

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)

© ISO/IEC 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

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

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

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

7.22.2 Intent49

7.22.3 Examples50

7.23 Package attribution text field50

7.23.1 Description50

7.23.2 Intent51

7.23.3 Examples51

8 File information section51

8.1 File name field51

8.1.1 Description51

8.1.2 Intent52

8.1.3 Examples52

8.2 File SPDX identifier field52

8.2.1 Description52

8.2.2 Intent52

8.2.3 Examples52

8.3 File type field53

8.3.1 Description53

8.3.2 Intent54

8.3.3 Examples54

8.4 File checksum field54

8.4.1 Description54

8.4.2 Intent55

8.4.3 Examples55

8.5 Concluded license field56

8.5.1 Description56

8.5.2 Intent56

8.5.3 Examples56

8.6 License information in file field57

8.6.1 Description57

8.6.2 Intent58

8.6.3 Examples58

8.7 Comments on license field58

8.7.1 Description58

8.7.2 Intent59

8.7.3 Examples59

8.8 Copyright text field59

8.8.1 Description59

8.8.2 Intent60

8.8.3 Examples60

8.9 Artifact of project name field (deprecated)60

8.9.1 Description60

8.9.2 Intent61

8.9.3 Examples61

8.10 Artifact of project homepage field (deprecated)61

8.10.1 Description61

8.10.2 Intent61

8.10.3 Examples61

8.11 Artifact of project uniform resource identifier field (deprecated)62

8.11.1 Description62

8.11.2 Intent62

8.11.3 Examples62

8.12 File comment field63

8.12.1 Description63

8.12.2 Intent63

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

9.10 Snippet name field78

9.10.1 Description78

9.10.2 Intent78

9.10.3 Examples78

9.11 Snippet attribution text field78

9.11.1 Description78

9.11.2 Intent79

9.11.3 Examples79

10 Other licensing information detected section79

10.1 License identifier field.....79

10.1.1 Description79

10.1.2 Intent80

10.1.3 Examples80

10.2 Extracted text field.....80

10.2.1 Description80

10.2.2 Intent81

10.2.3 Examples81

10.3 License name field82

10.3.1 Description82

10.3.2 Intent82

10.3.3 Examples82

10.4 License cross reference field.....82

10.4.1 Description82

10.4.2 Intent83

10.4.3 Examples83

10.5 License comment field.....83

10.5.1 Description83

10.5.2 Intent83

10.5.3 Examples83

11 Relationships between SPDX elements information section84

11.1 Relationship field.....84

11.1.1 Description84

11.1.2 Intent89

11.1.3 Examples89

11.2 Relationship comment field90

11.2.1 Description90

11.2.2 Intent90

11.2.3 Examples90

12 Annotations information section.....91

12.1 Annotator field.....91

12.1.1 Description91

12.1.2 Intent91

12.1.3 Examples91

12.2 Annotation date field92

12.2.1 Description92

12.2.2 Intent92

12.2.3 Examples92

12.3 Annotation type field93

12.3.1 Description93

12.3.2 Intent93

12.3.3 Examples93

12.4 SPDX identifier reference field.....93

12.4.1 Description93

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: omissible 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

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

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

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

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.

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.

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>