license list matching guidelines ... 118

B.2 How these guidelines are applied ... 118

B.2.1 Purpose ... 118

B.2.2 Guideline: official license headers ... 118

B.3 Substantive text ... 118

B.3.1 Purpose ... 118

B.3.2 Guideline: verbatim text ... 118

B.3.3 Guideline: no additional text ... 119

B.3.4 Guideline: replaceable text ... 119

B.3.5 Guideline: omittable text ... 119

B.4 Whitespace ... 119

B.4.1 Purpose ... 119

B.4.2 Guideline ... 119

B.5 Capitalization ... 119

B.5.1 Purpose ... 119

B.5.2 Guideline ... 120

B.6 Punctuation ... 120

B.6.1 Purpose ... 120

Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: ISO_IEC 5962_2021

B.6.2 Guideline: punctuation ... 120
B.6.3 Guideline: hyphens, dashes ... 120
B.6.4 Guideline: quotes ... 120
B.7 Code comment indicators ... 120
B.7.1 Purpose ... 120
B.7.2 Guideline ... 120
B.8 Bullets and numbering ... 120
B.8.1 Purpose ... 120
B.8.2 Guideline ... 121
B.9 Varietal word spelling ... 121
B.9.1 Purpose ... 121
B.9.2 Guideline ... 121
B.10 Copyright symbol ... 121
B.10.1 Purpose ... 121
B.10.2 Guideline ... 121
B.11 Copyright notice ... 121
B.11.1 Purpose ... 121
B.11.2 Guideline ... 122
B.12 License name or title ... 122
B.12.1 Purpose ... 122
B.12.2 Guideline ... 122
B.13 Extraneous text at the end of a license ... 122
B.13.1 Purpose ... 122
B.13.2 Guideline ... 122
B.14 HTTP protocol ... 122
B.14.1 Purpose ... 122
B.14.2 Guideline ... 122
B.15 SPDX license list ... 123
B.15.1 Template access ... 123
B.15.2 Template format ... 123
Annex C (Normative) RDF object model and identifier syntax ... 124
C.1 Introduction ... 124
C.2 Agent and tool identifiers ... 125
Annex D (Normative) SPDX license expressions ... 126
D.1 Overview ... 126
D.2 Case sensitivity ... 127
D.3 Simple license expressions ... 127

Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: ISO_IEC 5962_2021

D.4 Composite license expressions ... 127
D.4.1 Introduction ... 127
D.4.2 Disjunctive "OR" Operator ... 128
D.4.3 Conjunctive "AND" Operator ... 128
D.4.4 Exception "WITH" Operator ... 128
D.4.5 Order of precedence and parentheses ... 129
D.4.6 License expressions in RDF ... 129
Annex E (Informative) Using SPDX license list short identifiers in source files ... 131
E.1 Introduction ... 131
E.2 Format for SPDX-License-Identifier ... 131
E.3 Representing single license ... 132
E.4 Representing multiple licenses ... 132
Annex F (Normative) External repository identifiers ... 134
F.1 Introduction ... 134
F.2 Security ... 134
F.2.1 cpe22Type ... 134
F.2.2 cpe23Type ... 134
F.3 Package-Manager ... 135
F.3.1 maven-central ... 135
F.3.2 npm ... 135
F.3.3 nuget ... 135
F.3.4 bower ... 136
F.3.5 purl ... 136
F.4 Persistent-Id ... 136
F.4.1 swh ... 136
F.5 Other ... 137
F.5.1 [idstring] ... 137
Annex G (Normative) SPDX Lite ... 138
G.1 Explanation of SPDX Lite ... 138
G.2 Format of SPDX Lite ... 138
G.3 Table of SPDX Lite fields ... 138
Annex H (Informative) SPDX file tags ... 140
H.1 Rationale ... 140
H.2 Format ... 140
H.3 Caveats ... 141
Annex I (Informative) Differences from previous editions ... 142
I.1 Differences between V2.2.1 and V2.2 ... 142

Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: ISO_IEC 5962_2021

I.2 Differences from V2.2 and V2.1 ..... **143**
I.3 Differences between V2.1 and V2.0 ..... **143**
I.4 Differences between V2.0 and V1.2 ..... **144**
Bibliography **145**

Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: ISO_IEC 5962_2021

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by the Joint Development Foundation (JDF) (as SPDX® Specification V2.2.1) and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

Introduction

Companies and organizations (collectively "Organizations") are widely using and reusing open source and other software packages. Accurate identification of software is key for many supply chain processes. Vulnerability remediation starts with knowing the details of which version of software is in use on a system. Compliance with the associated licenses requires a set of analysis activities and due diligence that each Organization performs independently, which may include 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. With this document, the SPDX workgroup has created 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.

© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

Information technology — SPDX® Specification V2.2.1

1 Scope

This Software Package Data Exchange® (SPDX®) specification defines a standard data format for communicating the component and metadata information associated with software packages. An SPDX document can be associated with a set of software packages, files or snippets and contains information about the software in the SPDX format described in this specification.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Apache Maven, Apache Software Foundation, https://maven.apache.org/

Bower API, https://bower.io/docs/api/#install

Common Platform Enumeration (CPE) – Specification, The MITRE Corporation, https://cpe.mitre.org/files/cpe-specification_2.2.pdf

NISTIR 7695, *Common Platform Enumeration: Naming Specification Version 2.3*, NIST, https://csrc.nist.gov/publications/detail/nistir/7695/final

npm-package.json, npm Inc., https://docs.npmjs.com/files/package.json

NuGet documentation, Microsoft, https://docs.microsoft.com/en-us/nuget/

POSIX.1-2017 *The Open Group Base Specifications Issue 7*, 2018 edition, IEEE/Open Group, https://pubs.opengroup.org/onlinepubs/9699919799/

purl (package URL), https://github.com/package-url/purl-spec

Resource Description Framework (RDF), 2014-02-25, W3C, http://www.w3.org/standards/techs/rdf

RFC-1321, *The MD5 Message-Digest Algorithm*, The Internet Society Network Working Group, https://tools.ietf.org/html/rfc1321

RFC-3174, *US Secure Hash Algorithm 1 (SHA1)*, The Internet Society Network Working Group, https://tools.ietf.org/html/rfc3174

RFC-3986, *Uniform Resource Identifier (URI): Generic Syntax*, The Internet Society Network Working Group, https://tools.ietf.org/html/rfc3986

RFC-5234, *Augmented BNF for Syntax Specifications: ABNF*, The Internet Society Network Working Group, https://tools.ietf.org/html/rfc5234

RFC-6234, *US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)*, The Internet Society Network Working Group, https://tools.ietf.org/html/rfc6234

SoftWare Heritage persistent IDentifiers (SWHIDs), https://docs.softwareheritage.org/devel/swh-model/persistent-identifiers.html

SPDX and RDF Ontology, http://spdx.org/rdf/ontology/spdx-2-2

SPDX License list, Linux Foundation, https://spdx.org/licenses/

SPDX License Exceptions list, Linux Foundation, https://spdx.org/licenses/exceptions-index.html

AVA Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: ISO_IEC 5962_2021

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1

annotations information section

section (3.9) type, an instance of which contains comments about an SPDX document, SPDX file, SPDX package, or SPDX snippet

3.2

field

a piece of information contained in a *section* (3.9)

3.3

file information section

section (3.9) type, an instance of which contains facts specific to files

3.4

other licensing information detected section

section (3.9) type, an instance of which contains a way to capture information about and refer to licenses that are not on the SPDX license List

3.5

package

any unit of content that can be associated with a distribution of software

3.6

package information section

section (3.9) type, an instance of which contains facts that are common properties of a *package*

3.7

relationships between SPDX elements information section

section (3.9) type, an instance of which contains information on how documents, *packages* (3.5), files and snippets relate to each other

3.8

review information section

section (3.9) type, an instance of which contains information about persons, organizations or tools that have reviewed a document

3.9

section

a part of this SPDX specification

© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

3.10

snippet information section

section (3.9) type, an instance of which contains facts that are specific to a part of a file

3.11

SPDX document

collection of *section* (3.9) instances each of which contains information about software organized using the *SPDX format* (3.11)

3.12

SPDX document creation information section

section (3.9) type, an instance of which contains metadata that associates analysis results with a specific version of an *SPDX document* (3.11) and license for use, and provides information on how, when, and by whom the SPDX document was created

3.13

SPDX format

the data format defined by this document

3.14

sub-package

a package which is embedded in a larger package

4 Conformance

4.1 SPDX Current and Previous Versions

This edition has the version number 2.2.1 as part of its title. Although this is the first ISO edition of the SPDX Specification, earlier editions were published by the SPDX workgroup via the Linux Foundation. The SPDX Specification 2.2.1 was subsequently transposed into the Joint Development Foundation. [Those earlier editions are: 1.0 (August 2011), 1.1 (August 2012), 1.2 (October 2013), 2.0 (May 2015), 2.1 (November 2016), and 2.2 (May 2020).] Differences between this edition and earlier ones are reported in Annex I; see also [1].

4.2 Obsolete features

Over the life of a standard, some older approaches can become obsolete and are dropped from subsequent editions, possibly with a replacement approach being provided. Such action involves *deprecating* those outdated features. This edition identifies all currently deprecated features.

4.3 Alternate notation for some conformance requirements

This standard contains more than a few *cardinality assertions*, each of which indicates absolute, optional, or conditional requirements. Here are some examples:

— Cardinality: Mandatory, one.

— Cardinality: Optional, one or many.

Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: ISO_IEC 5962_2021

— Cardinality: Mandatory, one if {condition} is true or {feature} omitted, zero (shall be omitted) if {condition} is false.

— Cardinality: 0..1

— Cardinality: 0..*

— Cardinality: 1..1

— Cardinality: 1..*

Each of these assertions can easily be understood as to whether a feature is required, and if so, how many occurrences are required; also, whether a feature is permitted, and if so, in what number. As this is the format long familiar to the SPDX community, it has been preserved in this document.

4.4 Standard data format requirements

The data format specification and recommendations are subject to the following constraints:

— Shall be in a human readable form.

— Shall be in a syntax that a software tool can read and write.

— Shall be suitable to be checked for syntactic correctness automatically, independent of how it was generated (human or tool).

— The SPDX document character set shall support UTF-8 encoding.

— Multiple serialization formats may be used to represent the information being exchanged. Current supported formats include:

  — **YAML 1.2** see: https://yaml.org/spec/1.2/spec.html

  — **JavaScript Object Notation** (JSON) see: ECMA-404

    — The JSON Schema for SPDX can be found in the SPDX Spec Git Repository Schema directory

  — **Resource Description Framework** (RDF also referred to as RDF/XML) see: https://www.w3.org/TR/rdf-syntax-grammar/

  — **tag:value** flat text file as described in this specification

  — **.xls** spreadsheets

— In addition to the supported formats, the following format is in development with a plan to complete the specification in the next release:

  — **Extensible Markup Language** (XML) see: https://www.w3.org/TR/2008/REC-xml-20081126/

— Interoperability between all the supported file formats shall be preserved. SPDX defines how to validate a document in each supported format, and how to translate a valid document without loss to each other supported format.

© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

— Tags and format properties are case sensitive.

— Should be easy to recognize in a file system without opening the file. A suggested naming convention is:

Table 1 — Suggested naming convention

Format	Extension
tag:value	*.spdx
RDF	*.spdx.rdf
JSON	*.spdx.json
XML	*.spdx.xml
YAML	*.spdx.yaml or *.spdx.yml

— The convention in this specification is for the RDF examples to use `rdf:about="..."` to represent that a proper Universal Resource Indicator (URI) should be present.

4.5 Trademark Compliance

To be designated an SPDX document, a file shall comply with the requirements of the SPDX Trademark License (See the SPDX Trademark Page).

The official copyright notice that shall be used with any verbatim reproduction and/or distribution of this SPDX Specification 2.2.1 is:

"Official SPDX® Specification 2.2.1 Copyright © 2010-2020 Linux Foundation and its Contributors. Licensed under the Creative Commons Attribution License 3.0 Unported. All other rights are expressly reserved."

The official copyright notice that shall be used with any non-verbatim reproduction and/or distribution of this SPDX Specification 2.2.1, 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 2.2.1 found at spdx.dev. These portions are Copyright © 2010-2020 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."

4.6 The SPDX Lite profile

Rather than conforming to this whole specification, an implementation may conform with SPDX Lite only, a profile that defines a subset of the SPDX specification. SPDX Lite aims at the balance between the SPDX standard and actual workflows in some industries. See Annex G for more information.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

5 Composition of an SPDX document

5.1 What this specification covers

This document contains the specification for an SPDX document, which is made up of a set of one or more sections, instances of which contain information in the form of *fields*. The following subclauses introduce the different kinds of sections allowed. The fields for each kind of section are defined in the clause corresponding to that section. Within an SPDX document, sections may be organized, as follows:

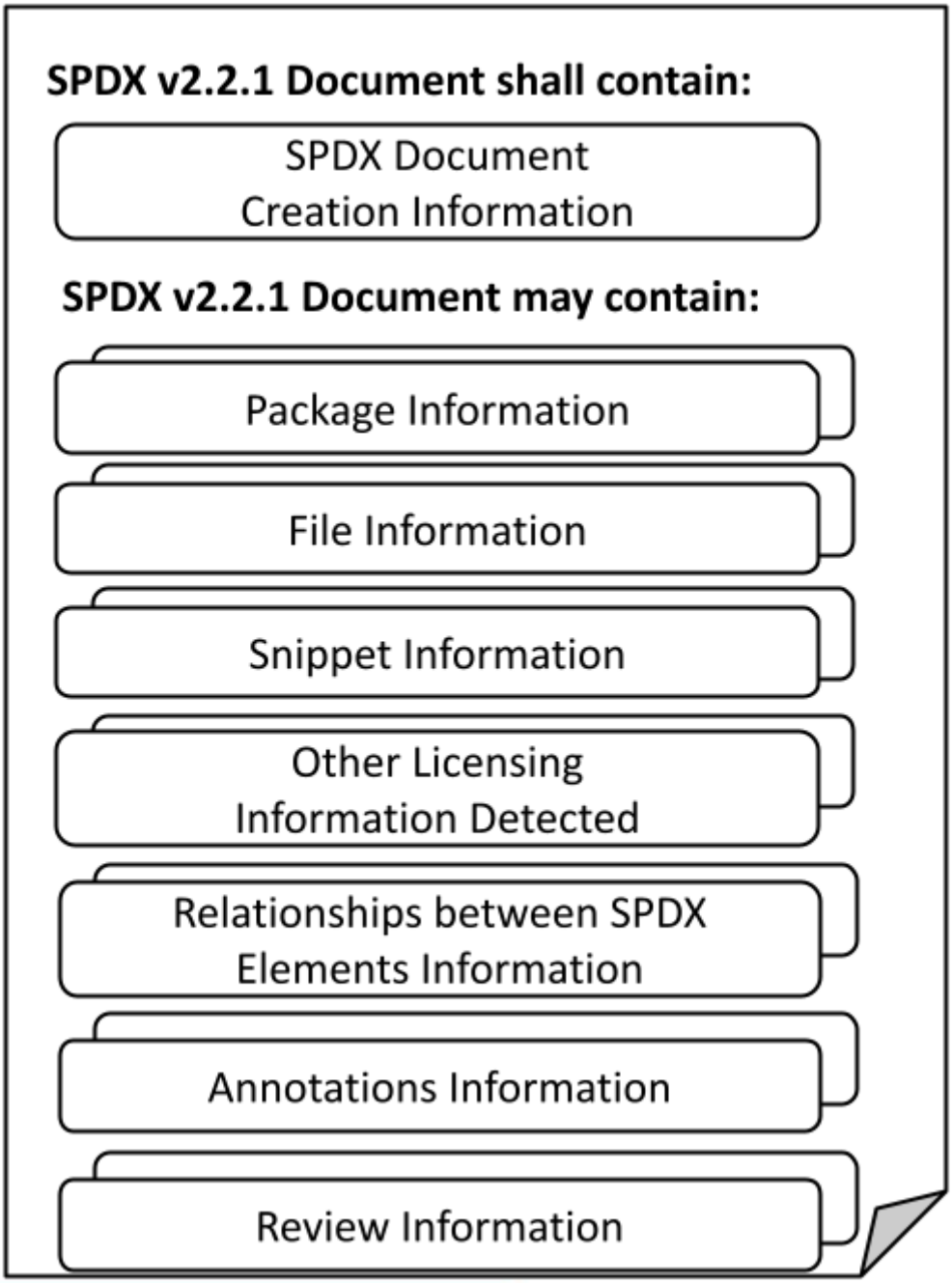

Figure 1 — SPDX document sections

The object model is illustrated by Annex C.

© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

5.2 Sections

5.2.1 SPDX document creation information section

An instance of this section provides the necessary information for forward and backward compatibility for processing tools.

One instance shall be present for each SPDX document produced.

Cardinality: Mandatory, one.

See Clause 6 for details of the fields in this kind of section.

5.2.2 Package information section

If SPDX information is being used to describe packages, then one instance of the Package Information per package being described shall exist. It provides important meta information about the package as a whole. Packages are an abstract concept that can be used to refer to any distribution of software, typically consisting of one or more files and capable of containing sub-packages. Starting with SPDX 2.0, it is not necessary to have a package wrapping a set of files.

A Package refers to any unit of content that can be associated with a distribution of software. Typically, a Package is composed of one or more files. An SPDX document may, but is not required to, provide details about the individual files comprising a Package (see Clause 8).

Any of the following non-limiting examples may be (but are not required to be) represented in SPDX as a Package:

— a tarball, zip file or other archive

— a directory or sub-directory

— a separately distributed piece of software which another Package or File uses or depends upon (e.g., a Python package, a Go module, ...)

— a container image, and/or each image layer within a container image

— a collection of one or more sub-packages

— a Git repository snapshot from a particular point in time

Note that some of these could be represented in SPDX as a File as well.

In an SPDX document, Relationship elements can be used to indicate relationships between Packages, such as dependency relationships.

Cardinality: Optional, one or many.

See Clause 7 for details of the fields in this kind of section.

In `tag:value` format, the order in which package and files occur is syntactically significant.

— A new Package Information section is denoted by the Package Name (7.1) field.

— All Package Information fields shall be grouped together before the start of a Files section (Clause 8), if file(s) are present.

— All files contained in a package shall immediately follow the applicable Package Information.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

— A new Package Information section (via Package Name) denotes the start of another package.

— Sub-packages shall not be nested inside a Package Information section, but shall be separate and shall use a Relationship to clarify.

— Annotations and Relationships for the package may appear after the Package Information before any file information.

5.2.3 File information section

One instance of the File Information shall exist for each file in the software package. It provides important meta information about a given file including licenses and copyright. Starting with SPDX 2.0, it is not necessary to have a package wrapping a set of files.

Cardinality: Optional, one or many.

See Clause 8 for details of the fields in this kind of section.

When implementing `tag:value` format, the positioning of File elements is syntactically significant:

— Files are assumed to be associated with the Package Information that immediately precedes it, if a package exists.

— Presence of a new Package Information signals the end of the set of files associated with the preceding package, unless an explicit Relationship is used.

— If a package contains files, the File Information sections shall follow its Package Information section.

— If a File is not part of any package, it shall precede any Package Information section reference in the SPDX document.

— The first field to start off the description of a File shall be the File Name in `tag:value` format.

— File information is associated with the File Name that precedes it.

— Annotations on the file and Relationships from the file may appear after the file information, before the next file or Package Information section.

When implementing file information in RDF, the `spdx:hasFile` property is used to associate the package with the file.

5.2.4 Snippet information section

Snippets can optionally be used when a file is known to have some content that has been included from another original source. They are useful for denoting when part of a file may have been originally created under another license.

Each instance of Snippet Information shall be associated with a specific file in an SPDX document.

Cardinality: Optional, one or many.

See Clause 9 for details of the fields in this kind of section.

When implementing `tag:value` format, the positioning of Snippet elements is syntactically significant:

— If a File contains Snippets, the Snippet Information section shall follow a related File Information section (if it exists in the document).

Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: ISO_IEC 5962_2021

— Presence of a new file or package section signals the end of the set of snippets associated with the original file, unless an explicit Relationship is used.

— The first field to start off the description of a Snippet shall be the Snippet Identifier in `tag:value` format.

— Annotations on the Snippet and Relationships from the Snippet may appear after the Snippet Information, before the next file or Package section.

5.2.5 Other licensing information detected section

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 https://spdx.org/licenses/. The SPDX License List can also be found in Annex A.

One instance shall be created for every unique license or licensing information being referenced that does not match one of the licenses on the SPDX License List.

Cardinality: Optional, one or many.

See Clause 10 for details of the fields in this kind of section.

5.2.6 Relationships between SPDX elements information section

Packages, files, and snippets are all considered to be SPDX Elements, and relationships can be made explicit between these SPDX elements by using the fields in this section.

Cardinality: Optional, one or many.

See Clause 11 for details of the fields in this kind of section.

5.2.7 Annotations information section

Annotations permit the addition of information to validate and clarify ambiguous SPDX Elements (Packages, Files or Snippets).

Cardinality: Optional, one or many.

See Clause 12 for details of the fields in this kind of section.

This section is now the preferred home for review information.

5.2.8 Review information section

The review information section is included for compatibility with SPDX 1.2, and is deprecated since SPDX 2.0. Any review information shall use an Annotation (as described in Clause 12) with an annotation type of `REVIEW`.

Review information may be added after the initial SPDX document has been created. The set of fields are optional and multiple instances may be added. Once a Reviewer entry is added, the Review Date associated with the review is mandatory. The Created date shall not be modified as a result of the addition of information regarding the conduct of a review. A Review Comments is optional.

See Clause 13 for details of the fields in this kind of section.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

5.3 What this specification does not cover

This document does not address the following:

— Information that cannot be derived from an inspection (whether manual or using automated tools) of the package to be analyzed.

— How the data stored in an SPDX document is used by the recipient.

— Any identification of any patent(s) which may or may not relate to the package.

— Legal interpretation of the licenses or any compliance actions that have been or may need to be taken.

6 SPDX document creation information section

6.1 SPDX version field

6.1.1 Description

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 shall be incremented when incompatible changes between versions are made (one or more sections are created, modified or deleted). The minor field shall be incremented when backwards compatible changes are made. The metadata for the SPDX version field is shown in Table 2.

Table 2 — Metadata for the SPDX version field

Attribute	Value
Required	Yes
Cardinality	1..1
Format	`SPDX-M.N` where: • `M` is major version number • `N` is minor version number.

6.1.2 Intent

Here, parties exchanging information in accordance with the SPDX specification need to provide 100% transparency as to which SPDX specification version such information is conforming to.

6.1.3 Examples

EXAMPLE 1 Tag: `SPDXVersion:`

```
SPDXVersion: SPDX-2.2
```


© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

EXAMPLE 2 RDF: Property `spdx:specVersion` in class `spdx:SpdxDocument`

```
<SpdxDocument rdf:about="...">
   <specVersion>SPDX-2.2</specVersion>
</SpdxDocument>
```

This specification uses the prefix `rdf:` to refer to the RDF/XML namespace:

`http://www.w3.org/1999/02/22-rdf-syntax-ns#`

6.2 Data license field

6.2.1 Description

Compliance with this document includes populating the SPDX fields therein with data related to such fields ("SPDX-Metadata"). This document contains numerous fields where an SPDX document creator may provide relevant explanatory text in SPDX-Metadata. Without opining on the lawfulness of "database rights" (in jurisdictions where applicable), such explanatory text is copyrightable subject matter in most Berne Convention countries. The metadata for the data license field is shown in Table 3.

Table 3 — Metadata for the data license field

Attribute	Value
Required	Yes
Cardinality	1..1
Format	`CC0-1.0`

6.2.2 Intent

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

6.2.3 Examples

EXAMPLE 1 Tag: `DataLicense:`

```
DataLicense: CC0-1.0
```

EXAMPLE 2 RDF: Property `spdx:dataLicense` in class `spdx:SpdxDocument`

```
<SpdxDocument rdf:about="...">
  <dataLicense rdf:resource="http://spdx.org/licenses/CC0-1.0" />
</SpdxDocument>
```

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

6.3 SPDX identifier field

6.3.1 Description

Identify the current SPDX document which may be referenced in relationships by other files, packages internally and documents externally. To reference another SPDX document in total, this identifier should be used with the external document identifier preceding it. See Clause 11 for examples. The metadata for the SPDX identifier field is shown in Table 4.

Table 4 — Metadata for SPDX identifier field

Attribute	Value
Required	Yes
Cardinality	1..1
Format	`SPDXRef-DOCUMENT`

6.3.2 Intent

Provide a way for the document to refer to itself in relationship to other elements.

6.3.3 Examples

EXAMPLE 1 Tag: `SPDXID:`

```
SPDXID: SPDXRef-DOCUMENT
```

EXAMPLE 2 RDF:

The URI for the document is the document namespace appended by

```
#SPDXRef-DOCUMENT
```

```
<spdx:SpdxDocument
  rdf:about="http://spdx.org/spdxdocs/spdx-example-444504E0-4F89-41D3-9A0
C-0305E82C33123#SPDXRef-DOCUMENT">
  ...
</spdx:SpdxDocument>
```

6.4 Document name field

6.4.1 Description

Identify name of this document as designated by creator. The metadata for the document name field is shown in Table 5.

© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

Table 5 — Metadata for the document name field

Attribute	Value
Required	Yes
Cardinality	1..1
Format	Single line of text.

6.4.2 Intent

Here, the name of each document is an important convention and easier to refer to than the URI.

6.4.3 Examples

EXAMPLE 1 Tag: `DocumentName:`

```
DocumentName: glibc-v2.3

DocumentName: ubuntu-14.04
```

EXAMPLE 2 RDF: Property `spdx:name` in class `spdx:SpdxDocument`

```
<SpdxDocument rdf:about="...">
  <name>glibc-v2.3</name>
</SpdxDocument>

<SpdxDocument rdf:about="...">
  <name>ubuntu-14.04</name>
</SpdxDocument>
```

6.5 SPDX document namespace field

6.5.1 Description

Provide an SPDX document-specific namespace as a unique absolute Uniform Resource Identifier (URI) as specified in RFC-3986, with the exception of the '#' delimiter. The SPDX document URI shall not contain a URI "part" (e.g. the "#" character), since the '#' is used in SPDX element URIs (packages, files, snippets, etc) to separate the document namespace from the element's SPDX identifier. Additionally, a scheme (e.g. "https:") is required.

The URI shall be unique for the SPDX document including the specific version of the SPDX document. If the SPDX document is updated, thereby creating a new version, a new URI for the updated document shall be used. There may only be one URI for an SPDX document and only one SPDX document for a given URI. The metadata for the SPDX document namespace field is shown in Table 6.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

Table 6 — Metadata for the SPDX document namespace field

Attribute	Value
Required	Yes
Cardinality	1..1
Format	Unique absolute Uniform Resource Identifier (URI) as specified in RFC-3986, with the following exceptions: The SPDX document URI cannot contain a URI "part" (e.g. the # delimiter), since the # is used to uniquely identify SPDX element identifiers. The URI shall contain a scheme (e.g., `https:`). The URI shall be unique for the SPDX document including the specific version of the SPDX document. If the SPDX document is updated, thereby creating a new version, a new URI for the updated document shall be used. There can only be one URI for an SPDX document and only one SPDX document for a given URI.

6.5.2 Intent

The URI provides an unambiguous mechanism for other SPDX documents to reference SPDX elements within this SPDX document. See 6.6 for a description on how external documents are referenced. Although it is not required, the URI can be constructed in a way which provides information on how the SPDX document can be found. For example, the URI can be a URL referencing the SPDX document itself, if it is available on the internet. A best practice for creating the URI for SPDX documents available on the public internet is `http://[CreatorWebsite]/[pathToSpdx]/[DocumentName]-[UUID]` where:

— `CreatorWebsite` is a website hosted by the creator of the document. (e.g. an SPDX document provided by SPDX would be spdx.org)

— `PathToSpdx` is a path to where SPDX documents are stored on the website (e.g. /spdx/spdxdocs)

— `DocumentName` is a name given to the SPDX document itself, typically the (set of) package name(s) followed by the version. (See 6.4.)

— `UUID` is a universally unique identifier. The UUID could be a version 4 random UUID which can be generated from the Online UUID Generator or a version 5 UUID generated from a sha1 checksum known to be unique for this specific SPDX document version.

— If the creator does not own their own website, a default SPDX CreatorWebsite and PathToSpdx can be used `spdx.org/spdxdocs`. Note that the SPDX documents are not currently stored or accessible on this website. The URI is only used to create a unique ID following the above conventions.

NOTE The URI does not have to be accessible. It is only intended to provide a unique ID. In many cases, the URI will point to a web accessible document, but this should not be assumed to be the case.

© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

6.5.3 Examples

EXAMPLE 1 Tag: `DocumentNamespace:`

```
DocumentNamespace: http://spdx.org/spdxdocs/spdx-tools-v1.2-3F2504E0-4F89
-41D3-9A0C-0305E82...
```

EXAMPLE 2 RDF: The unique ID is the URI for the SPDX document

```
<SpdxDocument rdf:about="http://spdx.org/spdxdocs/spdx-tools-v1.2-3F2504E
0-4F89-41D3-9A0C-0305E82...">
    <rdfs:comment>This document was created using SPDX 2.0 using
    licenses from the web site.</rdfs:comment>
</SpdxDocument>
```

This specification uses the prefix `rdfs:` to refer to the RDF Schema namespace:

`http://www.w3.org/2000/01/rdf-schema#`

6.6 External document references field

6.6.1 Description

Identify any external SPDX documents referenced within this SPDX document. The metadata for the external document references field is shown in Table 7.

Table 7 — Metadata for the external document references field

Attribute	Value
Required	No
Cardinality	1..*
Format	DocumentRef-`[idstring] [SPDX document URI] [Checksum]` where `[idstring]` is a unique string containing letters, numbers, `.`, – and/or +. `[SPDX document URI]` is the unique ID for the external document as defined in 6.5 of that referenced document, `[Checksum]` is a checksum of the external document following the checksum format defined in 8.4.

6.6.2 Intent

SPDX elements within this document may be related to other SPDX elements referenced from external SPDX documents. An SPDX element could be a snippet, file, package, license reference or SPDX document.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

6.6.3 Examples

EXAMPLE 1 Tag: `ExternalDocumentRef:`

```
ExternalDocumentRef:DocumentRef-spdx-tool-1.2 http://spdx.org/spdxdocs/sp
dx-tools-v1.2-3F2504E0-4F89-41D3-9A0C-0305E82C3301 SHA1: d6a770ba38583ed4
bb4525bd96e50461655d2759
```

EXAMPLE 2 RDF: Property `spdx:externalDocumentRef` in class `spdx:SpdxDocument range ExternalDocumentRef`.

The ExternalDocumentRef contains two properties:

— spdxDocument - the SpdxDocument being referenced

— checksum - the checksum of the referenced SPDX document

```
<SpdxDocument rdf:about="...">
  <externalDocumentRef rdf:ID="DocumentRef-spdx-tool-1.2">
    <ExternalDocumentRef>
        <spdxDocument rdf:about="http://spdx.org/spdxdocs/spdx-tools-v1.2
-3F2504E0-4F89-41D3-9A0C-0305E82..." />
        <checksum>
            <Checksum>
                <algorithm rdf:resource="checksumAlgorithm_sha1"/>
                <checksumValue>d6a770ba38583ed4bb4525bd96e50461655d2758
                </checksumValue>
            </Checksum>
        </checksum>
    </ExternalDocumentRef>
  </externalDocumentRef>
</SpdxDocument>
```

NOTE In RDF, a namespace can be created for the external document reference if a short form name for the external reference is desired.

6.7 License list version field

6.7.1 Description

An optional field for creators of the SPDX document to provide the version of the SPDX License List used when the SPDX document was created. The metadata for the license list version field is shown in Table 8.

© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

Table 8 — Metadata for the license list version field

Attribute	Value
Required	No
Cardinality	1..1
Format	`M.N` where: `M` is major version number `N` is minor version number.

6.7.2 Intent

Recognizing that licenses are added to the SPDX License List with each subsequent version, the intent is to provide recipients of the SPDX document with the version of the SPDX License List used. This anticipates that in the future, an SPDX document might have used a version of the SPDX License List that is older than the then current one.

6.7.3 Examples

EXAMPLE 1 Tag: `LicenseListVersion:`

```
LicenseListVersion: 3.8
```

EXAMPLE 2 RDF: Property `licenseListVersion` in class `spdx:CreationInfo`

```
<CreationInfo>
    <licenseListVersion>3.8</licenseListVersion>
</CreationInfo>
```

6.8 Creator field

6.8.1 Description

Identify who (or what, in the case of a tool) created the SPDX document. If the SPDX document was created by an individual, indicate the person's name. If the SPDX document was created on behalf of a company or organization, indicate the entity name. If the SPDX document was created using a software tool, indicate the name and version for that tool. If multiple participants or tools were involved, use multiple instances of this field. Person name or organization name may be designated as “anonymous” if appropriate. The metadata for the creator field is shown in Table 9.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

Table 9 — Metadata for the creator field

Attribute	Value
Required	Yes
Cardinality	1..*

Format	Single line of text with the following keywords:
	`"Person: person name" and optional "(email)"`
	`"Organization: organization" and optional "(email)"`
	`"Tool: toolidentifier-version"`

6.8.2 Intent

Here, the generation method will assist the recipient of the SPDX document in assessing the general reliability/accuracy of the analysis information.

6.8.3 Examples

EXAMPLE 1 Tag: `Creator:`

```
Creator: Person: Jane Doe ()
Creator: Organization: ExampleCodeInspect ()
Creator: Tool: LicenseFind-1.0
```

EXAMPLE 2 RDF: Property `spdx:creator` in class `spdx:CreationInfo`

```
<CreationInfo>
    <creator> Person: Jane Doe () </creator>
    <creator> Organization: ExampleCodeInspect () </creator>
    <creator> Tool: LicenseFind-1.0 </creator>
</CreationInfo>
```

6.9 Created field

6.9.1 Description

Identify when the SPDX document was originally created. The date is to be specified according to combined date and time in UTC format as specified in ISO 8601 standard. This field is distinct from the fields in Clause 12, which involves the addition of information during a subsequent review. The metadata for the created field is shown in Table 10.

© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

Table 10 — Metadata for the created field

Attribute	Value
Required	Yes
Cardinality	1..1
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 • `Z` is universal time indicator

6.9.2 Intent

Here, the time stamp can serve as an indication as to whether the analysis needs to be updated.

6.9.3 Examples

EXAMPLE 1 Tag: `Created:`

```
Created: 2010-01-29T18:30:22Z
```

EXAMPLE 2 RDF: Property `spdx:created` in class `spdx:CreationInfo`

```
<CreationInfo>
    <created> 2010-01-29T18:30:22Z </created>
</CreationInfo>
```

6.10 Creator comment field

6.10.1 Description

An optional field for creators of the SPDX document to provide general comments about the creation of the SPDX document or any other relevant comment not included in the other fields. The metadata for the Creator comment field is shown in Table 11.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

Table 11 — Metadata for the Creator comment field

Attribute	Value
Required	No
Cardinality	1..1
Format	Free form text that can span multiple lines. In `tag:value` format this is delimited by `<text> .. </text>`, in RDF, it is delimited by `<rdfs:comment>`.

6.10.2 Intent

Here, the intent is to provide recipients of the SPDX document with comments by the creator of the SPDX document.

6.10.3 Examples

EXAMPLE 1 Tag: `CreatorComment:`

```
CreatorComment: <text>This SPDX document was created by a combination of
using a free tool, as indicated above, and manual analysis by several aut
hors of the code.</text>
```

EXAMPLE 2 RDF: Property `rdfs:comment` in class `spdx:CreationInfo`

```
<CreationInfo>
    <rdfs:comment>This SPDX document was created by a combination of
    using a free tool, as indicated above, and manual analysis
    by several authors of the code.</rdfs:comment>
</CreationInfo>
```

6.11 Document comment field

6.11.1 Description

An optional field for creators of the SPDX document content to provide comments to the consumers of the SPDX document. The metadata for the document comment field is shown in Table 12.

Table 12 — Metadata for the document comment field

Attribute	Value
Required	No
Cardinality	1..1
Format	Free form text that can span multiple lines. In `tag:value` format this is delimited by `<text> .. </text>`, in RDF, it is delimited by `<rdfs:comment>`.

© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

6.11.2 Intent

Here, the intent is to provide readers/reviewers with comments by the creator of the SPDX document about the SPDX document.

6.11.3 Examples

EXAMPLE 1 Tag: `DocumentComment:`

```
DocumentComment: <text>This document was created using SPDX 2.0, version
2.3 of the SPDX License List and refering to licenses in file MyCompany.A
pproved.Licenses.spdx.</text>
```

EXAMPLE 2 RDF: Property `rdfs:comment` in class `SpdxDocument`

```
<SpdxDocument rdf:about="...">
    <rdfs:comment>
      This document was created using SPDX 2.0, version 2.3 of the SPDX
      License List and refering to licenses in file
      MyCompany.Approved.Licenses.spdx.
    </rdfs:comment>
</SpdxDocument>
```

7 Package information section

7.1 Package name field

7.1.1 Description

Identify the full name of the package as given by the Package Originator (7.6). The metadata for the SPDX version field is shown in Table 13.

Table 13 — Metadata for the package name field

Attribute	Value
Required	Yes
Cardinality	1..1
Format	Single line of text.

7.1.2 Intent

The name of each package is an important conventional technical identifier to be maintained for each package.

7.1.3 Examples

EXAMPLE 1 Tag: `PackageName:`

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

```
PackageName: glibc
```

EXAMPLE 2 RDF: Property `spdx:name` in class `spdx:Package`

```
<Package rdf:about="...">
    <name>glibc</name>
</Package>
```

7.2 Package SPDX identifier field

7.2.1 Description

Uniquely identify any element in an SPDX document which may be referenced by other elements. These may be referenced internally and externally with the addition of the SPDX document identifier. The metadata for the SPDX identifier field is shown in Table 14.

Table 14 — Metadata for the SPDX identifier field

Attribute	Value
Required	Yes
Cardinality	1..1
Format	"SPDXRef-"`[idstring]` where `[idstring]` is a unique string containing letters, numbers, `.`, and/or –.

7.2.2 Intent

There may be several versions of the same package within an SPDX document. Each element needs to be able to be referred to uniquely so that relationships between elements can be clearly articulated.

7.2.3 Examples

EXAMPLE 1 Tag: `SPDXID:`

```
SPDXID: SPDXRef-1
```

EXAMPLE 2 RDF: The URI for the element will follow the form:

```
[SPDX document namespace]#[SPDX identifier]
```

See 6.5 for the definition of the SPDX document namespace and 6.3 for the definition of the SPDX identifier

Using `xml:base`:

```
<rdf:RDF xml:base="http://acme.com/spdxdocs/acmeproj/v1.2/1BE2A4FF-5F1A-4
8D3-8483-28A9B0349A1B">
    ...
    <Package rdf:about="#SPDXRef-1">
    ...
```


© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

```
    </Package>
</rdf:RDF>
```

Using document URI:

```
<Package rdf:about="http://acme.com/spdxdocs/acmeproj/v1.2/1BE2A4FF-5F1A-
48D3-8483-28A9B0349A1B#SPDXRef-1">
    ...
</Package>
```

7.3 Package version field

7.3.1 Description

Identify the version of the package. The metadata for the package version field is shown in Table 15.

Table 15 — Metadata for the package version field

Attribute	Value
Required	No
Cardinality	1..1
Format	Single line of text.

7.3.2 Intent

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

7.3.3 Examples

EXAMPLE 1 Tag: `PackageVersion:`

```
PackageVersion: 2.11.1
```

EXAMPLE 2 RDF: Property `spdx:versionInfo` in class `spdx:Package`

```
<Package rdf:about="...">
    ...
    <versionInfo>2.11.1</versionInfo>
    ...
</Package>
```

7.4 Package file name field

7.4.1 Description

Provide the actual file name of the package, or path of the directory being treated as a package. This may include the packaging and compression methods used as part of the file name, if appropriate. The metadata for the package file name field is shown in Table 16.

Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: ISO_IEC 5962_2021

Table 16 — Metadata for the package file name field

Attribute	Value
Required	No
Cardinality	1..1
Format	Single line of text.

7.4.2 Intent

The actual file name of the compressed file containing the package may be a significant technical element that needs to be included with each package identification information. If a grouping, like a set of files in a sub-directory, is being treated as a package, the sub-directory name may be appropriate to provide. Sub-directory name is preceded with a `./`. See RFC 3986 for syntax.

7.4.3 Examples

EXAMPLE 1 Tag: `PackageFileName:`

```
PackageFileName: glibc-2.11.1.tar.gz
```

Sub-directory being treated as a package:

```
PackageFileName: ./myrootdir/mysubdir1
```

EXAMPLE 2 RDF: Property `spdx:packageFileName` in class `spdx:Package`

```
<Package rdf:about="...">
    ...
    <packageFileName>glibc 2.11.1.tar.gz</packageFileName>
    ...
</Package>
```

Sub-directory being treated as a package:

```
<Package rdf:about="...">
   ...
   <packageFileName>./myrootdir/mysubdir1</packageFileName>
   ...
</Package>
```

7.5 Package supplier field

7.5.1 Description

Identify the actual distribution source for the package/directory identified in the SPDX document. This might or might not be different from the originating distribution source for the package. The name of the Package Supplier shall be an organization or recognized author and not a web site. For example, SourceForge is a host website, not a supplier, the supplier for https://sourceforge.net/projects/bridge/ is "The Linux Foundation."

© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

Use `NOASSERTION` if:

— the SPDX document creator has attempted to but cannot reach a reasonable objective determination;

— the SPDX document creator has made no attempt to determine this field; or

— the SPDX document creator has intentionally provided no information (no meaning should be implied by doing so).

The metadata for the package supplier field is shown in Table 17.

Table 17 — Metadata for the package supplier field

Attribute	Value
Required	No
Cardinality	1..1
Format	Single line of text with one of the following keywords | `NOASSERTION` • `Person:` person name and optional `(<email>)` • `Organization:` organization name and optional `(<email>)`

7.5.2 Intent

Assist with understanding the point of distribution for the code in the package. This field is vital for ensuring that downstream package recipients can address any ambiguity or concerns that might arise with the information in the SPDX document or the contents of the package it documents.

7.5.3 Examples

EXAMPLE 1 Tag: `PackageSupplier:`

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

EXAMPLE 2 RDF: Property `spdx:supplier` in class `spdx:Package`

```
<Package rdf:about="...">
    ...
    <supplier>Person: Jane Doe (jane.doe@example.com)</supplier>
    ...
</Package>
```

7.6 Package originator field

7.6.1 Description

If the package identified in the SPDX document originated from a different person or organization than identified as Package Supplier (see 7.5 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

AVA Documents
Document Sharing Hub

© ISO/IEC 2021 – All rights reserved

Full document details: ISO_IEC 5962_2021

party than the Package Supplier of the package. For example, the SPDX document identifies the package glibc and Red Hat as the Package Supplier, but the Free Software Foundation is the Package Originator.

Use `NOASSERTION` if:

— the SPDX document creator has attempted to but cannot reach a reasonable objective determination;

— the SPDX document creator has made no attempt to determine this field; or

— the SPDX document creator has intentionally provided no information (no meaning should be implied by doing so).

The metadata for the package originator field is shown in Table 18.

Table 18 — Metadata for the package originator field

Attribute	Value
Required	No
Cardinality	1..1
Format	Single line of text with one of the following keywords | `NOASSERTION` • `Person`: person name and optional `(<email>)` • `Organization`: organization name and optional `(<email>)`

7.6.2 Intent

Assist 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 document or the contents of the Package it documents.

7.6.3 Examples

EXAMPLE 1 Tag: `PackageOriginator:`

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

EXAMPLE 2 RDF: Property `spdx:originator` in class `spdx:Package`

```
<Package rdf:about="...">
    <originator>Organization: ExampleCodeInspect
    (contact@example.com)</originator>
</Package>
```


© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

7.7 Package download location field

7.7.1 Description

This section identifies the download Universal Resource Locator (URL), or a specific location within a version control system (VCS) for the package at the time that the SPDX document was created.

Use:

— `NONE` if there is no download location whatsoever.

— `NOASSERTION` if:

  — the SPDX document creator has attempted to but cannot reach a reasonable objective determination;

  — the SPDX document creator has made no attempt to determine this field; or

  — the SPDX document creator has intentionally provided no information (no meaning should be implied by doing so).

The metadata for the package download location field is shown in Table 19.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

Table 19 — Metadata for the package download location field

Attribute	Value
Required	Yes
Cardinality	1..1
Format	Uniform resource locator | VCS location | `NONE` | `NOASSERTION` For version-controlled files, the VCS location syntax is similar to a URL and has the: `<vcs_tool>+<transport>://<host_name>[/<path_to_repository>][@<revision_tag_or_branch>][#<sub_path>]` This VCS location compact notation (inspired and mostly adopted from pip as of 2015-02-20) supports referencing locations in version control systems such as Git, Mercurial, Subversion and Bazaar, and specifies the type of VCS tool using url prefixes: `git+`, `hg+`, `bzr+`, `svn+` and specific transport schemes such as SSH or HTTPS. Specifying sub-paths, branch names, a commit hash, a revision or a tag name is recommended, and supported using the `@` delimiter for commits and the `#` delimiter for sub-paths. Using user names and password in the `<host_name>` is not supported and should be considered as an error. User access control to URLs or VCS repositories shall be handled outside of an SPDX document. In VCS location compact notations, the trailing slashes in `<host_name>`, `<path_to_repository>` are not significant. Leading and trailing slashes in `<sub_path>` are not significant.

7.7.2 Intent

Where and how to download the exact package being referenced is critical verification and tracking data.

7.7.3 Examples

EXAMPLE 1 Tag: `PackageDownloadLocation:`

If ambiguous:

```
PackageDownloadLocation: NOASSERTION
```

```
PackageDownloadLocation: NONE
```

For a plain URL:

```
PackageDownloadLocation: http://ftp.gnu.org/gnu/glibc/glibc-ports-2.15.tar.gz
```

For Git:

© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

SPDX supported schemes are: `git`, `git+git`, `git+https`, `git+http`, and `git+ssh`. `git` and `git+git` are equivalent.

Here are the supported forms:

```
PackageDownloadLocation: git://git.myproject.org/MyProject

PackageDownloadLocation: git+https://git.myproject.org/MyProject.git

PackageDownloadLocation: git+http://git.myproject.org/MyProject

PackageDownloadLocation: git+ssh://git.myproject.org/MyProject.git

PackageDownloadLocation: git+git://git.myproject.org/MyProject

PackageDownloadLocation: git+git@git.myproject.org:MyProject
```

To specify a sub-path to a file or directory inside a repository use the # delimiter:

```
PackageDownloadLocation: git://git.myproject.org/MyProject#src/somefile.c

PackageDownloadLocation: git+https://git.myproject.org/MyProject#src/Clas
s.java
```

To specify branch names, a commit hash or a tag name, use the `@` delimiter:

```
PackageDownloadLocation: git://git.myproject.org/MyProject.git@master

PackageDownloadLocation: git+https://git.myproject.org/MyProject.git@v1.0

PackageDownloadLocation: git://git.myproject.org/MyProject.git@da39a3ee5e
6b4b0d3255bfef95601890afd80709
```

Sub-paths and branch names or commit hash can be combined too:

```
PackageDownloadLocation: git+https://git.myproject.org/MyProject.git@mast
er#/src/MyClass.cpp

PackageDownloadLocation: git+https://git.myproject.org/MyProject@da39a3ee
5e6b4b0d3255bfef95601890afd80709#lib/variable.rb
```

For Mercurial:

SPDX supported schemes are: `hg+http`, `hg+https`, `hg+static-http`, and `hg+ssh`.

The supported forms are:

```
PackageDownloadLocation: hg+http://hg.myproject.org/MyProject

PackageDownloadLocation: hg+https://hg.myproject.org/MyProject

PackageDownloadLocation: hg+ssh://hg.myproject.org/MyProject
```

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

To specify a sub-path to a file or directory inside a repository use the # delimiter:

```
PackageDownloadLocation: hg+https://hg.myproject.org/MyProject#src/somefi
le.c
```

```
PackageDownloadLocation: hg+https://hg.myproject.org/MyProject#src/Class.
java
```

To pass branch names, a commit hash, a tag name or a local branch name use the @ delimiter:

```
PackageDownloadLocation: hg+https://hg.myproject.org/MyProject@da39a3ee5e
6b
```

```
PackageDownloadLocation: hg+https://hg.myproject.org/MyProject@2019
```

```
PackageDownloadLocation: hg+https://hg.myproject.org/MyProject@v1.0
```

```
PackageDownloadLocation: hg+https://hg.myproject.org/MyProject@special_fe
ature
```

Sub-paths and branch names or commit hash can be combined too:

```
PackageDownloadLocation: hg+https://hg.myproject.org/MyProject@master#/sr
c/MyClass.cpp
```

```
PackageDownloadLocation: hg+https://hg.myproject.org/MyProject@da39a3ee5e
6b#lib/variable.rb
```

For Subversion:

SPDX supported schemes are: `svn`, `svn+svn`, `svn+http`, `svn+https`, `svn+ssh`. `svn` and `svn+svn` are equivalent.

The supported forms are:

```
PackageDownloadLocation: svn://svn.myproject.org/svn/MyProject
```

```
PackageDownloadLocation: svn+svn://svn.myproject.org/svn/MyProject
```

```
PackageDownloadLocation: svn+http://svn.myproject.org/svn/MyProject/trunk
```

```
PackageDownloadLocation: svn+https://svn.myproject.org/svn/MyProject/trun
k
```

To specify a sub-path to a file or directory inside a repository use the # delimiter:

```
PackageDownloadLocation: svn+https://svn.myproject.org/MyProject#src/some
file.c
```

```
PackageDownloadLocation: svn+https://svn.myproject.org/MyProject#src/Clas
s.java
```


© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

This support is less important for SVN since the URL path can also contain sub-paths; this two forms are equivalent:

```
PackageDownloadLocation: svn+https://svn.myproject.org/MyProject/trunk#sr
c/somefile.c
```

```
PackageDownloadLocation: svn+https://svn.myproject.org/MyProject/trunk/sr
c/somefile.c
```

You can specify a revision using the `@` delimiter:

```
PackageDownloadLocation: svn+https://svn.myproject.org/svn/MyProject/trun
k@2019
```

Sub-paths and revisions can be combined too:

```
PackageDownloadLocation: svn+https://svn.myproject.org/MyProject@123#/src
/MyClass.cpp
```

```
PackageDownloadLocation: svn+https://svn.myproject.org/MyProject/trunk@12
34#lib/variable/variable.rb
```

For Bazaar:

SPDX supported schemes are: `bzr+http`, `bzr+https`, `bzr+ssh`, `bzr+sftp`, `bzr+ftp`, and `bzr+lp`.

The supported forms are:

```
PackageDownloadLocation: bzr+https://bzr.myproject.org/MyProject/trunk
```

```
PackageDownloadLocation: bzr+http://bzr.myproject.org/MyProject/trunk
```

```
PackageDownloadLocation: bzr+sftp://myproject.org/MyProject/trunk
```

```
PackageDownloadLocation: bzr+ssh://myproject.org/MyProject/trunk
```

```
PackageDownloadLocation: bzr+ftp://myproject.org/MyProject/trunk
```

```
PackageDownloadLocation: bzr+lp:MyProject
```

To specify a sub-path to a file or directory inside a repository use the `#` delimiter:

```
PackageDownloadLocation: bzr+https://bzr.myproject.org/MyProject/trunk#sr
c/somefile.c
```

```
PackageDownloadLocation: bzr+https://bzr.myproject.org/MyProject/trunk#sr
c/Class.java
```

You can specify a revision or tag using the `@` delimiter:

```
PackageDownloadLocation: bzr+https://bzr.myproject.org/MyProject/trunk@20
19
```

```
PackageDownloadLocation: bzr+http://bzr.myproject.org/MyProject/trunk@v1.
0
```

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

Sub-paths and revisions can be combined too:

```
PackageDownloadLocation: bzr+https://bzr.myproject.org/MyProject/trunk@20
19#src/somefile.c
```

EXAMPLE 2 RDF: Property `spdx:downloadLocation` in class `spdx:Package`

```
<Package rdf:about="...">
    <downloadLocation>http://ftp.gnu.org/gnu/glibc/glibc-ports-2.15.tar.g
z</downloadLocation>
</Package>

<Package rdf:about="...">
    <downloadLocation>
        git+https://git.myproject.org/MyProject.git@v10.0#src/lib.c
    </downloadLocation>
</Package>

<Package rdf:about="...">
    <downloadLocation rdf:resource="spdx:noassertion"/>
</Package>

<Package rdf:about="...">
    <downloadLocation rdf:resource="spdx:none"/>
</Package>
```

7.8 Files analyzed field

7.8.1 Description

Indicates whether the file content of this package has been available for or subjected to analysis when creating the SPDX document. If `false`, indicates packages that represent metadata or URI references to a project, product, artifact, distribution or a component. If `false`, the package shall not contain any files. The metadata for the files analyzed field is shown in Table 20.

Table 20 — Metadata for the files analyzed field

Attribute	Value
Required	No. If omitted, the default value of `true` is assumed.
Cardinality	1..1
Format	Boolean

7.8.2 Intent

A package can refer to a project, product, artifact, distribution or a component that is external to the SPDX document.

Some examples:

a) **A bundle of external products**: Package A can be metadata about Packages and their dependencies. It may also be a loosely organized manifest of references to Packages involved in a product or project. Build or execution may transitively discover more Packages and dependencies. All of these

© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

referenced Packages can have their own SPDX documents. In this case, Package A may be defined with its File Analyzed attribute set to `false`. Package A includes External Document References to SPDX documents containing Packages referenced in all the available relationships. The Relationships section then relates the SPDX documents and contained SPDX elements with appropriate semantics per the dependencies in the scope of Package A.

b) **Package relation to external product**: Package A can have a STATIC_LINK relationship to Package B, but the binary representation of Package B is furnished by the build process and thus not contained in the file list of Package A. In this case, Package B needs to be defined with its Files Analyzed attribute set to false and all the other attributes subject to the subsequently defined constraints. Then, the relationship between Package A and Package B can be documented as described in Clause 11.

c) **File derived from external product**: Package A contains multiple files derived from an outside project. Rather than use the `artifactOf*` attributes (F.9-4.11) to describe the relation of these files to their project, the outside project can be represented by another package, Package B, whose `FilesAnalyzed` (7.8) attribute is set to `false`. Each of the binary files can then have a relationship to package B (Clause 10). This allows the outside project to be represented by a single SPDX identifier (the identifier of Package B). It also allows the relationship(s) between the outside project and each of the files be represented in much more detail.

7.8.3 Examples

EXAMPLE 1 Tag: `FilesAnalyzed`

```
FilesAnalyzed: false
```

EXAMPLE 2 RDF: Property `spdx:filesAnalyzed` in class `spdx:Package`

```
<Package rdf:about="...">
    ...
    <filesAnalyzed>false</filesAnalyzed>
    ...
</Package>
```

7.9 Package verification code field

7.9.1 Description

This field provides an independently reproducible mechanism identifying specific contents of a package based on the actual files (except the SPDX document itself, if it is included in the package) that make up each package and that correlates to the data in this SPDX document. 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 document as part of a package. The metadata for the package verification code field is shown in Table 21.

© ISO/IEC 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021

Table 21 — Metadata for the package verification code field

Attribute	Value
Required	Yes
Cardinality	0..1 if `FilesAnalyzed` (7.8) is `true` or omitted, 0..0 (shall be omitted) if `FilesAnalyzed` is `false`.
Algorithm	(see the algorithm below)
Format	Single line of text with 160-bit binary represented as 40 lowercase hexadecimal digits

Algorithm

```
verificationcode = 0
filelist = templist = ""
for all files in the package {
    if file is an "excludes" file, skip it /* exclude SPDX analysis file(
s) */

        append templist with "SHA1(file)/n"
    }
sort templist in ascending order by SHA1 value
filelist = templist with "/n"s removed. /* ordered sequence of SHA1 value
s with no separators */
verificationcode = SHA1(filelist)
```

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

Required sort order: '0','1','2','3','4','5','6','7','8','9','a','b','c','d','e','f' (ASCII order)

7.9.2 Intent

Provide a unique identifier based on the files inside each package, eliminating confusion over which version or modification of a specific package the SPDX document refers to. This field also permits embedding the SPDX document within the package without altering the identifier.

7.9.3 Examples

EXAMPLE 1 Tag: `PackageVerificationCode:` (and optionally `(excludes: FileName)`)

`FileName` is specified in 8.1.

```
PackageVerificationCode: d6a770ba38583ed4bb4525bd96e50461655d2758 (exclud
es: ./package.spdx)
```


© ISO/IEC 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 5962_2021