ICS 35.100.05
CCS L79

SJ

中华人民共和国电子行业标准

SJ/T XXXXX—XXXX

信息技术 软件物料清单数据格式规范

Information technology—Software bill of materials data format specification

（报批稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国工业和信息化部　　发布

目 次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息技术标准化技术委员会（SAC/TC28）提出并归口。

本文件起草单位：中国电子技术标准化研究院、清华大学、国家工业信息安全发展研究中心、北京大学、华为技术有限公司、浪潮通用软件有限公司、中兴通讯股份有限公司、北京百度网讯科技有限公司、蚂蚁科技集团股份有限公司、苏州棱镜七彩信息科技有限公司、上海探巡科技有限公司、北京迪力科技有限责任公司、北京安普诺信息技术有限公司、中电金信软件有限公司、南方电网数字电网研究院股份有限公司、北京中科微澜科技有限公司、湖南智擎科技有限公司、北京奥思研工智能科技有限公司、腾讯云计算（北京）有限责任公司、中国人寿保险股份有限公司、京东科技信息技术有限公司、北京天融信网络安全技术有限公司。

本文件主要起草人：范科峰、王威伟、黄向东、杨丽蕴、于昕、苏伟、周明辉、周峻松、邓昌义、徐亮、贾昌国、柯猛、崔锦国、郑伟波、仪思奇、项曙明、李响、马红伟、白晓媛、武延军、梁大功、黄浩东、辛华、王宇、杨杰、黄振恒、张涛、董毅、陈行、姜倩、武剑凌、况文川、章澜、杨牧天、尹刚、李彦成、耿航航、陈少鹏、卢晓梅、陈永梅、董淑照、余瞰、韩翼、郑伟娜、蔡斌哲、王龑、张静。

信息技术 软件物料清单数据格式规范

1 范围

本文件给出了软件物料清单数据格式，包括：文档基本信息、软件组成信息、环境信息和扩展信息。

本文件适用于指导软件物料清单的生成、存储、维护与交付。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 7408.1-2023 日期和时间 信息交换表示法 第1部分：基本原则

ISO/IEC 5962 信息技术 SPDX规范2.2.1版本（Information technology - SPDX Specification V2.2.1）

3 术语和定义

下列术语和定义适用于本文件。

3.1

软件物料清单 software bill of materials

描述软件产品的组成成分、许可证信息、组成要素之间关系等信息的文档。

[来源：GB/T 43698-2024,3.8,有修改]

3.2

组件 component

组件是具有封装性、独立性和可复用性的软件单元，其内部封装数据和代码逻辑，对外提供标准接口，可独立发布并被第三方集成。

3.3

文件 file

文件是构成软件包的基本数据单元，每个文件都关联一个文件信息实例，该实例包含了文件的许可证条款、版权声明等关键元数据属性。

3.4

代码片段 snippet

代码片段是指文件中具有连续性的代码区域，作为文件的组成部分，可独立标识和引用。

3.5

构建环境 build environment

构建环境是指用于编译、链接和打包软件的完整系统环境，涵盖CPU架构、操作系统、构建工具素，记录了软件的生成条件。

3.6

运行环境 runtime environment

运行环境是指软件执行所依赖的系统环境条件的完整描述，涵盖CPU架构、操作系统以及软件运行所必需的系统组件、网络服务等必要环境条件信息。

4 缩略语

下列缩略语适用于本文件。

AI 人工智能（Artificial Intelligence）

API 应用程序编程接口（Application Programming Interface）

BIN 二进制（BINary）

CPU 中央处理器（Central Processing Unit）

GIF 图形交换格式（Graphics Interchange Format）
HTML 超文本标记语言（Hyper Text Markup Language）
ID 标识（IDentity）
JPEG 联合图像专家组制定的一种图像压缩格式（Joint Photographic Experts Group）
JSON JavaScript对象表示法（JavaScript Object Notation）
MIME 多用途互联网邮件扩展类型(Multipurpose Internet Mail Extensions)
MP3 动态影像专家压缩标准音频层Ⅲ编码（Moving Picture Experts Group Audio Layer Ⅲ）
NPM Node包管理器（Node Package Manager）
OS 操作系统（Operating System）
PURL 包统一资源定位符（Package Uniform Resource Locator）
SBOM 软件物料清单（Software Bill Of Materials）
SHA 安全散列算法（Secure Hash Algorithm）
SPDX 软件包数据交换（Software Package Data eXchange）
URI 统一资源标识符（Uniform Resource Identifier）
URL 统一资源定位符（Uniform Resource Locator）
UTC 协调世界时（Universal Time Coordinated）
UTF-8 8位Unicode转换格式（8-bit Unicode Transformation Format）
VCS 版本控制系统（Version Control System）
XML 可扩展标记语言（eXtensible Markup Language）
YAML YAML标记语言（YAML Ain't Markup Language）

5 软件物料清单组成

5.1 概述

SBOM由文档基本信息、软件组成信息、环境信息和扩展信息等元素组成，见图1。

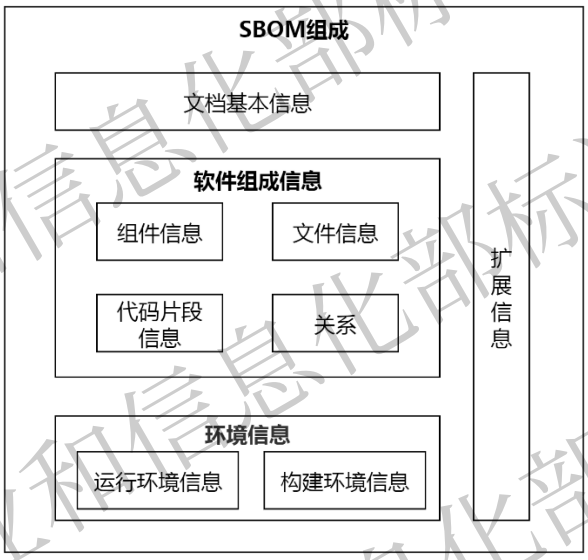

图1 SBOM 组成

每个组成元素的说明如下。

a） 文档基本信息（Document Basic Information）：SBOM 文档所涉及的版本号、标识、创建者、创建时间等信息，为处理工具的前向和后向兼容性提供必要的信息。

b） 软件组成信息（Software Compostition Information）：软件中具体组成成分的信息，包括：组件信息、文件信息、代码片段信息和关系。其中，组件与文件为非强关联，文件可以

独立存在，不归属任何组件；代码片段则属于某个特定文件，见图 2。

- 组件信息（Component Information）：SBOM文档所描述的软件产品涉及的软件组件的相关信息。
- 文件信息（File Information）：SBOM文档所描述的软件产品涉及的文件的相关信息。
- 代码片段信息（Snippet Information）：与SBOM文档中所描述的某一特定文件相关。当已知文件中某些内容包含在另一原始源文件时，可选择使用代码片段信息进行标注。当文件的某些内容可能是在另一个许可证下创建的，也可用代码片段信息进行标注。
- 关系（Relationships）：描述SBOM文档中组件、文件和代码片段等元素之间的关系。

c）环境信息（Environment Information）：对软件构建环境和运行环境的主要信息进行说明，提升软件供应链的追溯性，包括：构建环境信息和运行环境信息。

d）扩展信息（Extended Information）：描述本文件中未定义的其他软件物料信息，以便更全面的描述和管理软件供应链。

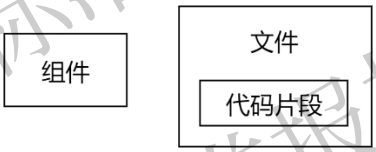

图2　SBOM 组件、文件与代码片段之间的层次关系

软件物料清单各元素按照“应、宜、可”的方式进行分层级管理（一级指标要求），各元素中具体字段按照“必选、可选”的必要性提出要求（二级指标要求），见表1。

表1　软件物料清单元素与字段总表

元素名		一级指标要求	字段名（全称）	中文名称	SBOM中使用的字段名	二级指标要求
文档基本信息（Document Basic Information）		应	SBOM Format	文档使用的数据格式	sbomFormat	必选
			Document License	文档许可证	documentLicense	可选
			Document Name	文档名称	documentName	必选
			Document Version	文档版本	documentVersion	必选
			Document Namespace	文档命名空间	documentNamespace	可选
			Tool Information	工具信息	toolInfo	必选
			SBOM Author	创建者信息	sbomAuthor	必选
			Timestamp	文档时间戳	timestamp	必选
			SBOM Author Comments	创建者备注	sbomAuthorComments	必选
			SBOM Comments	文档其他信息	sbomComments	必选
软件组成信息（Software Compostition Information）	组件信息（Component Information）	应	Component Identifier	组件标识符	componentId	必选
			Component Name	组件名称	componentName	必选
			Component Version	组件版本	componentVersion	必选
			Component Author	组件作者	componentAuthor	必选
			Component Provider	组件供应商	componentProvider	必选
			Component Home	组件主页	componentHome	可选
			Component Download	组件下载位置	componentDownload	可选
			Component License	组件许可证	license	必选
			Comments on Component License	组件许可证其他信息	componentLicComments	可选
			Component Copyright	组件版权信息	componentCopyright	可选
			Component Hash Value	组件哈希值	componentHashValue	必选
			Component Timestamp	组件时间戳	componentTimestamp	必选
			Component Platform	组件平台架构	componentPlatform	可选
			AI Function	人工智能功能	componentAIFunction	可选
			Component Comments	组件其他信息	componentComments	可选

表1　软件物料清单元素与字段总表（续）

元素名		一级指标要求	字段名（全称）	中文名称	SBOM中使用的字段名	二级指标要求
			Component Extended Information	组件扩展信息	componentExtInfo	可选
	文件信息（File Information）	宜	File Identifier	文件标识符	fileId	必选
			File Name	文件名	fileName	必选
			File Type	文件类型	fileType	可选
			File License	文件许可证	fileLicense	必选
			Comments on File License	文件许可证其他信息	fileLicComments	可选
			File Copyright	文件版权信息	fileCopyright	可选
			File Author	文件作者	fileAuthor	可选
			File URL	文件溯源信息	fileUrl	可选
			File Hash Value	文件哈希值	fileHashValue	必选
			File Comments	文件其他信息	fileComments	可选
			File Extended Information	文件扩展信息	fileExtInfo	可选
	代码片段信息（Snippet Information）	可	Snippet Identifier	代码片段标识符	snippetId	必选
			Snippet Name	代码片段名称	snippetName	可选
			Snippet from File Identifier	代码片段关联文件标识符	snippetFileId	必选
			Snippet Source URL	代码片段来源信息	snippetSourceUrl	必选
			Snippet Byte Range	代码片段字节范围	snippetByteRange	必选
			Snippet Line Range	代码片段行范围	snippetLineRange	可选
			Snippet License	代码片段许可证	snippetLicense	必选
			Comments on Snippet License	代码片段许可证其他信息	snippetLicComments	可选
			Snippet Copyright	代码片段版权信息	snippetCopyright	必选
			AI Generated Snippet	人工智能生成代码片段	snippetAIGenerated	可选
			Snippet Comments	代码片段其他信息	snippetComments	可选
			Snippet Extended Information	代码片段扩展信息	snippetExtInfo	可选
	关系（Relationships）	应	SBOM Element Identifier	SBOM元素标识符	sbomElementId	必选
			Relationship Type	关系类型	relationshipType	必选
			Related SBOM Element Identifier	相关SBOM元素标识符	relatedSbomElementId	必选
环境信息（Environment Information）	构建环境信息（Build Environment Information）	可	Build Environment Architecture	构建环境CPU架构	buildArch	必选
			Build Environment OS	构建环境操作系统	buildOS	必选
			Build Environment Software Dependencies	构建环境第三方软件依赖	buildSoftDeps	可选
			Build Time	构建时间	buildTime	可选
			Build Pipeline Number	构建流水线号	buildPipeNo	可选
			Build Tool	构建工具	buildTool	可选
	运行环境信息（Runtime Information）	可	Runtime Environment Architecture	运行环境CPU架构	runtimeArch	必选
			Runtime Environment OS	运行环境操作系统	runtimeOS	必选

表1 软件物料清单元素与字段总表（续）

元素名		一级指标要求	字段名（全称）	中文名称	SBOM中使用的字段名	二级指标要求
			Runtime Environment Software Dependencies	运行环境第三方软件依赖	runtimeSoftDeps	可选
			Runtime Environment Network Services Dependencies	运行环境网络服务依赖	runtimeNetServDeps	可选
扩展信息（Extended Information）		可	Extended Information	扩展信息	extendedInfo	必选

5.2 格式基本要求

SBOM文档符合以下要求：

a) 应具有可读性，采用明确清晰的层次结构，包含适当的标题、描述和注释；
b) 应采用软件工具可以读写的语法；
c) 应支持语法自动检查；
d) SBOM 文档应使用 UTF-8 编码；
e) 应使用的文件格式：

- JSON
- XML
- YAML

5.3 文档基本信息（Document Basic Information）

5.3.1 概述

文档基本信息包括的字段见表2。

表2 文档基本信息字段

字段名（全称）	中文名称	SBOM中使用的字段名	必要性
SBOM Format	文档使用的数据格式	sbomFormat	必选
Document License	文档许可证	documentLicense	可选
Document Name	文档名称	documentName	必选
Document Version	文档版本	documentVersion	必选
Document Namespace	文档命名空间	documentNamespace	可选
Tool Information	工具信息	toolInfo	必选
SBOM Author	创建者信息	sbomAuthor	必选
Timestamp	文档时间戳	timestamp	必选
SBOM Author Comments	创建者备注	sbomAuthorComments	必选
SBOM Comments	文档其他信息	sbomComments	必选

5.3.2 文档使用的数据格式（SBOM Format）

本字段记录使用的SBOM数据格式，由格式名称和版本号组成。考虑到软件是数字产品的核心，为了便于依据本文件生成、转换、验证和管理SBOM，用“BOM-SW”作为符合本文件的标识和缩写，用v2.0作为版本号。

数据格式为：BOM-SW-格式版本。

示例：“sbomFormat”: “BOM-SW-v2.0”

5.3.3 文档许可证（Document License）

本字段记录文档许可证，其约束的范围包括填入SBOM文档的数据。

SBOM文档创建者和接收者可选择许可证或签订协议，限制SBOM文档或特定元数据的发布和识别。若许可证表达式为ISO/IEC 5962标准中SPDX许可证列表所列许可证，则应按其许可证列表中许可证缩写书写。

数据格式为：许可证表达式，或其他文本。

示例：“documentLicense”: “CC0-1.0”

5.3.4 文档名称（Document Name）

本字段记录创建者指定此SBOM文档的名称。应具有唯一名称，包含软件名称及版本。

数据格式为：文本。

示例：“documentName”: “glibc-v2.3”

5.3.5 文档版本（Document Version）

本字段记录每次更新、删除、修改或重新生成SBOM文档时，SBOM文档的版本信息。

数据格式为：文本。

示例：“documentVersion”: “2.1.1”

5.3.6 文档命名空间（Document Namespace）

本字段记录SBOM文档特定的命名空间，其作为唯一的统一资源标识符(URI)，其中不应包含“#”分隔符。

SBOM文档的每一个版本都应对应一个唯一的URI。

数据格式为：唯一的统一资源标识符(URI)。

示例：“documentNamespace”: “http://license.coscl.org.cn/XXX-SBOM”

5.3.7 工具信息（Tool Information）

本字段记录生成SBOM文档的工具信息，包括厂商名称、工具名称和工具版本等。

数据格式为：厂商-工具名称-版本。

示例：“toolInfo”: “ABC-XCheck-v1.0”

5.3.8 创建者信息（SBOM Author）

本字段记录指定创建此文档的工具、个人或组织。

数据格式为：文本。

示例：“sbomAuthor”: “Jane Doe”

5.3.9 文档时间戳（Timestamp）

本字段记录最初创建SBOM文档以及每次更新的时间，应按GB/T 7408.1-2023标准中规定的UTC格式的合并日期和时间指定。

数据格式为：YYYY-MM-DDThh:mm:ssTZD。

示例：“timestamp”: “2023-03-29T18:30:22+08:00”

5.3.10 创建者备注（SBOM Author Comments）

用于记录关于SBOM文档的创建者的附加说明。

数据格式为：文本。

示例：“sbomAuthorComments”: “文档审核状态：内部已复核。”

5.3.11 文档其他信息（SBOM Comments）

本字段记录对SBOM文档进行附加的说明解释或描述。

数据格式为：文本。

示例：“sbomComments”: “no comments”

5.4 软件组成信息（Software Composition Information）

5.4.1 组件信息（Component Information）

5.4.1.1 概述

组件信息包括的字段见表3。

表3 组件信息字段

字段名（全称）	中文名称	SBOM中使用的字段名	必要性
Component Identifier	组件标识符	componentId	必选
Component Name	组件名称	componentName	必选
Component Version	组件版本	componentVersion	必选
Component Author	组件作者	componentAuthor	必选
Component Provider	组件供应商	componentProvider	必选
Component Home	组件主页	componentHome	可选
Component Download	组件下载位置	componentDownload	可选
Component License	组件许可证	license	必选
Comments on Component License	组件许可证其他信息	componentLicComments	可选
Component Copyright	组件版权信息	componentCopyright	可选
Component Hash Value	组件哈希值	componentHashValue	必选
Component Timestamp	组件时间戳	componentTimestamp	必选
Component Platform	组件平台架构	componentPlatform	可选
AI Function	人工智能功能	componentAIFunction	可选
Component Comments	组件其他信息	componentComments	可选
Component Extended Information	组件扩展信息	componentExtInfo	可选

5.4.1.2 组件标识符（Component Identifier）

本字段用于识别组件或作为相关数据库查询的唯一标识符。本文件使用PURL作为唯一标识符。

数据格式为：文本。

示例： “componentId”: “pkg:deb/debian/curl@7.50.3-1?arch=i386&distro=Jessie”

5.4.1.3 组件名称（Component Name）

本字段记录组件发起方应提供的组件的全名。

数据格式为：文本。

示例1：“componentName”: “glibc”

示例2：“componentName”: “log4j-src”

5.4.1.4 组件版本（Component Version）

本字段记录组件的版本，用于识别组件版本和指示组件版本的后续更改，应至少包含主版本号与次版本号。

数据格式为：文本。

示例：“componentVersion”: “2.11.1”

5.4.1.5 组件作者（Component Author）

本字段记录软件组件的创作者或主要贡献者相关信息。应详细说明作者的姓名、所属组织（若有）、联系电子邮箱（若有）以及在组件创建过程中的角色或主要贡献等。

数据格式为：

——“name: 姓名”；

——“organization: 组织名称”；

——“email: 电子邮箱地址”；

——“role: 角色或贡献”。

示例：

```
“componentAuthor”: [
 {
      “name”: “张三”,
      “organization”: “XYZ公司”,
```

```
        "email": "john.smith@abctech.com",
        "role": "测试。张三对软件组件进行了广泛的测试，并识别和报告错误。"
    }
]
```

5.4.1.6 组件供应商（Component Provider）

本字段记录提供软件组件的实体相关信息。应包含供应商的完整名称、供应商的简称（若有）、供应商的官方网站（若有）、供应商的联系方式（如电话、邮箱等，若有）以及供应商在软件供应链中的位置和主要业务范围等。

数据格式为：

——“fullName: 公司全称”；

——“shortName: 公司缩写”；

——“webSite: 公司网站”；

——“contactNumber: 联系电话”；

——“email: 电子邮箱”；

——“description: 公司简介”。

示例：

```
"componentProvider": {
    "fullName": "ABC公司",
    "shortName": "ABC",
    "webSite": "https://www.abc.com",
    "contactNumber": "+1-425-882-8888",
    "email": "support@abc.com",
    "description": "ABC公司是一家全球领先的技术公司，提供广泛的软件组件和服务。"
}
```

5.4.1.7 组件主页（Component Home）

本字段记录组件主页网站位置。

数据格式为：URL，或NONE，或NOASSERTION。具体要求如下：

——NONE，如果不存在组件主页；

——NOASSERTION，如果 SBOM 文档创建者未提供任何信息。

示例："componentHome": "http://ftp.gnu.org/gnu/glibc"

5.4.1.8 组件下载位置（Component Download）

本字段记录创建时用于下载组件的统一资源定位符(URL)或在版本控制系统(VCS)中的特定位置。

数据格式为：URL，或VCS位置，或NONE，或NOASSERTION。具体要求如下：

——NONE，如果没有任何下载位置；

——NOASSERTION，如果 SBOM 文档创建者未提供任何信息。

示例："componentDownload": "http://ftp.gnu.org/gnu/glibc/glibc-ports-2.15.tar.gz"

5.4.1.9 组件许可证（Component License）

本字段记录组件作者已声明的许可证。若许可证表达式为ISO/IEC 5962标准中SPDX许可证列表所列许可证，则应按其许可证列表中许可证缩写书写。

数据格式为：[许可证名称1，许可证名称2]。

示例："license": ["LGPL-2.0-only"]

5.4.1.10 组件许可证其他信息（Comments on Component License）

本字段记录组件许可证原文信息。

数据格式为：文本，或NONE，或NOASSERTION。具体要求如下：

——NONE，如果组件中不包含任何许可证信息；

——NOASSERTION，如果 SBOM 文档创建者未提供任何信息。

示例："componentLicComments": "Permission is hereby granted, free of charge, to any person obtaining

a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.”

5.4.1.11 组件版权信息（Component Copyright）

本字段记录组件的版权所有者以及存在的任何日期。该字段的内容是从组件信息文件中提取的自由形式的文本。

数据格式为：文本，或NONE，或NOASSERTION。具体要求如下：

——与版权声明有关的任何文本，即使该文本不完整；

——NONE，如果软件组件不包含任何版权信息；

——NOASSERTION，如果 SBOM 文档创建者未提供任何信息。

示例：“componentCopyright”: “Copyright 2008-2010 John Smith”

5.4.1.12 组件哈希值（Component Hash Value）

本字段记录用于校验组件完整性的信息，避免在引用特定组件的某个版本或修订时发生混淆。该字段的值应采用安全的摘要算法（如：SHA224、SHA256、SHA384、SHA512、SM3）对该组件的完整内容进行摘要计算，将算法和摘要值共同作为组件的哈希值。

数据格式为：

——algorithm：算法标识符（如：SHA256）；

——hashValue：算法摘要值（小写十六进制数字）。

示例：

```
“componentHashValue”: [
 {
     “algorithm”: “SHA256”,
     “hashValue”: “60fd2bc1c230c958706ee28bbdf37a94d6ceef8ac79dfe82a42464401ce75381”
 },
 {
     “algorithm”: “SM3”,
     “hashValue”: “66C7F0F462EEEDD9D1F2D46BDC10E4E24167C4875CF2F7A2297DA02B8F4BA8E0”
 }
]
```

5.4.1.13 组件时间戳（Component Timestamp）

本字段记录组件SBOM数据生成或更新的时间戳。应按GB/T 7408.1-2023标准中规定的UTC格式的合并日期和时间指定。

数据格式为：YYYY-MM-DDThh:mm:ssTZD。

示例：“componentTimestamp”: “2023-03-29T18:30:22+08:00”

5.4.1.14 组件平台架构（Component Platform）

本字段记录组件所支持的操作系统与CPU架构。

数据格式为：[操作系统名称]/[CPU架构名称]。具体要求如下：

——若支持多种架构时，用“,”分割；

——若是没有平台架构要求，则填 NOARCH。

示例：“componentPlatform”: “linux/amd64,linux/arm64,darwin/arm64”

5.4.1.15 人工智能功能（AI Function）

本字段记录组件是否包含人工智能技术。

数据格式为：true，或false，或NOASSERTION。具体要求如下：

——true，表示指定组件包含人工智能技术；

——false，表示指定组件未包含人工智能技术；

——NOASSERTION，如果 SBOM 文档创建者未提供任何信息。

示例：“componentAIFunction”: true

5.4.1.16 组件其他信息（Component Comments）

本字段记录对组件进行附加的说明解释或描述。

数据格式为：文本。

示例：“componentComments”: “no comments”

5.4.1.17 组件扩展信息（Component Extended Information）

本字段记录在组件中未定义的、根据实际情况选择性扩充的组件信息。

数据格式为：使用对象的方式表达。

示例：

```
“componentExtInfo”: {
    “vulCveId”: “CVE-2024-38077”,
    “vulCveComments”: “Windows 远程桌面许可服务漏洞”
}
```

5.4.2 文件信息（File Information）

5.4.2.1 概述

文件信息包括的字段见表4。

表4 文件信息字段

字段名（全称）	中文名称	SBOM中使用的字段名	必要性
File Identifier	文件标识符	fileId	必选
File Name	文件名	fileName	必选
File Type	文件类型	fileType	可选
File License	文件许可证	fileLicense	必选
Comments on File License	文件许可证其他信息	fileLicComments	可选
File Copyright	文件版权信息	fileCopyright	可选
File Author	文件作者	fileAuthor	可选
File URL	文件溯源信息	fileUrl	可选
File Hash Value	文件哈希值	fileHashValue	必选
File Comments	文件其他信息	fileComments	可选
File Extended Information	文件扩展信息	fileExtInfo	可选

5.4.2.2 文件标识符（File Identifier）

本字段记录SBOM文档中可能被其他元素引用的文件标识，应确保每个文件标识符在SBOM文档内的唯一性。

数据格式为：SERef-file-[idstring]，其中，[idstring]是唯一的字串，包含字母、数字、“.”、“_”。

示例：“fileId”: “SERef-file-01”

5.4.2.3 文件名（File Name）

本字段记录文件的完整路径、文件名以及文件扩展名。

数据格式为：具有包存档或目录根的相对文件名，其中，每个文件名都以 ./ 开头，每个文件的路径应为该文件在当前软件包或存档的相对路径。

示例：“fileName”: “./package/foo.c”

5.4.2.4 文件类型（File Type）

本字段记录有关文件类型的信息。一个文件可能分配多个文件类型。

数据格式为：SOURCE，或BINARY，或TEXT，或IMAGE，或AUDIO，或VIDEO，或APPLICATION，或ML_MODEL，或SBOM，或OTHER。具体要求如下：

——SOURCE，如果文件是可读的源代码（.c、.html 等）；

——BINARY，如果文件是编译对象、目标映像或二进制可执行文件（.o、.a 等）；
——TEXT，如果文件是可读的文本文件（文本类 MIME）；
——IMAGE，如果文件与图片图像文件相关联（图像类 MIME，例如 .jpeg、.gif）；
——AUDIO，如果文件与音频文件相关联（音频类 MIME，例如 .mp3）；
——VIDEO，如果文件与视频文件类型（视频类 MIME）；
——APPLICATION，如果文件与特定的应用程序（应用类 MIME/*）相关联；
——ML_MODEL，如果文件代表机器学习模型（机器学习模型类文件，例如：.bin、.safetensors 等）；
——SBOM，如果该文件用作软件物料清单；
——OTHER，如果文件不属于上述类别（生成的工件、数据文件等）。

示例1：“fileType”: [“ML_MODEL”]
示例2：“fileType”: [“SOURCE”, “TEXT”]

5.4.2.5 文件许可证（File License）

本字段记录SBOM文档创建者推断出的用于管理文件的许可证或无法确定管理许可证的替代值。若许可证表达式为ISO/IEC 5962标准中SPDX许可证列表所列许可证，则应按其许可证列表中许可证缩写书写。

数据格式为：[许可证名称1，许可证名称2]。
示例：“fileLicense”: [“LGPL-2.0-only”]

5.4.2.6 文件许可证其他信息（Comments on File License）

本字段记录文件所采用的许可证相关的补充说明。

如果SBOM文档创建者对于文件所采取的许可证特定条款有补充或因为某些原因对文件采取有别于其他元素的许可证声明，可以在此处进行补充。

数据格式为：文本，或NONE，或NOASSERTION。具体要求如下：
——如果许可证中有特别需要注意的条款，可澄清特定许可证条款；
——如果文件的许可证与项目中其他部分的许可证有兼容性方面的考虑，可记录许可证兼容性信息；
——如果某个文件的许可证可能与整体项目的许可证冲突，可解释许可证冲突；
——NONE，如果 SBOM 文档创建者认为该文件没有需要补充说明的信息；
——NOASSERTION，如果 SBOM 文档创建者未提供任何信息。
示例：“fileLicComments”: “许可证继承自上游开源项目 GCC 的 GPL 许可证”

5.4.2.7 文件版权信息（File Copyright）

本字段记录文件的版权所有者，以及日期信息。
数据格式为：文本，或NONE，或NOASSERTION。具体要求如下：
——NONE，如果文件不包含任何版权信息；
——NOASSERTION，如果 SBOM 文档创建者未提供任何信息。
示例：“fileCopyright”: “版权所有 2008-2010 John Smith”

5.4.2.8 文件作者（File Author）

本字段记录文件的作者或主要贡献者相关信息。应详细说明作者的姓名、所属组织（若有）、联系邮箱（若有）以及在文件创建过程中的角色或主要贡献等。

数据格式为：
——“name: 姓名”；
——“organization: 组织名称”；
——“email: 电子邮箱地址”；
——“role: 角色或贡献”。

示例：
“fileAuthor”: [
{

```
    "name": "John Smith",
    "organization": "ABC Tech",
    "email": "john.smith@abctech.com",
    "role": "Lead Developer."
}
]
```

5.4.2.9 文件溯源信息（File URL）

本字段记录文件的可追溯信息。具体要求如下：

a) 如果通过URL直接溯源文件，应填写文件URL；

b) 如果通过VCS溯源文件，应填写文件所属项目地址、版本及其相对路径。

数据格式为：URL，或NONE，或NOASSERTION。具体要求如下。

——当通过 VCS 溯源文件时，URL 的具体格式为<repository_root_url>?version=<version>&path=<file_path>，要求如下：

- repository_root_url：文件所属仓库根路径的完整URL；
- version：当前文件内容所属的版本号，可以是仓库的 Tag 或 Commit ID；
- file_path：文件在所属仓库下的地址。

——NONE，如果不存在文件下载地址。

——NOASSERTION，如果 SBOM 文档创建者未提供任何信息。

示例1："fileUrl": "http://ftp.gnu.org/gnu/glibc"

示例2："fileUrl": "https://github.com/kubernetes/minikube.git?version=v1.33.1&path=/cmd/gvisor/gvisor.go"

示例3："fileUrl": "git@github.com:kubernetes/minikube.git?version=v1.33.1&path=/cmd/gvisor/gvisor.go"

5.4.2.10 文件哈希值（File Hash Value）

本字段记录用于校验文件完整性的信息，避免在引用特定文件的某个版本或修订时发生混淆。该字段的值应采用安全的摘要算法（如：SHA224、SHA256、SHA384、SHA512、SM3）对该文件的完整内容进行摘要计算，将算法和摘要值共同作为文件的哈希值。

数据格式为：

——algorithm: 算法标识符（如：SHA256）；

——value: 算法摘要值（小写十六进制数字）。

示例：

```
"fileHashValue": [
{
    "algorithm": "SHA256",
    "hashValue": "489cd5dbc708c7e541de4d7cd91ce6d0f1613573b7fc5b40d3942ccb9555cf35"
},
{
    "algorithm": "SHA224",
    "hashValue": "b6a5f4b3ecccf65022006bedfceae103b085bc378a76b8542af8be7"
}
]
```

5.4.2.11 文件其他信息（File Comments）

本字段记录对文件进行附加的说明解释或描述。

数据格式为：文本。

示例："fileComments": "no comments"

5.4.2.12 文件扩展信息（File Extended Information）

本字段记录在文件中未定义的、根据实际情况选择性扩充的文件信息。

数据格式为：使用对象的方式表达。

示例：

```
"fileExtInfo": {
```

```
    "fileSrcType": "Open SOURCE"
}
```

5.4.3 代码片段信息（Snippet Information）

5.4.3.1 概述

代码片段信息包括的字段见表5。

表5 代码段信息字段

字段名（全称）	中文名称	SBOM中使用的字段名	必要性
Snippet Identifier	代码片段标识符	snippetId	必选
Snippet Name	代码片段名称	snippetName	可选
Snippet from File Identifier	代码片段关联文件标识符	snippetFileId	必选
Snippet Source URL	代码片段来源信息	snippetSourceUrl	必选
Snippet Byte Range	代码片段字节范围	snippetByteRange	必选
Snippet Line Range	代码片段行范围	snippetLineRange	可选
Snippet License	代码片段许可证	snippetLicense	必选
Comments on Snippet License	代码片段许可证其他信息	snippetLicComments	可选
Snippet Copyright	代码片段版权信息	snippetCopyright	必选
AI Generated Snippet	人工智能生成代码片段	snippetAIGenerated	可选
Snippet Comments	代码片段其他信息	snippetComments	可选
Snippet Extended Information	代码片段扩展信息	snippetExtInfo	可选

5.4.3.2 代码片段标识符（Snippet Identifier）

本字段记录SBOM文档中可能被其他元素引用的代码片段，应确保每个代码片段标识符在SBOM文档内的唯一性。

数据格式为：SERef-snip-[idstring]，其中，[idstring]是唯一的字串，包含字母、数字、“.”、“-”。

示例：“snippetId”: “SERef-snip-01”

5.4.3.3 代码片段名称（Snippet Name）

本字段记录代码片段名称，以提供便捷的方式识别特定的代码片段。

数据格式为：文本。

示例：“snippetName”: “from Linux kernel”

5.4.3.4 代码片段关联文件标识符（Snippet from File Identifier）

本字段记录代码片段在本软件包内所关联源码文件的文件标识符。

数据格式为：SERef-file-[idstring]，其中，[idstring]是唯一的字串，包含字母、数字、“.”、“-”。

示例：“snippetFileId”: “SERef-file-01”

5.4.3.5 代码片段来源信息（Snippet Source URL）

本字段记录代码片段来源的URL地址。

数据格式为：URL。

示例：”snippetSourceUrl”: “https://logging.apache.org/log4j/2.x/”

5.4.3.6 代码片段字节范围（Snippet Byte Range）

本字段记录代码片段信息应用于关联源码文件中的字节范围。字节范围独立于各种格式，是指代差异最准确的方式。

数据格式为：number1:number2，其中，number1大于等于1，小于等于number2，且number2小于或等于文件的字节总数。

示例： “snippetByteRange”: “310:420”

5.4.3.7 代码片段行范围（Snippet Line Range）

本字段记录代码片段信息应用于关联源码文件中的行范围。对于有已知行分隔符的文件，行范围更容易参考。如果字节范围和行范围之间存在不一致，优先考虑字节范围值。

数据格式为：number1:number2，其中，number1大于等于1，小于等于number2，且number2小于或等于文件的总行数。

示例：“snippetLineRange”: “5:23”

5.4.3.8 代码片段许可证（Snippet License）

本字段记录SBOM文档创建者认为该代码片段所使用的许可证。若许可证表达式为ISO/IEC 5962标准中SPDX许可证列表所列许可证，则应按其许可证列表中许可证缩写书写。

数据格式为：[许可证名称1，许可证名称2]。

示例：“snippetLicense”: [“GPL-2.0-only”]

5.4.3.9 代码片段许可证其他信息（Comments on Snippet License）

本字段记录向SBOM文档的接收者提供许可证的详细解释。

数据格式为：文本，或NOASSERTION，其中，如果SBOM文档创建者未提供任何信息，则使用NOASSERTION。

示例：”snippetLicComments”: “The concluded license was taken from package xyz, from which the snippet was copied into the current file.
The concluded license information was found in the COPYING.txt file in package xyz.″

5.4.3.10 代码片段版权信息（Snippet Copyright）

本字段记录代码片段的版权所有者，以及任何出现的日期。

数据格式为：文本，或NONE，或NOASSERTION。具体要求如下：

——任何与版权声明相关的文本，无论完整与否；

——NONE，如果代码片段不包含任何版权信息；

——NOASSERTION，如果 SBOM 文档创建者未提供任何信息。

示例：“snippetCopyright”: “Copyright 2008-2010 John Smith”

5.4.3.11 人工智能生成代码片段（AI Generated Snippet）

本字段记录指定代码片段是否使用人工智能技术生成。

数据格式为：true，或false，或NOASSERTION。具体要求如下：

——true，表示指定代码片段使用人工智能技术生成；

——false，表示指定代码片段未使用人工智能技术生成；

——NOASSERTION，如果 SBOM 文档创建者未提供任何信息。

示例：“snippetAIGenerated”: true

5.4.3.12 代码片段其他信息（Snippet Comments）

本字段记录SBOM文档创建者提供代码片段注释的位置，以提供更多代码片段的详细信息。

数据格式为：文本。

示例：“snippetComments”: “This snippet was identified as significant and highlighted in this Apache-2.0 file, when a commercial scanner identified it as being derived from file fooin package xyz which is licensed under GPL-2.0.”

5.4.3.13 代码片段扩展信息（Snippet Extended Information）

本字段记录在代码片段中未定义的、根据实际情况选择性扩充的代码片段信息。

数据格式为：使用对象的方式表达。

示例：

```
“snippetExtInfo”: {
      “isReview”: true,
      “reviewComments”: “Not found security risks”
  }
```

5.4.4 关系（Relationships）

5.4.4.1 概述

关系包括的字段见表6。

表6 关系字段

字段名（全称）	中文名称	SBOM中使用的字段名	必要性
SBOM Element Identifier	SBOM元素标识符	sbomElementId	必选
Relationship Type	关系类型	relationshipType	必选
Related SBOM Element Identifier	相关SBOM元素标识符	relatedSbomElementId	必选

5.4.4.2 SBOM元素标识符（SBOM Element Identifier）

本字段记录存在关系的组件、文件或代码片段的标识符。

数据格式为：组件标识符，或文件标识符，或代码片段标识符。

示例：“sbomElementId”: “pkg:npm/myapp@1.0.0”

5.4.4.3 关系类型（Relationship Type）

本字段记录两个元素之间关系的信息。例如，可以表示组件、文件或代码片段之间的关系。

数据格式为：contains，或contained，或dependsOn，或dependencyOf，或generates，或generated，或variantOf，或copyOf，或dynamicLink，或staticLink，或other。

所支持的两个元素之间的关系如下：

——contains，contained，包含关系：一个元素包含了另一个元素；

——dependsOn，dependencyOf，依赖关系：一个元素依赖另一个元素；

——generates，generated，生成关系：一个元素是由另一个元素生成的；

——variantOf，copyOf，衍生关系：一个元素复制自另一个元素或从另一个元素修改而来；

——dynamicLink，staticLink，链接关系：两个元素通过动态/静态链接；

——other，其他关系。

示例：“relationshipType”: “dependsOn”

5.4.4.4 相关SBOM元素标识符（Related SBOM Element Identifier）

本字段记录与当前SBOM元素相关联的其他元素，应为组件、文件或代码片段部分中存在的标识符。

数据格式为：组件标识符，或文件标识符，或代码片段标识符。

示例：“relatedSbomElementId”: “pkg:npm/express@4.17.1”

5.5 环境信息（Environment Information）

5.5.1 构建环境信息（Build Environment Information）

5.5.1.1 概述

构建环境信息包括的字段见表7。

表7 构建环境信息字段

字段名（全称）	中文名称	SBOM中使用的字段名	必要性
Build Environment Architecture	构建环境CPU架构	buildArch	必选
Build Environment OS	构建环境操作系统	buildOS	必选
Build Environment Software Dependencies	构建环境第三方软件依赖	buildSoftDeps	可选
Build Time	构建时间	buildTime	可选
Build Pipeline Number	构建流水线号	buildPipeNo	可选
Build Tool	构建工具	buildTool	可选

5.5.1.2 构建环境CPU架构（Build Environment Architecture）

本字段记录软件构建环境所使用的CPU架构列表。

数据格式为：文本，其中，如果支持多种架构，则用“,”分割。

示例：“buildArch”: “amd64,arm64”

5.5.1.3 构建环境操作系统（Build Environment OS）

本字段记录软件构建环境使用的操作系统清单。
数据格式为：文本，其中，如果支持多种操作系统，则用“,”分割。
示例：“buildOS”: “XXX Linux Server V9.X SPX”

5.5.1.4 构建环境第三方软件依赖（Build Environment Software Dependencies）

本字段记录软件构建时所需的第三方软件列表。
数据格式为：文本。具体要求如下：
——每个第三方软件依赖采用{软件发起方标识}:{软件名称}:{软件版本}的格式进行标识；
——若包含多个第三方软件依赖时，用“,”分割；
——若是没有第三方软件依赖要求，则填NOBSDEP。
示例：“buildSoftDeps”: “gnu.org:gcc:9.1,git.io:git:2.39.3”

5.5.1.5 构建时间（Build Time）

本字段记录软件构建开始的时间，应按GB/T 7408.1-2023标准中规定的UTC格式的合并日期和时间指定。
数据格式为：YYYY-MM-DDThh:mm:ssZ。
示例：“buildTime”: “2023-03-29T18:30:22Z”

5.5.1.6 构建流水线号（Build Pipeline Number）

本字段记录软件构建当次流水线编号。
数据格式为：文本。
示例：“buildPipeNo”: “bulid-827”

5.5.1.7 构建工具（Build Tool）

本字段记录软件构建工具列表，包含每个工具的名称和版本号等基本信息。
数据格式为：[name]-[version]。具体要求如下：
——[name]表示工具的名称；
——[version]表示工具的版本；
——如果构建工具有多个，则用“,”分割。
示例：”buildTool”: “maven-3.6.5,npm-10.5.0”

5.5.2 运行环境信息（Runtime Environment Information）

5.5.2.1 概述

运行环境信息包括的字段见表8。

表8 运行环境信息字段

字段名（全称）	中文名称	SBOM中使用的字段名	必要性
Runtime Environment Architecture	运行环境CPU架构	runtimeArch	必选
Runtime Environment OS	运行环境操作系统	runtimeOS	必选
Runtime Environment Software Dependencies	运行环境第三方软件依赖	runtimeSoftDeps	可选
Runtime Environment Network Services Dependencies	运行环境网络服务依赖	runtimeNetServDeps	可选

5.5.2.2 运行环境 CPU 架构（Runtime Architecture）

本字段记录提供软件运行时可支持的CPU架构范围。
数据格式为：文本。具体要求如下：
——若支持多种架构时，用“,”分割；

——若是没有 CPU 架构要求，则填 NOARCH。

示例：“runtimeArch”: “amd64,arm64”

5.5.2.3 运行环境操作系统（Runtime OS）

本字段记录提供软件运行时可支持的操作系统清单。

数据格式为：文本。具体要求如下：

——若支持多种操作系统时，用“,”分割；

——若是没有操作系统要求，则填NOOS。

示例：“runtimeOS”: “XXX Linux Server V9.X SPX”

5.5.2.4 运行环境第三方软件依赖（Runtime Software Dependencies）

本字段记录提供软件运行时所依赖的的第三方软件列表。

数据格式为：文本。具体要求如下：

——每个第三方软件依赖采用{软件发起方标识}:{软件名称}:{软件版本}的格式进行标识；

——若包含多个第三方软件依赖时，用“,”分割；

——若是没有第三方软件依赖要求，则填NORSDEP。

示例：“runtimeSoftDeps”: “gnu.org:gcc:9.1,git.io:git:2.39.3”

5.5.2.5 运行环境网络服务依赖（Runtime Network Services Dependencies）

本字段记录提供软件运行时所依赖的网络服务或网络API接口列表。

数据格式为：键值对组合的列表。具体要求如下：

——网络服务标识（id），数据格式为SBOM文档内唯一的网络服务标识文本；

——网络服务名称（name），数据格式为文本；

——网络服务供应商（vendor），数据格式为文本；

——网络服务必要性（necessity），数据格式为true 或 false；

——网络服务协议类型（protocol），数据格式为文本；

——网络服务地址（address），数据格式为文本。

示例：

```
“runtimeNetServDeps”: [
    {
        “id”: “ocr-service”,
        “name”: “发票识别服务”,
        “vendor”: “Example”,
        “necessity”: true,
        “protocol”: “HTTPS”,
        “address”: “https://api.example.com/ocr”
    }
]
```

5.6 扩展信息（Extended Information）

扩展信息包括的字段见表9。

表9 扩展信息字段

字段名（全称）	中文名称	SBOM中使用的字段名	必要性
Extended Information	扩展信息	extendedInfo	必选

本字段记录在本文件中未定义的、根据实际情况选择性扩充的SBOM信息。

数据格式为：使用对象的方式表达。

示例：

```
“extendedInfo”: {
    “patches”: {
        “name”: “Function Update”,
        “updateTime”: “2024-07-28T02:21:09+08:00”
    },
```

```
        “database”: “MySQL-8.0.35”
    }
```

附 录 A
（资料性）
软件物料清单字段说明

A.1 SBOM 文档根元素

字段	类型	描述	备注
documentBasicInfo	object	文档基本信息	
softwareCompositionInfo	object	软件组成信息，包含组件、文件、代码片段及相互之间关系	
environmentInfo	object	环境信息，包含构建环境与运行环境信息	
extendedInfo	object	扩展信息	

A.1.1 documentBasicInfo的元素（文档基本信息）

字段	类型	描述	备注
sbomFormat	string	文档使用的数据格式	
documentLicense	string	文档许可证	
documentName	string	文档名称	
documentVersion	string	文档版本	
documentNamespace	string	文档命名空间	
toolInfo	string	工具信息	
sbomAuthor	string	创建者信息	
timestamp	string	文档时间戳	
sbomAuthorComments	string	创建者备注	
sbomComments	string	文档其他信息	

A.1.2 softwareCompositionInfo的元素（软件组成信息）

字段	类型	描述	备注
components	array<object>	组件信息	
files	array<object>	文件信息	
snippets	array<object>	代码片段信息	
relationships	array<object>	关系	

A.1.2.1 components 的元素（组件信息）

字段名	类型	描述	备注
componentId	string	组件标识符	
componentName	string	组件名称	
componentVersion	string	组件版本	
componentAuthor	array<object>	组件作者	
componentProvider	object	组件供应商	
componentHome	string	组件主页	
componentDownload	string	组件下载位置	
license	array<string>	组件许可证	
componentLicComments	string	组件许可证其他信息	
componentCopyright	string	组件版权信息	
componentHashValue	array<object>	组件哈希值	
componentTimestamp	string	组件时间戳	
componentPlatform	string	组件平台架构	
componentAIFunction	string	人工智能功能	枚举，取值范围：true，false，NOASSERTION
componentComments	string	组件其他信息	
componentExtInfo	object	组件扩展信息	

A.1.2.1.1 componentAuthor 的元素（组件作者）

字段名	类型	描述	备注
name	string	姓名	
organization	string	组织名称	
email	string	电子邮箱地址	
role	string	角色或贡献	

A.1.2.1.2 componentProvider 的元素（组件供应商）

字段名	类型	描述	备注
fullName	string	公司全称	
shortName	string	公司缩写	
webSite	string	公司网站	
contactNumber	string	联系电话	
email	string	电子邮箱	
description	string	公司简介	

A.1.2.1.3 componentHashValue 的元素（组件哈希值）

字段	类型	描述	备注
algorithm	string	算法标识符	枚举，取值范围： SM3、SHA1、BLAKE3、SHA3-384、SHA256、SHA384、BLAKE2b-512、BLAKE2b-256、SHA3-512、MD2、ADLER32、MD4、SHA3-256、BLAKE2b-384、SHA512、MD6、MD5、SHA224等
hashValue	string	算法摘要值	

A.1.2.1.4 componentExtInfo 的元素（组件扩展信息）

字段	类型	描述	备注
/	object、array、string等	需要扩展的组件相关信息	在componentExtInfo下可根据需要，任意新增定义元素，同时补充相关字段与值

A.1.2.2 files 的元素（文件信息）

字段名	类型	描述	备注
fileId	string	文件标识符	
fileName	string	文件名	
fileType	array<string>	文件类型	枚举，取值范围： SOURCE，BINARY，TEXT，IMAGE，AUDIO，VIDEO，APPLICATION，ML_MODEL，SBOM，OTHER
fileLicense	array<string>	文件许可证	
fileLicComments	string	文件许可证其他信息	
fileCopyright	string	文件版权信息	
fileAuthor	array<object>	文件作者	
fileUrl	string	文件溯源信息	
fileHashValue	array<object>	文件哈希值	
fileComments	string	文件其他信息	
fileExtInfo	object	文件扩展信息	

A.1.2.2.1 fileAuthor 的元素（文件作者）

字段名	类型	描述	备注
name	string	姓名	
organization	string	组织名称	

字段名	类型	描述	备注
email	string	电子邮箱地址	
role	string	角色或贡献	

A.1.2.2.2 fileHashValue 的元素（文件哈希值）

字段	类型	描述	备注
algorithm	string	算法标识符	枚举，取值范围： SM3、SHA1、BLAKE3、SHA3-384、SHA256、SHA384、BLAKE2b-512、BLAKE2b-256、SHA3-512、MD2、ADLER32、MD4、SHA3-256、BLAKE2b-384、SHA512、MD6、MD5、SHA224等
hashValue	string	算法摘要值	

A.1.2.2.3 fileExtInfo 的元素（文件扩展信息）

字段	类型	描述	备注
/	object、array、string等	需要扩展的文件相关信息	在fileExtInfo下可根据需要，任意新增定义元素，同时补充相关字段与值

A.1.2.3 snippets 的元素（代码片段信息）

字段名	类型	描述	备注
snippetId	string	代码片段标识符	
snippetName	string	代码片段名称	
snippetFileId	string	代码片段关联文件标识符	
snippetSourceUrl	string	代码片段来源信息	
snippetByteRange	string	代码片段字节范围	
snippetLineRange	string	代码片段行范围	
snippetLicense	array<string>	代码片段许可证	
snippetLicComments	string	代码片段许可证其他信息	
snippetCopyright	string	代码片段版权信息	
snippetAIGenerated	string	人工智能生成代码片段	枚举，取值范围： true，false，NOASSERTION
snippetComments	string	代码片段其他信息	
snippetExtInfo	object	代码片段扩展信息	

A.1.2.3.1 snippetExtInfo 的元素（代码片段扩展信息）

字段	类型	描述	备注
/	object、array、string等	需要扩展的代码片段相关信息	在snippetExtInfo下可根据需要，任意新增定义元素，同时补充相关字段与值

A.1.2.4 relationships 的元素（关系）

字段名	类型	描述	备注
sbomElementId	string	SBOM元素标识符	
relationshipType	string	关系类型	枚举，取值范围： contains，contained，dependsOn，dependencyOf，generates，generated，variantOf，copyOf，dynamicLink，staticLink，other
relatedSbomElementId	string	相关SBOM元素标识符	

A.1.3 environmentInfo的元素（环境信息）

字段名	类型	描述	备注
buildInfo	object	构建环境信息	
runtimeInfo	object	运行环境信息	

A.1.3.1 buildInfo 的元素（构建环境信息）

字段名	类型	描述	备注
buildArch	string	构建环境CPU架构	
buildOS	string	构建环境操作系统	
buildSoftDeps	string	构建环境第三方软件依赖	
buildTime	string	构建时间	
buildPipeNo	string	构建流水线号	
buildTool	string	构建工具	

A.1.3.2 runtimeInfo 的元素（运行环境信息）

字段名	类型	描述	备注
runtimeArch	string	运行环境CPU架构	
runtimeOS	string	运行环境操作系统	
runtimeSoftDeps	string	运行环境第三方软件依赖	
runtimeNetServDeps	array<object>	运行环境网络服务依赖	

A.1.3.2.1 runtimeNetServDeps 的元素（运行环境网络服务依赖）

字段名	类型	描述	备注
id	string	网络服务标识	
name	string	网络服务名称	
vendor	string	网络服务供应商	
necessity	string	网络服务必要性	枚举，取值范围：true，false
protocol	string	网络服务协议类型	
address	string	网络服务地址	

A.1.4 extendedInfo的元素（扩展信息）

字段名	类型	描述	备注
/	object、array、string等	需要扩展的其他SBOM相关信息	在extendedInfo下可根据需要，任意新增定义元素，同时补充相关字段与值

附 录 B
（资料性）
软件物料清单示例参考

B.1 文档基本信息

JSON格式示例：

```
{
    "documentBasicInfo": {
        "sbomFormat": "BOM-SW-v2.0",
        "documentLicense": "CC0-1.0",
        "documentName": "glibc-v2.3",
        "documentVersion": "2.1.1",
        "documentNamespace": "http://license.coscl.org.cn/XXX-SBOM",
        "toolInfo": "ABC-XCheck-v1.0",
        "sbomAuthor": "Jane Doe",
        "timestamp": "2023-03-29T18:30:22+08:00",
        "sbomAuthorComments": "文档审核状态：内部已复核。",
        "sbomComments": "no remarks"
    }
}
```

B.2 组件信息

JSON格式示例：

```
{
    "components": [
        {
            "componentId": "pkg:deb/debian/xxx?arch=i386&distro=XXX",
            "componentName": "glibc",
            "componentVersion": "2.15",
            "componentAuthor": [
                {
                    "name": "张三",
                    "organization": "ABC公司",
                    "email": "john.smith@abctech.com",
                    "role": "测试。张三对软件组件进行了广泛的测试，并识别和报告错误。
"
                },
                {
                    "name": "李四",
                    "organization": "XYZ公司",
                    "email": "mary.johnson@xyztech.com",
                    "role": "贡献者。李四为该组件的UI设计和用户体验增强做出了贡献，提
高了整体可用性。"
                }
            ],
            "componentProvider": {
                "fullName": "ABC公司",
```

```
                "shortName": "ABC",
                "webSite": "https://www.abc.com",
                "contactNumber": "+1-425-882-8888",
                "email": "support@abc.com",
                "description": "ABC公司是一家全球领先的技术公司，提供广泛的软件组件和
服务。"
            },
            "componentHome": "http://ftp.xxx.org/gnu/glibc",
            "componentDownload": "http://ftp.xxx.org/gnu/glibc/glibc-ports-2.15.tar.g
z",
            "license": ["LGPL-2.0-only"],
            "componentLicComments": "This license was released: June 1991. This licen
se has been superseded by LGPL-2.1. This license identifier refers to the choice to use t
he code under LGPL-2.0-only, as distinguished from use of code under LGPL-2.0-or-later
(i.e., LGPL-2.0 or some later version). The license notice (as seen in the Standard Licen
se Header field below) states which of these applies to the code in the file. The example
 in the exhibit to the license shows the license notice for the or later approach.",
            "componentCopyright": "Copyright 2008-2010 John Smith",
            "componentHashValue": [
                {
                    "algorithm": "SHA256",
                    "hashValue": "60fd2bc1c230c958706ee28bbdf37a94d6ceef8ac79dfe82a42
464401ce75381"
                },
                {
                    "algorithm": "SM3",
                    "hashValue": "66C7F0F462EEEDD9D1F2D46BDC10E4E24167C4875CF2F7A2297
DA02B8F4BA8E0"
                }
            ],
            "componentTimestamp": "2023-03-29T18:30:22+08:00",
            "componentPlatform": "linux/amd64,linux/arm64,darwin/arm64",
            "componentAIFunction": false,
            "componentComments": "no remarks",
            "componentExtInfo": {
                "vulCveId": "CVE-20XX-XXXXX",
                "vulCveComments": "该漏洞可能会引起XXXX问题"
            }
        },
        {
            "componentId": "pkg:maven/org.xxx.logging.log4j/log4j-api@2.24.3?type=jar
",
            "componentName": "Log4j",
            "componentVersion": "2.24.3",
            "componentAuthor": [
                {
                    "name": "Li Lei",
                    "organization": "The XXX Software Foundation",
                    "email": "lilei@xxx.org",
```

```
                "role": "开发人员。"
            }
        ],
        "componentProvider": {
            "fullName": "XYZ公司",
            "shortName": "XYZ",
            "webSite": "https://www.xyz.com",
            "contactNumber": "+1-425-882-6666",
            "email": "support@xyz.com",
            "description": "XYZ公司是一家全球领先的技术公司，提供广泛的软件组件和
服务。"
        },
        "componentHome": "https://logging.xxx.org/log4j/2.x/",
        "componentDownload": "https://repository.xxx.org/service/local/staging/de
ploy/maven2",
        "license": ["Apache-2.0"],
        "componentLicComments": "NOASSERTION",
        "componentCopyright": "NOASSERTION",
        "componentHashValue": [
            {
                "algorithm": "SHA256",
                "hashValue": "18fd1bbc0207603d84f9cd6434b477baa88d8636459c18520b2
488a79249fe68"
            }
        ],
        "componentTimestamp": "2023-03-29T18:30:22+08:00",
        "componentPlatform": "windows/x86",
        "componentAIFunction": false,
        "componentComments": "no remarks"
    }
  ]
}
```


B.3 文件信息

JSON格式示例：


```
{
  "files": [
    {
        "fileId": "SERef-file1",
        "fileName": "./package/foo.c",
        "fileType": ["SOURCE"],
        "fileLicense": ["LGPL-2.0-only"],
        "fileLicComments": "许可证继承自上游开源项目 GCC 的 GPL 许可证",
        "fileCopyright": "版权所有 2008-2010 John Smit",
        "fileAuthor": [
            {
                "name": "John Smith",
                "organization": "ABC Tech",
                "email": "john.smith@abctech.com",
```

```
                "role": "Lead Developer."
            }
        ],
        "fileUrl": "https://abc.com/xxx/minik,ube.git?version=v1.33.1&path=/cmd/gvisor/1.go",
        "fileHashValue": [
            {
                "algorithm": "SHA256",
                "hashValue": "489cd5dbc708c7e541de4d7cd91ce6d0f1613573b7fc5b40d3942ccb9555cf35"
            },
            {
                "algorithm": "SHA224",
                "hashValue": "b6a5f4b3ecccf65022006bedfceae103b085bc378a76b8542af8be7"
            }
        ],
        "fileComments": "no remarks"
        "fileExtInfo": {
            "fileSrcType": "Open SOURCE"
        }
    },
    {
        "fileId": "SERef-file2",
        "fileName": "./package/foo.c",
        "fileType": ["SOURCE", "TEXT"],
        "fileLicense": ["LGPL-2.0-only"],
        "fileLicComments": "许可证继承自上游开源项目 GCC 的 GPL 许可证",
        "fileCopyright": "版权所有 2008-2010 John Smith",
        "fileAuthor": [
            {
                "name": "John Smith",
                "organization": "ABC Tech",
                "email": "john.smith@abctech.com",
                "role": "Lead Developer."
            }
        ],
        "fileUrl": "https://abc.com/xxx/minik,ube.git?version=v1.33.1&path=/cmd/gvisor/2.go",
        "fileHashValue": [
            {
                "algorithm": "SHA256",
                "hashValue": "77e6f78af45f649c5f3b8ebe484a91a144eb203a34a89c8dc5b1c4ca87bc6f71"
            }
        ],
        "fileComments": "no remarks"
    }
]
```

```
}
```

B.4 代码片段信息

JSON格式示例：

```
{
    "snippets": [
        {
            "snippetId": "SERef-snip1",
            "snippetName": "from log4j",
            "snippetFileId": "SERef-file1",
            "snippetSourceUrl": "https://logging.xxx.org/log4j/2.x/",
            "snippetByteRange": "310:420",
            "snippetLineRange": "5:23",
            "snippetLicense": ["Apache-2.0"],
            "snippetLicComments": "no remarks",
            "snippetCopyright": "Copyright 2008-2010 John Smith",
            "snippetAIGenerated": true,
            "snippetComments": "no remarks",
            "snippetExtInfo": {
                "isReview": true,
                "reviewComments": "Not found security risks"
            }
        },
        {
            "snippetId": "SERef-snip2",
            "snippetName": "from Apache Tomcat",
            "snippetFileId": "SERef-file1",
            "snippetSourceUrl": "https://tomcat.xxx.org/",
            "snippetByteRange": "310:420",
            "snippetLineRange": "5:23",
            "snippetLicense": ["Apache-2.0"],
            "snippetLicComments": "no remarks",
            "snippetCopyright": "Copyright 2008-2010 John Smith",
            "snippetAIGenerated": true,
            "snippetComments": "no remarks"
        }
    ]
}
```

B.5 关系

JSON格式示例：

```
{
    "relationships": [
        {
            "sbomElementId": "pkg:npm/myapp@1.0.0",
            "relationshipType": "dependsOn",
            "relatedSbomElementId": "pkg:npm/express@4.17.1"
        },
        {
```

```
            "sbomElementId": "pkg:npm/myapp@1.0.0",
            "relationshipType": "dependsOn",
            "relatedSbomElementId": "pkg:npm/redis@4.0.0"
        }
    ]
}
```

B.6 构建环境信息

JSON格式示例：

```
{
    "buildInfo": {
        "buildArch": "amd64,arm64",
        "buildOS": "XXX Linux Server V9.X SPX",
        "buildSoftDeps": "gnu.org:gcc:9.1,git.io:git:2.39.3",
        "buildTime": "2023-03-29T18:30:22Z",
        "buildPipeNo": "bulid-827",
        "buildTool": "maven-3.6.5"
    }
}
```

B.7 运行环境信息

JSON格式示例：

```
{
    "runInfo":{
        "runtimeArch": "amd64,arm64",
        "runtimeOS": "XXX Linux Server V9.X SPX",
        "runtimeSoftDeps": "gnu.org:gcc:9.1,git.io:git:2.39.3",
        "runtimeNetServDeps": [
            {
                "id": "ocr-service",
                "name": "发票识别服务",
                "vendor": "Example",
                "necessity": true,
                "protocol": "HTTPS",
                "address": "https://api.example.com/ocr"
            },
            {
                "id": "llm-service",
                "name": "大模型服务"
                "vendor": "Example"
                "necessity": false
                "protocol": "WebSocket"
                "address": "wss://api.example.com/llm"
            }
        ]
    }
}
```

B.8 扩展信息

JSON格式示例：

```
{
    "extendedInfo":
    {
        "patches": {
            "name": "Function Update",
            "updateTime": "2024-07-28T02:21:09+08:00"
        },
        "database": "MySQL-8.0.35"
    }
}
```

参 考 文 献

[1] GB/T 43698-2024 网络安全技术 软件供应链安全要求