ICS 35.080
CCS L70

团　体　标　准

CQAE*****—2025

软件物料清单构成和要求

Composition and Requirements for Software Bill of Materials

（报批稿）

202X- XX-XX 发布　　202X- XX-XX 实施

中国电子质量管理协会　发布

目　次

前言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 2
5 总体要求 2
5.1 概述 2
5.2 主要构成 2
6 文档信息数据字段 3
6.1 文档名称 3
6.2 文档版本 3
6.3 文档时间戳 4
6.4 数据格式 4
6.5 工具信息 4
6.6 创建者信息 4
6.7 创建者备注 4
6.8 文档备注 5
7 基本数据字段 5
7.1 作者名称 5
7.2 供应商名称 5
7.3 组件名称 6
7.4 组件版本 6
7.5 组件哈希值 6
7.6 唯一标识符 7
7.7 许可证 7
7.8 依赖关系 7
7.9 时间戳 8
8 可选数据字段 8
8.1 SBOM 类型 8
8.2 与其它组件关系 9
8.3 组件安全信息 10
8.4 组件来源信息 11
8.5 组件版权信息 11
8.6 补丁信息 11
8.7 组件描述 12
8.8 文件信息 12
9 支持工具要求 14
9.1 能力要求 14

9.2 能力类型 14
9.3 格式支持 15
9.4 生成深度 15
9.5 兼容性 15
9.6 易用性 16
10 管理和应用要求 16
10.1 概述 16
10.2 覆盖范围 16
10.3 更新和版本管理 17
10.4 SBOM 采用类型 17
10.5 声明未详尽信息 17
10.6 分发和交付 17
10.7 维护和监控 17
10.8 与其他关键信息系统的互操作性 17
10.9 访问控制 17
10.10 完整真实 18
10.11 其他 18
附录 A （规范性） DP-SBOM 格式参考 19
A.1 概述 19
A.2 兼容性 19
A.3 JSON 数据模型 19
附录 B （资料性） DP-SBOM 与 SPDX、CycloneDX 的对比 31
参考文献 33

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。

本文件由国家工业信息安全发展研究中心提出。

本文件由中国电子质量管理协会归口。

本文件起草单位：国家工业信息安全发展研究中心、中国电子技术标准化研究院、华为技术有限公司、北京大学、南京大学、中国科学院软件所、中科南京软件技术研究院、海通证券股份有限公司、中国建设银行股份有限公司、中移动信息技术有限公司、北京中电飞华通信有限公司、东吴证券股份有限公司、北京中标服检验技术研究院有限公司、北京数企云服信息技术有限公司、北京安普诺信息技术有限公司、苏州棱镜七彩信息科技有限公司、上海安势信息技术有限公司、北京交通大学、中国海洋石油集团有限公司、中海油信息科技有限公司北京分公司、中移（苏州）软件技术有限公司

本文件主要起草人：周峻松、徐亮、邓昌义、冯璐铭、李郁佳、刘泊言、于昕、柯猛、周明辉、贾昌国、张天、李重、魏怡琳、崔星、刘斌、高卉、王东、马冰、钟志军、邓夏阳、杨达、刘斌、刘迪、许放、唐淑艳、马骏俊、张涛、宁戈、梁大功、黄浩东、高琨、张超杰、陶耀东、张百川、梁峰、邢献红、温章义、胡蝶、谢晓辉、李志刚、刘晨昱、苑舒斌、晏菲、胡宗棠、戴正元

软件物料清单构成和要求

1 范围

本文件确立了软件物料清单构成的总体要求，规定了文档信息数据字段、基本数据字段、可选数据字段、支持工具要求和管理应用要求。

本文件适用于软件供应链管理的全生存周期，包括开发、采购、运维等环节。也可用于SBOM生成、转换、验证和管理需求的其他场景。

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构成本文件的必不可少条款。其中，注日期的引用文件，仅该日期的版本适用于本文件；未注日期的引用文件，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

3 术语和定义

下列术语和定义适用于本文件。

3.1

物料清单 bill of materials;BOM

描述产品所需零部件明细及其结构的技术文件。

[来源：GB/T 25109.1-2010，4.3.5]

3.2

软件物料清单 software bill of materials;SBOM

一种正式的、结构化的、机器和人可读的数据记录，用于唯一标识构成软件的具体成分，详细记录软件产品的组成要素，并描述组成要素之间的关系。

注：构成软件的具体成分可以是软件包、组件、文件、代码片段等中的一种或多种。

3.3

开源软件 open source software

一种可以获取源代码的计算机软件。

注：软件的著作权持有人通过开源许可证将软件的复制、修改、再发布的权利向公众开放。

[来源：GB/T 42927-2023，3.1]

3.4

开源许可证 open source license

用于规范受著作权保护的软件在规定条款、条件下被使用或分发等行为的许可证。

注：一般指具备广泛认可性的、具有法律性质的协议，也称开源协议，目的是减少作者及用户针对开源软件权责的法律解释成本。常见开源许可证有通用公共许可证（GNU General Pubic License, GPL）、Mozilla公共许可证（Mozilla Public License, MPL）、BSD许可证（Berkeley Software Distribution license, BSD License）等。

[来源：GB/T 42927-2023，3.2]

4 缩略语

下列缩略语适用于本文件。

CD 持续交付（Continuous Delivery）
CI 持续集成（Continuous Integration）
CPE 通用平台枚举（Common Platform Enumeration）
DP 数字产品（Digital Product）
JSON JavaScript对象表示法（JavaScript Object Notation）
PURL 包统一资源定位器（Package Uniform Resource Locator）
SBOM 软件材料清单（Software Bill of Materials）
SIEM 安全信息和事件管理（Security Information and Event Management）
SOC 安全运营中心（Security Operations Center）
SPDX 软件包数据交换（Software Package Data Exchange）
SWID 软件标识（Software Identification）
TIP 威胁情报平台（Threat Image Projection）
URL 统一资源定位器（Uniform Resource Locator）
URN 统一资源名称（Uniform Resource Name）
UUID 通用唯一识别码（Universally Unique Identifier）

5 总体要求

5.1 概述

SBOM的所有数据应基于JSON格式构建。SBOM通过明确识别和详细记录软件组件及其相互关系、安全性、版权和许可证等成分数据，实现对组成成分的追踪溯源，提前防御风险。在软件产品受到安全威胁时，SBOM使用者应快速定位受影响的组件并及时进行补救，提高安全与合规事件响应速度。

5.2 主要构成

本文件由SBOM文档信息数据字段、基本数据字段、可选数据字段、支持工具要求、管理和应用要求构成。其中：

a）文档信息数据字段包括文档名称、文档版本、文档时间戳、数据格式、工具信息、创建者信息、创建者备注和文档备注；

b）基本数据字段包括作者名称、供应商名称、组件名称、组件版本、组件哈希值、唯一标识符、许可证、时间戳和依赖关系；

c）可选数据字段包括SBOM类型、与其他组件关系、组件安全信息、组件来源信息、组件版权信息、补丁信息、组件描述、文件信息；

d）支持工具要求包括能力类型、格式支持、生成深度、易用性和兼容性；

e）管理和应用要求包括覆盖范围、更新和版本管理、SBOM采用类型、声明未详尽信息、分发和交付、维护和监控、与其他信息系统互操作性、访问控制、完整真实和其他。

各部分之间的构成和关系见图1。

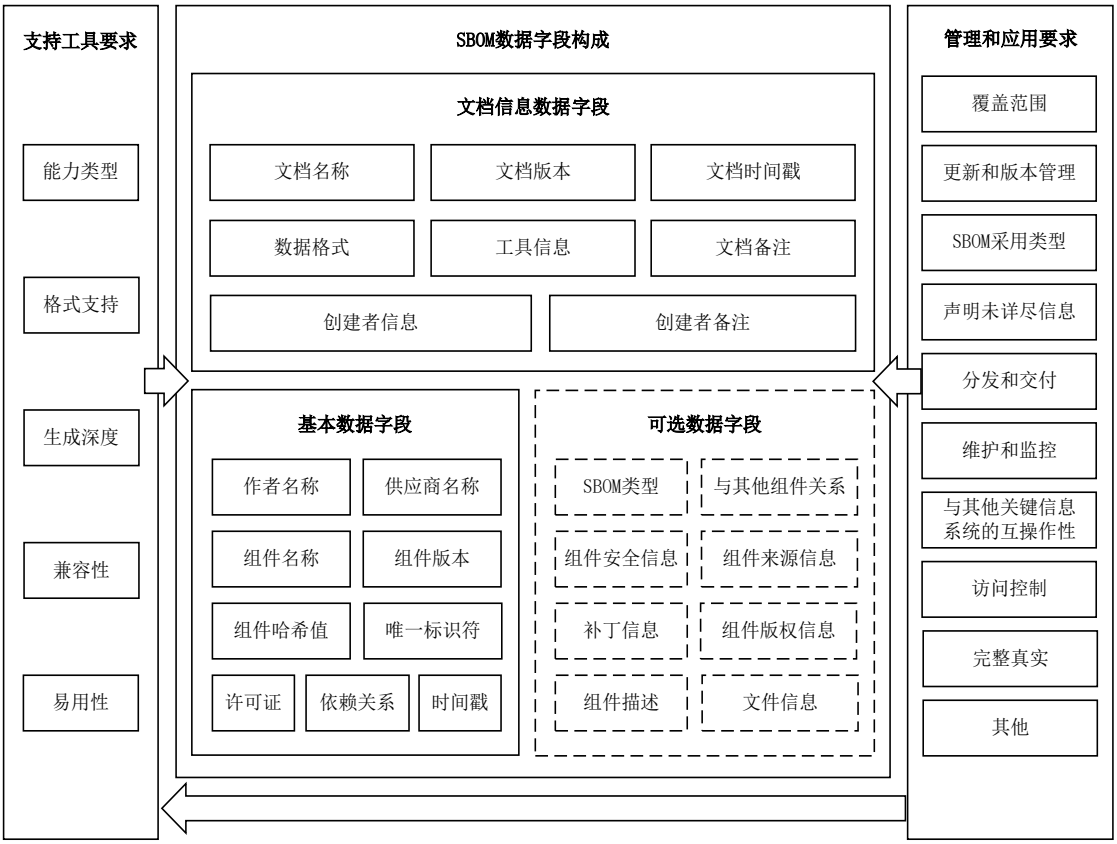

图1　软件物料清单构成要素及关系

本文件的第5章至第9章分别详细规定了SBOM各组成要素的要求。为了便于理解和使用本文件规定的SBOM格式，附录A给出了JSON格式的SBOM数据模型。

6　文档信息数据字段

6.1　文档名称

SBOM文档应具有唯一名称，包含软件名称及版本。

是否必须：是

字段名称：documentName

数据类型：字符串

数据格式：单行文本

示例：documentName: glibc-v2.3

6.2　文档版本

每次更新、删除、修改或重新生成SBOM文档时，均应记录版本信息。

是否必须：是

字段名称：documentVersion
数据类型：字符串
数据格式：M.N.P，其中，M是主要版本号，N是次要版本号，P是修订号。
示例："documentVersion": "2.2.1"

6.3 文档时间戳

首次创建SBOM文档及每次更新时，均应记录时间戳。时间戳应符合《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》标准格式。
是否必须：是
字段名称：timestamp
数据类型：字符串
数据格式：YYYY-MM-DDTHH:mm:ssTZD
示例："timestamp": "2024-11-20T00:00:01TZD"

6.4 数据格式

SBOM文档应明确使用的数据格式，包括格式名称和版本号。
是否必须：是
字段名称：bomFormat
数据类型：字符串
数据格式：DP-SBOM-格式版本
示例："bomFormat": "DP-SBOM-1.0"

6.5 工具信息

应记录生成SBOM文档的工具信息，包括厂商名称、工具名称和工具版本等。
是否必须：是
字段名称：tool
数据类型：字符串
数据格式：厂商－工具名称－版本
示例："tool": "ABC-XCheck-1.0"

6.6 创建者信息

指定创建此文档的工具、个人或组织。
是否必须：是
字段名称：bomAuthor
数据类型：字符串
数据格式：单行文本
示例："bomAuthor": "xtool"

6.7 创建者备注

用于记录关于此文档的创建者的附加说明。
是否必须：是
字段名称：bomAuthorComment

数据类型：字符串
数据格式：单行文本
示例："bomAuthorComment":"文档审核状态：内部已复核。"

6.8 文档备注

用于记录关于此文档的附加说明。
是否必须：是
字段名称：bomComment
数据类型：字符串
数据格式：单行文本
示例："bomComment":"新增xx组件许可证分析模块。"

7 基本数据字段

7.1 作者名称

用于明确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。
是否必须：是
字段名称：componentAuthor
数据类型：字典列表
数据格式：[{"name":姓名,"organization":公司名称,"email":电子邮箱地址,"role":角色或贡献}]
示例 1："componentAuthor":[{"name":"张三","organization":"ABC公司", "email":"john.smith@abctech.com","role":"首席开发人员,负责软件组件的总体架构和主要功能实现。"}
示例 2："componentAuthor":{"name":"张三","Email":"mary.johnson@gmail.com","role":"贡献者,张三为该组件的UI设计和用户体验增强做出了贡献,提供了宝贵的见解和设计理念,提高了整体可用性。"}]
示例 3："componentAuthor":[{"name":"张三","organization":"XYZ公司","role":"测试.张三对软件组件进行了广泛的测试，确保其质量，并识别和报告错误。他细致的测试工作有助于提高组件的稳定性和可靠性。"}]
示例4："componentAuthor":[{"name":"张三","email":"zs@cic.cn"},{"name":"李四","email":"ls@cic.cn"}]

7.2 供应商名称

用于标识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。
是否必须：是
字段名称：componentProvider
数据类型：字典

数据格式：{"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 1："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，它是操作系统、生产力软件和云计算市场的主要参与者."}

示例 2："componentProvider":{"fullName":"ACD公司","shortName":"ACD","webSite":"https://www.acd.com","contactNumber":"+1-650-506-7777","email":"info@acd.com","description":"ACD公司以其数据库管理系统和企业软件解决方案而闻名。它提供了广泛用于企业级应用程序和数据管理的软件组件."}

示例 3："componentProvider":{"fullName":"AFD公司","shortName":"AFD","webSite":"https://www.afd.com","contactNumber":"+1-888-733-4321","email":"support@afd.com","description":"AFD公司是一家著名的开源软件公司。它提供各种软件组件，特别是在Linux操作系统和中间件领域，并为其产品提供企业支持和服务."}

7.3 组件名称

标识组件发起方提供的组件的全名，应使用原始供应商定义的组件完整名称。组件名称应具备处理多个名称或别名的功能。组件名称可以包含供应商名称。

是否必须：是

字段名称：componentName

数据类型：字符串

数据格式：单行文本

示例 1："componentName":"glibc"

示例 2："componentName":"log4j-src"

7.4 组件版本

标识组件的版本，应至少包含主版本号与次版本号。应标明供应商使用的用于指定较之前版本软件变更的标识符，用于标识组件版本信息。若组件初次创建时无版本信息，应为其创建一个版本号。

是否必须：是

字段名称：componentVersion

数据类型：字符串

数据格式：M.N.P，其中，M是主要版本号，N是次要版本号，P是修订号。

示例："componentVersion":"2.11.1"

7.5 组件哈希值

组件的哈希值应作为其固有标识符，哈希值生成算法应明确，可以为一个组件或多个组件的集合提供多个哈希值。

是否必须：是

字段名称：componentChecksums

数据类型：字符串

数据格式：由哈希算法名称（如 SHA-256）和对应的哈希值（十六进制字符串）组成，格式为{"componentChecksums": 算法名称:哈希值}

示例 1："componentChecksums":" SHA-256:3a7bd3e2360a3d29eea436fcfb7e44c716e7f537ab8ee5"

示例 2："componentChecksums": "SHA-384:56e410b092b40811b353b1b13c26149799466007105 33"

示例 3："componentChecksums": "SHA-512:7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677"

7.6 唯一标识符

应标明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。

是否必须：是

字段名称：componentId

数据类型：字符串

数据格式：单行文本

示例："componentId": "pkg:deb/debian/curl@7.50.3-1?arch=i386"

7.7 许可证

应标明组件或文件的许可证信息，标识该组件或文件所使用的开源许可证或商业许可证。

是否必须：是

字段名称：license

数据类型：数组

数据格式：[许可证名称1，许可证名称2]

示例："license":["Apache-2.0"]

7.8 依赖关系

应清晰描述组件之间的依赖关系，标明软件中包含上游组件的情况。

是否必须：是

字段名称：dependencies

数据类型：字典

数据格式：dependencies:[

```
    {
        "ref": "唯一标识符",
        "dependsOn":[
            {
                    "target": "该组件的直接依赖组件的唯一标识符"
             },
            {
                    "target": "其他直接依赖的唯一标识符"
            }
        ]
```

```
    },
    { 其他组件的依赖关系 }
]
示例："dependencies":[
            {
                    "ref": "pkg:pkg:npm/myapp@1.0.0",
                    "dependsOn": [
                        {"target": "pkg:npm/express@4.17.1"},
                        {"target": "pkg:npm/redis@4.0.0"}
                    ]
            }
    ]
```

7.9 时间戳

应记录组件SBOM数据生成或更新的时间戳。时间戳应符合《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》标准格式。

是否必须：是

字段名称：componentTimestamp

数据类型：字符串

数据格式：YYYY-MM-DDTHH:mm:ssTZD

示例："componentTimestamp": "2024-11-20T00:00:01TZD"

8 可选数据字段

8.1 SBOM 类型

8.1.1 SBOM 类别

按照生成方式区分，SBOM可分为分析型和构建型等类型。

是否必须：否

字段名称：bomType

数据类型：枚举类型

数据格式：SBOM类型字符串（分析型-analyzed，构建型-build）

可选值范围: ["build","analyzed"]

示例："bomType": "analyzed"

8.1.2 分析型 SBOM

可通过分析现有的代码库、二进制文件或容器镜像生成分析性SBOM。

适用于建立对存量软件的透明度，或验证供应商、软件制作商提供的SBOM，以发现其他SBOM生成工具在不同阶段无法检测到的依赖项。

示例："bomType": "analyzed"

8.1.3 构建型 SBOM

构建型SBOM可由构建系统自动生成，包含构建产品构件所需的数据，包括但不限于在构建过程中实际使用的所有依赖项、工具和环境信息等。

示例："bomType": "build"

8.2 与其他组件关系

可标明组件之间除依赖关系之外的其他关系，如包含关系、源码引用等。

可体现直接依赖之外的派生依赖关系，说明虽然某组件类似于一些其他已知组件，但已做出了一些变更。

是否必须：否

字段名称：otherRelationships

数据类型：数组

数据格式：依赖的组件的 PRUL。在依赖关系中添加

```
otherRelationships:[
    {
        "ref": "唯一标识符",
        "relationships": [
        {
            "target": "该组件的直接依赖组件的唯一标识符"
            "relationshipType": "与组件的依赖关系类型"
        },
        {
            "target": "其他直接依赖的唯一标识符",
            " relationshipType": "与组件的依赖关系类型"
        }
    ]
},
{ 其他组件的依赖关系 }
]
```

可选值范围：

1. 依赖关系：
   - 运行时依赖：runtime
   - 构建依赖：build
   - 测试依赖：test
   - 开发依赖：dev
   - 可选依赖：optional
2. 包含关系：
   - 包含：contains
   - 被包含： contained
3. 生成关系：
   - 生成：generates
   - 由...生成：generated
4. 演变关系：

- 祖先版本：ancestor
- 后代版本：descendant
- 变体：variant
- 补丁：patch

5. 其他关系：
- 强依赖： requires
- 前置条件：prerequisites

示例："otherRelationships": [


```
            {
                    "ref": "pkg:pkg:npm/myapp@1.0.0",
                    "relationships": [
                        {
                            "target": "pkg:npm/express@4.17.1",
                            "relationshipType": "runtime"
                        },
                        {
                            "target": "pkg:npm/redis@4.0.0",
                            "relationshipType": "test"
                        }
                    ]
            }
        ]
```


8.3 组件安全信息

可标明组件的安全管理信息。组件的安全管理信息包括以下内容：

a）安全漏洞记录。列出已知的安全漏洞及修复状态。

是否必须：否

字段名称：vulRecord

数据类型：字典列表

数据格式：[{"vulId": 漏洞编号,"source": 漏洞地址,"status": 漏洞状态}]

漏洞状态可选值范围：[已修复:fixed,已缓解:misinformation,风险可接受:tolerable,误报:false-alarm,未处理:unsolved]

示例："vulRecord":[{"vul-id": "cve-2024-xxxx", "source": "https://xx.xx.xx", "status":" fixed"}, {"vul-id": "cve-2024-xxxx", "source": "https://xx.xx.xx", "status": "misinformation"}, {"vul-id": "cve-2024-xxxx", "source": "https://xx.xx.xx", "status":"tolerable"}, {"vul-id": "cve-2024-xxxx", "source":"https://xx.xx.xx", "status": "misinformation"}]

b）安全更新和补丁。记录与组件相关的安全更新和补丁历史及其适用版本。

是否必须：否

字段名称：securityPatches

数据类型：字典列表

数据格式：[{"version": 补丁版本, "applicableversions": 适用的版本范围, "description": 补丁描述, "resolves": 对应修复的漏洞编号}]

示例："securityPatches":[{"version": "2.5.4-hotfix", "applicableversions": ["1.0,1.1"]}, "description": "关于cve-2024-xxxx漏洞的修复补丁", "resolves": ["cve-2024-xxxx"]]

c）安全配置建议。提供提高安全性的配置建议或最佳实践。

是否必须：否

字段名称：securityAdvice

数据类型：字典列表

数据格式：[{"description": 安全配置建议, "doc": 文档地址}]

示例：securityAdvice: [{"description": "应当关闭XML外部实体解析功能", "doc": "https://xx.xx.xx"}]

d）安全测试结果。记录组件经过的安全测试结果，如静态分析、动态分析或渗透测试的报告和证书。

是否必须：否

字段名称：securityTest

数据类型：字典列表

数据格式：[{"type": 工具类型, "tool": 工具名称, "source": 结果地址}]

示例："securityTest": [{"type": "sast", "tool": "xmaze-sast-v3.6", "result-source": "download.abc.com/aaa.pdf"}]

8.4 组件来源信息

可标明组件的来源及取得方式。

如果组件通过公开下载获得，可提供下载URL。当组件存在上游社区时，可提供上游社区的信息，如源码仓库URL、官方网站URL等。

是否必须：否

字段名称：componentDownloadLocation

数据类型：字符串

数据格式：单行文本

示例："componentDownloadLocation": "https://xx.xx.xx"

8.5 组件版权信息

用来明确软件组件的版权归属及相关许可信息。可详细说明版权所有者、版权起始与结束年份（若适用）。

是否必须：否

字段名称：componentCopyrightText

数据类型：数组

数据格式：[{"Owner":所有者, "CopyrightText": 版权文本}]

示例："componentCopyrightText": [{"Owner": "Company A", "CopyrightText": "Copyright © 2024 Example Corp."}]

8.6 补丁信息

用来对软件组件所应用的补丁进行详细说明。应提供补丁的相关信息，包括补丁名称、版本、发布日期、修复内容等。

是否必须：否

字段名称：componentPatchDetails

数据类型：数组

数据格式：[{"patchName": 补丁名称, "patchVersion": 补丁版本, "releaseDate": 发布时间, "fixes": 修复内容}]

示例 ："componentPatchDetails": [{"patchName": "Patch-001", "patchVersion": "1.0", "releaseTime": "2024-01-01", "fixes": "解决了一个关键bug."}]

8.7 组件描述

用来对软件组件进行附加的说明解释或描述。可标明组件的描述信息，说明组件的基本功能、用途和主要特性等。

是否必须：否

字段名称：componentComments

数据类型：字符串

数据格式：多行文本

示例1："componentComments": "没有评论"

示例2："componentComments": "这是开发人员的工具"

8.8 文件信息

8.8.1 文件名称

标识文件发起方应提供的文件的全名。

应使用原始供应商定义的组件完整名称，避免使用缩写或模糊名称。

文件名称应具备处理多个名称或别名的功能。

是否必须：否

字段名称：fileName

数据类型：字符串

数据格式：单行文本

示例 1："fileName": "header.h"

8.8.2 文件作者

用于明确文件的作者或主要贡献者相关信息。可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。

是否必须：否

字段名称：fileAuthor

数据类型：字典列表

数据格式：多行文本

示例 1："fileAuthor":{"Name":"John Smith","Organization":"ABC Tech","Email":"john.smith@abctech.com","Role":"Lead Developer. John was responsible for the overall architecture and major functionality implementation of the software component."}

8.8.3 文件哈希值

用于为文件提供唯一的数字指纹标识信息。

文件的哈希值应作为其固有标识符，哈希值生成算法应明确。

可以为一个文件或多个文件的集合提供多个哈希值。

是否必须：否

字段名称：fileChecksums

数据类型：字典

数据格式：由哈希算法名称（如 SHA-256）和对应的哈希值（十六进制字符串）组成，格式为“算法名称:哈希值”

示例 1："fileChecksums": "SHA-256:3a7bd3e2360a3d29eea436fcfb7e44c716e7f537ab8ee5"

示例 2："fileChecksums": "SHA-384:56e410b092b40811b353b1b13c26149979946600710533"

示例 3："fileChecksums": "SHA-512:7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677"

8.8.4 文件版权信息

用来明确文件的版权归属及相关许可信息。可详细说明版权所有者、版权起始与结束年份（若适用）。

是否必须：否

字段名称： fileCopyrightText

数据类型：数组

数据格式：多行文本

示例："fileCopyrightText" :["Owner": "Company A", "Years":" 2020 - 2024"]

8.8.5 文件描述

用来对文件进行附加的说明解释或描述。可标明文件的描述信息，说明文件的基本功能、用途和主要功能等。

是否必须：否

字段名称：fileComments

数据类型：字符串

数据格式：多行文本

示例1："fileComments": "no remarks"

示例2："fileComments": "This is a tool for developers."

8.8.6 代码片段信息

8.8.6.1 代码片段标识

标识代码片段。

是否必须：否

字段名称：snippetId

数据类型：字符串

数据格式：单行文本

示例 1："snippetId": "DP-BOM-SNIPPET-XXXX"

8.8.6.2 代码片段范围

用于明确代码片段的作者或主要贡献者相关信息。可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。

是否必须：否

字段名称：snippetRange

数据类型：字典列表

数据格式：多行文本

示例 1："snippetRange": {"byte", "300:560"}

示例 2："snippetRange": {"line", "10:25"}

8.8.6.3 代码片段版权信息

用来明确代码片段的版权归属及相关许可信息。可详细说明版权所有者、版权起始与结束年份（若适用）。

是否必须：否

字段名称： snippetCopyrightText

数据类型：数组

数据格式：多行文本

示例："snippetCopyrightText":["Owner":" Company A, Years: 2020 - 2024"]

8.8.6.4 代码片段描述

用来对代码片段进行附加的说明解释或描述。可标明代码片段的描述信息，说明代码片段的基本功能、用途和主要功能等。

是否必须：否

字段名称：snippetComments

数据类型：字符串

数据格式：多行文本

示例1："snippetComments": "no remarks"

示例2："snippetComments": "This is a tool for developers."

9 支持工具要求

9.1 能力要求

SBOM支持工具应具备自动生成、更新和管理软件物料清单的能力，并能够提供全面的依赖关系分析。工具应支持与资产管理系统、许可证合规性分析、安全威胁情报、漏洞管理以及安全信息与事件管理等关键系统的集成，确保与现有开发和构建工具链的无缝对接。同时，工具应提供用户友好的界面。

9.2 能力类型

不同生态场景的工具应支持的基本能力类型，详见表1。

表1 工具能力分类

生态场景	能力类型	能力描述
文档生成	自动构建	文档作为构建工件的一部分自动创建，并且包含关于构建的信息
	分析审计	源代码分析或审计工具通过检查工件和相关来源生成文档
	手工填写	支持手工编辑信息
顶层应用	查看	支持人类可读的内容形式（图片、数字、表格、文本等），用于决策和业务流程
	比较	能够比较给定格式的两份文件，并清楚地显示差异。例如，比较一个软件的两个不同版本
	分析	能够能读取文档进行相关分析（例如进行软件风险评估）
中间转换	转换	从一种文件类型更改为另一种文件类型，同时保留相同的信息
	合并	出于分析和审计目的，可以将多个来源的文档合并在一起
	集成	支持以API和库的形式在其他工具中使用

9.3 格式支持

工具应支持国内外主流的 SBOM 数据格式，并满足本文件的要求。

9.4 生成深度

工具应确保生成的 SBOM 文档能够充分反映软件产品的组成结构、依赖关系等信息，以支持多种分析和管理需求。工具对生成深度的支持分为以下四个层级：

a）基础深度

列出软件产品中所有直接可识别的组件，记录软件中显式声明和直接包含的组件信息。包括但不限于操作系统、中间件、第三方库和应用程序代码包，并提供组件的基本信息，如供应商名称、组件名称和版本等。

b）中等深度

在基础深度的基础上，包括所有直接和间接依赖的组件及其版本，展示组件之间的依赖关系，涵盖直接依赖和间接依赖。

c）详细深度

在中等深度的基础上，提供详细的所有组成信息和组件间的所有直接和间接依赖关系，包括每个组件的许可证类型、供应商信息、来源和完整的依赖树。

d）动态深度

在详细深度的基础上，能实时跟踪和更新组件及其依赖信息。能持续更新 SBOM 信息，反映组件的动态变化，并具备报告和通知功能。

9.5 兼容性

工具应确保生成的 SBOM 具有广泛的系统、工具和流程适应性，保持良好的平台兼容性和自定义扩展性。具体要求包括：

a）主流格式兼容性

应兼容主流的 SBOM 格式，如 SPDX、CycloeDX，便于实现不同系统间的互操作性。有关本文件中规定的 SBOM 格式与 SPDX 和 CycloneDX 的对比，见附录 B。

b）工具兼容性

生成的 SBOM 应能够被多种主流的软件供应链安全工具、持续集成/持续部署（CI/CD）系统以及

合规性检查工具所支持。

c）平台兼容性

应能在不同操作系统和平台上操作 SBOM 工具进行读取和处理，包括但不限于 Windows、Linux、macOS、国产操作系统等。

d）自定义项兼容性

应允许使用者根据特定需求对 SBOM 进行自定义扩展，以包含额外的信息或字段，同时保持与标准格式的兼容性。

e）组件唯一标识符兼容性

应符合统一的唯一标识符格式。

9.6 易用性

9.6.1 概述

工具应具备高效、直观的操作界面，便于各种利益相关者理解和使用。

9.6.2 汉字支持

工具应在输入格式、输出格式和接口、网页界面等提供全面的汉字支持。

9.6.3 结构清晰

工具应具备清晰的结构，能够显示每个组件的层次和依赖关系。

9.6.4 易于搜索和过滤

工具应提供搜索和过滤功能，能够快速找到特定的组件或组件集合。

9.6.5 可扩展性

工具应支持灵活的扩展机制，以适应未来的新需求和技术发展。具体符合：

a）数据模型灵活性。SBOM 的数据模型应采用模块化设计，允许根据需要添加、删除或修改数据字段和实体；

b）插件与扩展机制。工具应提供插件或扩展点机制，允许第三方开发者或内部团队为 SBOM 系统添加新功能或扩展现有功能，而无需修改核心代码。

10 管理和应用要求

10.1 概述

SBOM管理和应用的核心要求旨在确保SBOM的有效性和全面性，以支持软件供应链的透明、安全、合规及可持续。

10.2 覆盖范围

SBOM应详尽列出软件组件的组成结构、依赖关系、许可证信息及安全状态，以满足不同场景下的合规性和安全性需求。数据应具备足够的深度，以便实现全面的分析和管理。

对于操作系统、数据库、中间件等基础软件，应至少列出软件产品中所有直接依赖的组件基本信息，包括供应商名称、组件名称和版本。

10.3 更新和版本管理

SBOM应与软件版本的更新和修订保持同步。应在软件的选型、设计、开发、使用等生命周期的不同阶段创建相应的SBOM。当软件组件更新或获取新的底层信息时，应对SBOM信息进行维护更新。

应对不同版本的SBOM进行有效管理，确保每次软件更新或修订时，SBOM版本能准确反映最新状态，同时能够对历史版本提供记录和查询。

10.4 SBOM 采用类型

应推动从分析型SBOM向构建型SBOM的转变。构建型SBOM在软件构建过程中生成，能够提供更准确、实时的组件信息，以适应现代软件开发中对持续集成和部署的需求。

10.5 声明未详尽信息

对于在SBOM中未列出完整依赖表的组件，SBOM作者应明确识别并声明未详尽列举的信息。如在依赖关系中清晰区分出不包含其他依赖的组件，以及依赖信息不明确或不完整的组件。

该数据应集成到工具中，并默认数据为不完整。SBOM提供者应明确说明是否已完全列出组件的所有直接依赖，或组件是否没有其他依赖。

10.6 分发和交付

SBOM应及时、安全地交付给需求方，并应采用加密技术保护SBOM的存储和传输过程，确保数据的机密性和完整性。

10.7 维护和监控

应对已分发和交付的 SBOM 建立监控机制,持续监控 SBOM 涉及的依赖组件。当出现新的风险时，应及时对软件进行修复升级，并更新 SBOM 文档。

10.8 与其他关键信息系统的互操作性

10.8.1 软件资产管理

应能够与软件资产管理系统互操作，符合如下使用要求：

a）能从组件名称、组件来源及版本维度查看软件资产；

b）能从组件出发，定位其被应用的已上线服务。

10.8.2 软件漏洞管理

应能够与软件漏洞管理系统互操作，满足如下使用要求：

a）能从安全漏洞出发，定位被影响的组件；

b）能从应用程序出发，查看应用程序SBOM的安全漏洞信息。

10.8.3 安全事件响应

应能与安全事件响应有关系统互操作，满足如下使用要求：

a）SBOM能与安全信息与事件管理系统（SIEM）集成，支持安全运营中心（SOC）的运营工作；

b）SBOM能与威胁情报平台（TIP）集成，支持威胁情报关联和匹配。

10.9 访问控制

应设置明确的访问权限和角色管理，以控制对SBOM数据的访问。只准许经过授权的用户或系统才能查看、修改或下载SBOM数据。

10.10 完整真实

SBOM数据及其来源应具有可验证性，所有SBOM文档在分发前应进行数字签名，接收时应验证数字签名，以提供身份认证和完整性校验。

10.11 其他

应尽可能详细地记录整个软件生命周期中的所有相关信息，并通过技术手段确保数据的完整性，以防止数据被篡改。同时，应提高SBOM的机器可读性，强化数据的标准化和规范化，以便更有效地管理和分析依赖关系。此外，动态依赖关系、第三方服务的调用、人工智能模型以及其他未直接包含在软件构建中的依赖关系应适当纳入SBOM管理范围。

附 录 A
（规范性）
DP-SBOM 格式参考

A.1 概述

DP-SBOM 数据格式聚焦于描述组成软件包成分清单，并标识软件包的身份信息，定义支持管理软件包成分的基础属性。

A.2 兼容性

为保证 SBOM 兼容性，应满足：

a) 采用 JSON 格式对软件包成分进行描述；
b) 采用 PURL 作为软件包唯一标识；
c) 满足 SBOM 基本数据字段要求；
d) 能够与常见的 SBOM 协议标准相互转换。

A.3 JSON数据模型

```
{
    "$schema": "http://json-schema.org/draft-07/schema#",
    "title": "SBOM 1.0",
    "type": "object",
    "properties": {
        "documentBasicInfo": {
            "type": "object",
            "properties": {
                "documentName": {
                    "type": "string",
                    "description": "由创建者指定此 SBOM 文档的名称"
                },
                "documentVersion": {
                    "description": "文档版本由主要版本字段、次要版本字段和修订版本字段组成。文档版本由主要版本字段、次要版本字段和修订版本字段组成",
                    "type": "string"
                },
                "timestamp": {
                    "description": "首次创建 SBOM 文档及每次更新时，均应记录时间戳。时间戳应符合《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》等标准格式。",
                    "type": "string"
                },
                "bomFormat": {
                    "description": "SBOM 文档应明确使用的数据格式，包括格式名称、版本号及相应的格式
```

```
标准或规范 URL",
                    "type": "string"
                },
                "tool": {
                    "description": "生成 SBOM 文档的工具信息，包括工具名称和工具版本等。",
                    "type": "string"
                },
                "bomAuthor": {
                    "name": "生成 SBOM 的作者",
                    "type": "string"
                },
                "bomAuthorComment": {
                    "name": "创建者备注",
                    "type": "string"
                },
                "bomComment": {
                    "name": "文档备注",
                    "type": "string"
                },
                "bomType": {
                    "description": "SBOM 的生成方式类型",
                    "type": "enumeration",
                    "enum": [
                        "ANALYZED",
                        "BUILD"
                    ]
                }
            },
            "required": [
                "documentName",
                "documentVersion",
                "timestamp",
                "bomFormat",
                "tool"
            ],
            "additionalProperties": false
        },
        "softwareCompositionInfo": {
            "type": "object",
            "properties": {
                "components": {
                    "type": "array",
```

```
"items": {
    "type": "object",
    "properties": {
        "componentAuthor": {
            "type": "object",
            "properties": {
                "name": {
                    "type": "string",
                    "description": "软件组件的创作者或主要贡献者名称"
                },
                "email": {
                    "type": "string",
                    "description": "软件组件的创作者或主要贡献者电子邮箱"
                },
                "organization": {
                    "type": "string",
                    "description": "软件组件的创作者或主要贡献者所在组织"
                }
            },
            "required": [ "name" ],
            "additionalProperties": false
        },
        "componentProvider": {
            "type": "object",
            "properties": {
                "name": {
                    "type": "string",
                    "description": "软件组件的供应商名称"
                },
                "email": {
                    "type": "string",
                    "description": "软件组件的供应商电子邮箱"
                },
                "organization": {
                    "type": "string",
                    "description": "软件组件的供应商所在组织"
                }
            },
            "required": [ "name" ],
            "additionalProperties": false
        },
        "componentName": {
```

```
                "type": "string",
                "description": "标识组件发起方应提供的组件的全名"
            },
            "componentVersion": {
                "type": "string",
                "description": "标识组件的版本，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"
            },
            "componentChecksums": {
                "type": "array",
                "items": {
                    "type": "object",
                    "properties": {
                        "algorithm": {
                            "type": "string",
                            "enum": [
                                "SHA1",
                                "BLAKE3",
                                "SHA3-384",
                                "SHA256",
                                "SHA384",
                                "BLAKE2b-512",
                                "BLAKE2b-256",
                                "SHA3-512",
                                "MD2",
                                "ADLER32",
                                "MD4",
                                "SHA3-256",
                                "BLAKE2b-384",
                                "SHA512",
                                "MD6",
                                "MD5",
                                "SHA224"
                            ]
                        },
                        "checksumValue": {
                            "type": "string"
                        }
                    },
                    "required": [
                        "algorithm",
                        "checksumValue"
```

```
        ],
        "additionalProperties": false
    }
},
"componentId": {
    "type": "string",
    "description": "用于识别组件或作为相关数据库查询的唯一标识符"
},
"license": {
    "type": "array",
    "description": "标识该组件或文件所使用的开源许可证或商业许可证"
},
"componentTimestamp": {
    "type": "string",
    "description": "组件 SBOM 数据生成或更新的时间戳"
},
"componentSecurityInfo": {
    "type": "object",
    "properties": {
        "vulRecord": {
            "type": "dict",
            "items": {
                "type": "object",
                "properties": {
                    "vulId": {
                        "type": "string"
                    },
                    "source": {
                        "type": "string"
                    },
                    "status": {
                        "type": "string"
                    }
                }
            }
        },
        "securityPatches": {
            "type": "dict",
            "items": {
                "type": "object",
                "properties": {
                    "version": {
```

```
                "type": "string"
            },
            "applicableVersions": {
                "type": "string"
            },
            "description": {
                "type": "string"
            },
            "resolves": {
                "type": "string"
            }
        }
    }
},
"securityAdvice": {
    "type": "dict",
    "items": {
        "type": "object",
        "properties": {
            "description": {
                "type": "string"
            },
            "doc": {
                "type": "string"
            }
        }
    }
},
"securityTest": {
    "type": "dict",
    "items": {
        "type": "object",
        "properties": {
            "type": {
                "type": "string"
            },
            "tool": {
                "type": "string"
            },
            "resultSource": {
                "type": "string"
            }
```

```
                    }
                }
            }
        },
        "componentDownloadLocation": {
            "type": "string",
            "description": "组件的来源及取得方式"
        },
        "componentCopyrightText": {
            "type": "array",
            "items": {
                "type": "string",
                "description": "确定组件的版权所有者，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"
            }
        },
        "componentPatchDetails": {
            "type": "array",
            "items": {
                "type": "string",
                "type": "string",
                "description": "软件组件所应用的补丁进行详细说明"
            }
        },
        "componentComment": {
            "type": "string"
        },
        "fileList": {
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "fileName": {
                        "type": "string"
                    },
                    "fileAuthor": {
                        "type": "string"
                    },
                    "fileCheckSums": {
                        "type": "dict",
                        "items": {
```

```
            "type": "object",
            "properties": {
                "algorithm": {
                    "type": "string",
                    "enum": [
                        "SHA1",
                        "BLAKE3",
                        "SHA3-384",
                        "SHA256",
                        "SHA384",
                        "BLAKE2b-512",
                        "BLAKE2b-256",
                        "SHA3-512",
                        "MD2",
                        "ADLER32",
                        "MD4",
                        "SHA3-256",
                        "BLAKE2b-384",
                        "SHA512",
                        "MD6",
                        "MD5",
                        "SHA224"
                    ]
                },
                "checksumValue": {
                    "type": "string"
                }
            },
            "required": [
                "algorithm",
                "checksumValue"
            ],
            "additionalProperties": false
        }
    },
    "fileCopyrightText": {
        "type": "array"
    },
    "fileComment": {
        "type": "string"
    },
    "snippetList": {
```

```
                "type": "array",
                "items": {
                    "type": "object",
                    "properties": {
                        "snippetId": {
                            "type": "string"
                        },
                        "snippetRange": {
                            "type": "dict",
                            "properties": {
                                "startLine": {
                                    "type": "integer"
                                },
                                "endLine": {
                                    "type": "integer"
                                }
                            }
                        },
                        "snippetCopyrightText": {
                            "type": "string"
                        },
                        "snippetComment": {
                            "type": "string"
                        }
                    },
                    "required": [
                        "snippetId",
                        "snippetRange"
                    ],
                    "additionalProperties": false
                }
            }
        },
        "required": [
            "fileName",
            "fileAuthor",
            "fileCheckSumAlg",
            "fileCheckSumValue"
        ],
        "additionalProperties": false
    }
}
```

```
                },
                "required": [
                    "componentAuthor",
                    "componentProvider",
                    "componentName",
                    "componentVersion",
                    "componentChecksums",
                    "componentId",
                        "license",
                        "dependencies",
                    "componentTimestamp"
                ],
                "additionalProperties": false
            }
        },
        "dependencies": {
            "type": "dict",
            "items": {
                "type": "object",
                "properties": {
                    "ref": {
                        "type": "string"
                    },
                    "dependsOn": {
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "ref": {
                                    "type": "string"
                                }
                            }
                        }
                    }
                },
                "required": [
                    "ref",
                    "dependsOn"
                ],
                "additionalProperties": false
            }
        },
```

```
    "otherRelationships": {
        "type": "array",
        "items": {
            "type": "object",
            "ref": {
                "type": "string"
            },
            "relationships": {
                "type": "array",
                "target": {
                    "type": "string"
                },
                "relationshipType": {
                    "type": "string";
                    "enum": [
                        "runtime",
                        "build",
                        "test",
                        "dev",
                        "optional",
                        "contains",
                        "contained",
                        "generates",
                        "generated",
                        "ancestor",
                        "descendant",
                        "variant",
                        "patch",
                        "requires",
                        "prerequisites"
                     ]
                }
            },
            "required": [
                "componentID",
                "includes"
            ],
            "additionalProperties": false
        }
    }
},
"required": [
```

```
                "components",
                "dependencies"
            ],
            "additionalProperties": false
        }
    },
    "required": [
        "documentBasicInfo",
        "softwareCompositionInfo"
    ],
    "additionalProperties": false
}
```

附 录 B
（资料性）
DP-SBOM 与 SPDX、CycloneDX 的对比

DP-SBOM 1.0从安全增强、元数据细粒度化、全链路治理三方面构建了一套更适用于复杂供应链场景的SBOM标准。与SPDX 2.2和CycloneDX 1.6相比，DP-SBOM 1.0主要有以下几点差别：

a）安全纵深扩展：引入安全配置建议、测试结果、补丁追踪等字段，覆盖漏洞修复、策略防御、结果验证的全流程，实现从“风险检测”到“主动加固”的能力提升；

b）溯源粒度升级：支持代码片段级版权声明（如行号范围标识）与文件作者溯源，相较于SPDX的文件级校验和、CycloneDX的组件级哈希，实现了更精细化的管理；

c）治理多维融合：相较于SPDX/CycloneDX侧重单一领域（合规或安全），整合了SBOM类型标识、文档版本控制、创建者备注等元数据，满足开发、合规、运维多角色实际业务需求；

d）动态威胁响应：内置漏洞记录、更新和补丁等字段，直接关联漏洞数据库与修复方案，避免了SPDX的外链依赖与CycloneDX的静态CVE条目局限。

DP-SBOM与SPDX、CycloneDX的主要字段对比如表2所示。

表2 DB-SBOM和SPDX、CycloneDX的数据字段对比

分类	字段名称	DP-SBOM 1.0	SPDX 2.2	CycloneDX 1.6
文档相关	文档名称	☑	☑	☒
	文档版本	☑	☑	☑（规范版本）
	文档时间戳	☑	☑ （创建时间）	☑（时间戳）
	数据格式	☑	☑	☑
	工具信息	☑	☑（创建工具）	☑（工具链）
	创建者信息	☑	☑（创建者）	☑（创建者）
	创建者备注	☑	☒	☒
	文档备注	☑	☑（文档注释）	☒
组件相关	作者名称	☑	☒	☒
	供应商名称	☑	☑（供应商）	☑（供应商）
	组件名称	☑	☑（名称）	☑（名称）
	组件版本	☑	☑（版本）	☑（版本）
	组件哈希值	☑	☑（校验码）	☑（哈希值）
	唯一标识符	☑	☑(SPDX ID)	☑(PURL/CPE))
	许可证	☑	☑（许可证声明）	☑（许可证）
	依赖关系	☑	☑（依赖树）	☑（依赖图）
	时间戳	☑	☒	☒
	SBOM 类型	☑	☒	☒
	与其他组件关系	☑	☑（元素关系）	☑（依赖关系）

	安全漏洞记录	☑	☒	☑（CVE 条目）
	安全更新和补丁	☑	☒	☒
	安全配置建议	☑	☒	☒
	安全测试结果	☑	☒	☒
	组件来源信息	☑	☑（下载地址）	☑（外部引用）
	组件版权信息	☑	☑（版权声明）	☑（版权声明）
	补丁信息	☑	☒	☒
	组件描述	☑	☑（描述）	☑（描述）
文件相关	文件名称	☑	☑	☑
	文件作者	☑	☒	☒
	文件哈希值	☑	☑（校验码）	☑（哈希值）
	文件版权信息	☑	☑（版权声明）	☑（版权声明）
	文件描述	☑	☑（描述）	☒
片段相关	片段标识	☑	☑（片段 ID）	☒
	片段范围	☑	☑（代码位置）	☒
	片段版权信息	☑	☑（版权声明）	☒
	片段描述	☑	☑（描述）	☒

参考文献

[1] GB/T 11457-2006 信息技术 软件工程术语
[2] GB/T 25069-2022 信息安全技术 术语
[3] GB/T 36475-2018 软件产品分类
[4] GB/T 25109.1-2010 企业资源计划 第1部分：ERP术语
[5] GB/T 42927-2023 金融行业开源软件测评规范