ICS 35.240

CCS:D07

团体标准

T/CCSA [XXXX]—[XXXX]

|  |
| --- |
| 数字公共产品评估规范 第1部分：通用要求  Assessment criteria of digital public goods  Part 1: General framework  [点击此处添加与国际标准一致性程度的标识]  （征求意见稿）  2022.09 |

[××××]-[××]-[××]发布

[××××]-[××]-[××]实施

中国通信标准化协会 发 布



目　　次

[目　　次 I](#_Toc118384762)

[前　　言 III](#_Toc118384763)

[引　　言 IV](#_Toc118384764)

[数字公共产品评估规范 第1部分：通用要求 1](#_Toc118384765)

[1 范围 1](#_Toc118384766)

[2 规范性引用文件 1](#_Toc118384767)

[3 术语定义和缩略语 1](#_Toc118384768)

[3.1 术语和定义 1](#_Toc118384769)

[3.2 缩略语 2](#_Toc118384770)

[4 数字公共产品能力框架 2](#_Toc118384771)

[5 非竞争排他性 3](#_Toc118384772)

[5.1 产品开放透明能力 3](#_Toc118384773)

[5.2 基础设施能力 4](#_Toc118384775)

[5.3 数据提取能力 5](#_Toc118384776)

[6 可扩展性 5](#_Toc118384777)

[6.1 产品迭代能力 5](#_Toc118384778)

[6.2 质量管理能力 5](#_Toc118384779)

[6.3 需求管理能力 5](#_Toc118384780)

[6.4 分支管理能力（可选） 5](#_Toc118384781)

[7 互操作性 6](#_Toc118384782)

[7.1 产品兼容能力 6](#_Toc118384783)

[7.2 依赖管理能力 6](#_Toc118384784)

[7.3 附属文档完备能力 6](#_Toc118384785)

[8 安全性 6](#_Toc118384786)

[8.1 安全保障能力 6](#_Toc118384787)

[8.2 漏洞修复能力 6](#_Toc118384788)

[8.3 无害处置能力 7](#_Toc118384789)

[9 可信性 7](#_Toc118384790)

[9.1 自主所有权保护能力 7](#_Toc118384791)

[9.2 隐私保护能力 8](#_Toc118384792)

[9.3 当地法律遵守能力 8](#_Toc118384793)

[10 可持续性 8](#_Toc118384794)

[10.1 数字发展规范能力 8](#_Toc118384795)

[10.2 可持续发展能力 8](#_Toc118384796)

|  |
| --- |
|  |



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》的规则起草。

YD/T ×××××—××××《数字公共产品评估规范》分为以下六个部分：

——第1部分：通用要求

——第2部分：开源软件

——第3部分：开放数据

——第4部分：开放人工智能模型

——第5部分：开放标准

——第6部分：开放内容

本文件为YD/T ×××××—××××的第1部分。

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这些专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国信息通信研究院，华为技术有限公司，深圳市腾讯计算机系统有限公司，腾讯云计算（北京）有限责任公司，中兴通讯股份有限公司，国际商业机器(中国)投资有限公司，中国移动通信集团有限公司。

本标准主要起草人：郭雪，张一阳，梁辰晔，高琨，陈哲，王勇，张亚军，刘海涛，苏强，项曙明，李响，李雪，袁泉，邓小华，高嵩，唐枕、吕思婕，顾荣。

引　　言

当前，随着人工智能、物联网等新兴数字技术的飞速进步，数字技术正在彻底改变全球经济和社会治理模式。然而，受限于碎片化的全球数字治理规则、相对薄弱的数字化基础设施，以及有待提高的民众数字素养等因素，围绕数字技术的潜在风险可能会不利于促进繁荣、包容和有韧性的社会的发展，破坏人们对关键机构的信任，通过侵犯隐私和虚假宣传活动侵蚀社会规范，从而加剧社会排斥和不平等。数字公共产品能够最大限度发挥数字技术的潜力，助推社会可持续发展目标的实现，同时也有助于克服人类当前面临的许多共同挑战。由于行业发展迅速，各厂商对数字公共产品认知不同，提供的产品类型多样，因此建立一套统一的要求标准，对于规范数字公共产品，促进社会健康可持续发展具有重要意义。

本文件结合当前国内数字公共产品建设的实际需要，将对数字公共产品应具备的通用要求进行规范，为提供方、用户方、实施方、贡献与维护方、资助方提供参考。

|  |
| --- |
|  |

数字公共产品评估规范 第1部分：通用要求

2. 范围

本文件规定了数字公共产品的规范要求及应遵循的指标。具体包括许可证合规能力、依赖管理能力、附属文档完备能力、所有权保障能力、隐私保护和法律合规能力、可持续发展能力等。

本文件适用于分析数字公共产品的非竞争排他性、可持续性、互操作性、可信性、安全性、可持续性等，完善产品相关功能。

1. 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 28458-2012 信息安全技术 安全漏洞标识与描述规范

1. 术语定义和缩略语
   1. 术语和定义

下列术语和定义适用于本文件。



开源 open source

即开放一类技术或一种产品的源代码，源数据，源资产，可以是各行业的技术或产品，其范畴涵盖文化、产业、法律、技术等多个社会维度。

开源社区 open source community

以开源项目的贡献者为主体，在开源项目贡献过程中形成的具有特定文化、组织结构、运行机制的共同体。

可信开源社区 trustworthy open source community

开源社区的可信即保证社区内治理架构和开源项目的可信，包括社区参与者的信息透明性、社区运营的包容性、社区开源项目的可用性、社区开源代码的安全性、社区工具平台的可靠性等。

开源软件 open source software

允许用户直接访问源代码，通过开源许可协议将其复制、修改、再发布的权利向公众开放的计算机软件。

开源组件 open source component

是开源软件系统中最小可识别且本身不再包含另外组件的、组件信息可在公共网站获取且可独立分发、开发过程中带有版本号并且可组装的软件实体。

开源许可证 open source license

开源软件的版权持有人授予用户可以学习、修改开源软件，并向任何人或为任何目的分发开源软件的权利。

安全漏洞 vulnerability

计算机信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷。这些缺陷以不同形式存在于计算机信息系统的各个层次和环节之中，一旦被恶意主体所利用，就会对计算机信息系统的安全造成损害，从而影响计算机信息系统的正常运行。

[来源：GB/T 28458-2012，定义3.10]

* 1. 缩略语

下列缩略语适用于本文件。

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

CI：持续集成（Continuous Integration）

CLA：贡献者协议（Contributor License Agreement）

CVE：通用漏洞披露（Common Vulnerabilities Exposures）

GA：软件正式发布版本（General Availability）

IDE：集成开发环境（Integrated Development Environment）

RC：软件候选版本（Release Candidate）

1. 数字公共产品能力框架

数字公共产品能力框架如图1所示，数字公共产品能力要求由非竞争排他性、互操作性、安全性、可信性、可扩展性、可持续性六个方面组成。

1. 非竞争排他性要求数字公共产品在不同应用场景下不排除任何人进行消费，同时要求使用对象之间不存在利益冲突；
2. 互操作性指数字公共产品在不同的计算机系统、网络等环境下应具备的运行和信息共享能力；
3. 安全性指数字公共产品应符合的安全基准；
4. 可信性指数字公共产品通过对用户的隐私、权益等方面保护和对当地法律遵守来保证产品用户信任度；
5. 可扩展性要求数字公共产品具备增加新的产品功能与修改原有功能的能力；
6. 可持续性要求数字公共产品符合可持续发展目标。

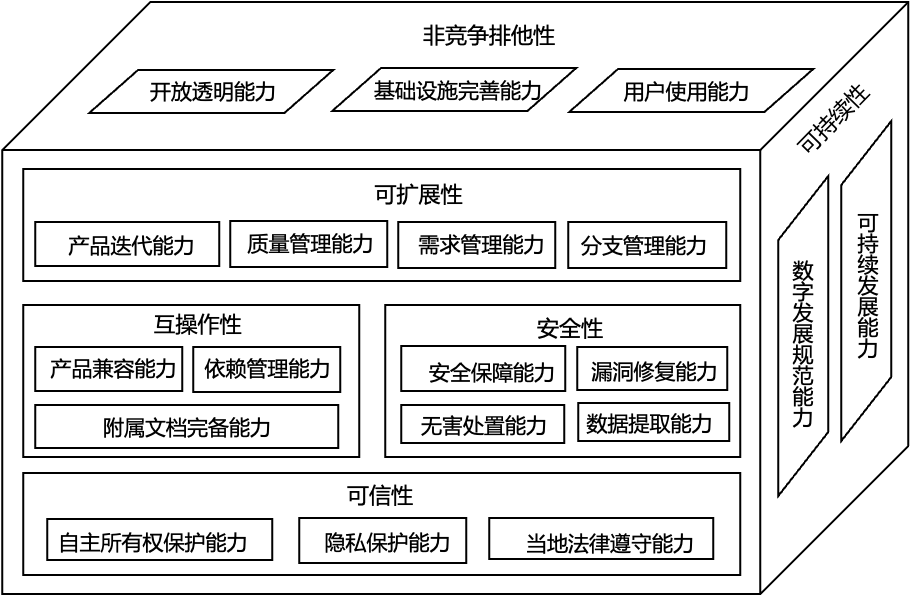


图1 数字公共产品能力框架

1. 非竞争排他性
   1. 产品开放透明能力
      1. 产品许可证规范性

应对数字公共产品的使用、复制、修改和再发布等进行规范。应在开源软件、公开数据集、公开人工智能模型、公开标准或附加文本中声明所使用的开源许可证名称。

应写明许可证应包含的内容

产品开源许可证内容应包括但不限于：

1. 是否保留版权；
2. 是否授予专利权；
3. 开源软件作者或版权持有人进行署名；
4. 明确开源许可证名称，保留许可证全文或链接；
5. 是否允许商业使用；
6. 是否允许修改及修改后再发布；
7. 是否允许私人使用；
8. 明确开源软件的作者或版权持有人不承担产品使用后的风险及产生的后果；
   * 1. 组件许可证规范性（可选）

应通过代码扫描等方式确认产品所含开源组件及许可证情况，对所有引用或依赖的第三方组件进行说明。确保引入的所有开源组件满足开源许可证的合规要求，且正确履行开源使用声明义务，如：

1. 许可证覆盖率；
2. 使用的许可证是否为OSI认证或其他被业界广泛使用的；
   * 1. 许可证兼容规范性（可选）

应明确开源产品的各个组件之间、组件与产品之间的许可证兼容性，解决可能存在的许可证条款冲突。

1. 明确每个组件的开源许可证详细范围，并判断组件许可证之间是否兼容，包括但不限于：
2. 是否允许商业使用；
3. 是否允许二次分发；
4. 合并/修改代码后二次分发时是否需要提供源代码；
5. 判断产品使用的许可证是否与组件许可证存在冲突。
   1. 基础设施能力
      1. 网站

开源产品应具有一个公开稳定的网站供用户进行访问，网站应清晰展示产品信息，包括产品使用场景、项目源代码获取方式、邮件列表、反馈方式等。

* + 1. 代码仓库

开源产品对在设计开发中需要修改的开源代码、数据集、模型、标准、文本应建立源码仓库存储，同时设置开源白名单，对需要引入的开源源码进行开源许可证、开源漏洞等方面审查，通过后方可使用。

* + 1. 开源组件组成成分分析工具（可选）

产品应运用工具识别代码中的开源组件及开源许可证，确保开源许可证合规使用，如有问题应及时作出相应处理。

* + 1. 安全漏洞扫描工具（可选）

产品应运用安全漏洞扫描工具发现代码、文本漏洞等安全问题，并及时作出相应处理。

* + 1. CLA签署工具（可选）

产品应运用CLA签署工具帮助产品贡献者签署贡献者协议。CLA签署工具应支持多语言，同时可支持自动化签署流程。

* + 1. 构建平台（可选）

产品如具有分支代码，应对各分支代码分别进行管理，保障各分支均明确负责人员，对每个分支进行同样的管理流程和测试步骤，标记并记录每个分支与主版本差异部分，同时构建平台应具备如下功能：

1. 启用编译器警告和类Lint的检查；
2. 执行静态分析工具并发现修复可被攻击利用的问题漏洞。
   * 1. 发布平台

产品应对交付物进行管理，对提供给用户的交付物进行开源识别和评估，保障交付物符合用户需求和开源合规要求。

* + 1. 测试平台（可选）

产品应具备稳定易用的测试平台，对代码、文本、数据等进行详细测试。

1. 测试平台可对产品代码进行硬件/操作系统/软件的组合测试；
2. 测试平台可拥有自动定位缺陷责任人的功能，平台自动找出引发故障的提交，并通过邮件发送缺陷报告给该提交的贡献者；
3. 测试平台可给开发者提供调试验证的环境，进行相关场景复现。
   1. 用户使用能力

产品应通过清晰的使用说明、用户友好的界面、备注等多种形式，降低使用门槛，方便用户操作，并保证在不同用户使用时不存在利益冲突。



1. 可扩展性
   1. 产品迭代能力

产品应定期发布新版本，并在每一次版本更新时说明所迭代的功能或修补的漏洞情况。应通过网站、代码托管平台等基础设施与用户建立活跃沟通渠道，维持产品活跃度。

* 1. 质量管理能力

产品应具备软件质量检查机制，在代码编写、数据格式等方面遵循业内标准；每个版本发布前需进行测试且测试覆盖度满足业内规范，确认产品符合规范方可发布。

* 1. 需求管理能力

产品内需求管理应具有端对端可追溯的能力，在分解分配、开发、测试验证过程的数据对象和关系都应被记录，可支撑相关过程记录与现场还原。

* 1. 分支管理能力（可选）

产品如具有分支版本，应对各分支版本进行管理，包括但不限于

1. 产品开发和使用可以根据用户的实际需求自由选择对应分支版本；
2. 产品开发可以采取不同于主版本的流程；
3. 分支在满足规范的条件下可以合入产品主干；
4. 合入到主干分支之前都要进行充分的测试。
5. 互操作性
   1. 产品兼容能力
      1. 版本兼容

产品版本号应遵循语义化版本号规范，同时保证产品所发布新版本的软件接口能够与以往发布的旧版本兼容。

* + 1. 运行环境兼容

产品应能够在不同的硬件架构、网络、操作系统中正常运行，兼容多种数据格式，并在不同数据库、浏览器等配合环境中运行应得到一致的运行结果。

* 1. 依赖管理能力

产品在设计之初应考虑灵活部署，模块化和互操作性。

* 1. 附属文档完备能力
     1. 产品说明文档

应具备完备的产品说明文档，包含产品设计说明、API接口信息、安装部署指南等信息。

* + 1. 产品使用文档

产品应具有高可用性的最终用户文档来提高产品的可靠性与易操作性。

* + 1. 产品开发文档

产品应具有高可用的开发文档来帮助用户进行二次开发，内容包括但不限于：

1. 如何获取源代码；
2. 代码组织和目录结构；
3. 如何设置构建系统；
4. 如何进行构建和单元测试。
   * 1. 产品变更文档

产品应具有详尽的变更文档来帮助用户了解迭代版本差异。

1. 安全性
   1. 安全保障能力

产品应组建专门安全团队或安全人员，定期跟踪用户反馈情况并及时修复安全漏洞等问题。

* 1. 漏洞修复能力
     1. 安全漏洞修复

产品根据实际情况有针对性的发布安全补丁或更新版本，并在新版本发布时说明漏洞或缺陷的修复情况。建立成熟的漏洞管理机制，控制漏洞影响范围，积极修复漏洞，对漏洞风险进行评估。同时具备完善的漏洞修复方案，修复方案应包含：

1. 产品具备版本生命周期内通过补丁修补漏洞的能力；
2. 确保修复方案正确修复漏洞；
3. 制定产品漏洞修复期限，确保漏洞修复进度符合版本发布周期；
4. 产品具备相应策略，决策哪些漏洞可以通过版本升级方式修复，通常是影响性较低的漏洞。
   * 1. 安全漏洞感知

产品应具备漏洞感知能力，确保产品具备合适的漏洞上报途径，且所有漏洞披露渠道都得到监控，且漏洞获取及时，无遗漏。

* + 1. 安全漏洞可追溯（可选）

产品应具备漏洞影响版本追溯能力。同时产品若存在上游依赖，应具备漏洞可追溯能力，对依赖组件的名称、对应版本版本等信息具备可追溯能力。

* 1. 无害处置能力
     1. 数据隐私与安全

数字公共产品在收集数据过程中必须识别收集和存储的数据类型，并确保数据的隐私和安全，具备相应措施防止产品收集、存储和分发数据时所产生的不利影响。如利用加密文件、使用双因素身份验证、限制访问权限、在安全服务器或安全云存储服务上存储数据、与所有数据共享合作伙伴达成数据共享协议等。

* + 1. 不适当及非法内容

数字公共产品在收集、存储或分发内容的过程中必须有识别不适当和非法内容的能力，以及用于检测、调节和删除不适当或非法内容的机制。例如儿童性虐待材料、社会地缘政治敏感信息、虚假宣传活动等。

* + 1. 防止骚扰

数字公共产品若存在用户贡献过程，应具有明确、包容的行为准则来规范产品用户和贡献者的行为，同时应提供违反准则者的约束措施，保护贡献者免受骚扰。

1. 可信性
   1. 自主所有权保护能力

通过数字公共产品所产生的资产所有权必须明确定义和记录。例如，通过版权、商标或其他公开信息进行保护。

* 1. 隐私保护能力

数字公共产品的设计和开发必须符合当地隐私法和其他适用的隐私保护规则。

* 1. 当地法律遵守能力

数字公共产品应证明在开发过程中必须符合当地国家法律法规、标准和技术规范。

1. 可持续性
   1. 数字发展规范能力

数字公共产品在设计和开发中应考虑数字发展原则，包括但不限于：

1. 与用户共同进行产品设计开发，通过构建数字工具更高效地与用户直接需求交互，不断收集和合并用户的反馈；
2. 应充分考虑文化、性别规范、政治环境、经济、技术基础设施和其他可以影响当地获取和使用技术或参与能力的因素；
3. 从设计之初就考虑使用规模，并保持设计简单、灵活、模块化；
4. 明确可持续的商业模式，尽量当地国家和政府以及其他实施组织参与；
5. 注重产品数据分析和运用，有效利用数据信息驱动决策判断；
6. 通过开放共享协调资源要素进行创新开发，如在确保数据隐私需求得到满足后，共享不敏感数据最大化其资源；
7. 考虑现有用户使用技术、数据和框架，保证产品未来的重用和改进；
8. 坚决遵守数据隐私保护原则，尽可能避免收集个人信息，维护用户隐私；
9. 制定全球合作计划，积极寻求全球各区域、组织、学科间协作。
   1. 可持续发展能力

数字公共产品应最大化满足可持续发展目标，包括但不限于：

1. 在全世界消除一切形式的贫困；
2. 消除饥饿，实现粮食安全，改善营养状况和促进可持续农业；
3. 确保健康的生活方式，促进各年龄段人群的福祉；
4. 确保包容和公平的优质教育，让全民终身享有学习机会；
5. 实现性别平等，增强所有妇女和女童权能；
6. 保证清洁饮水和卫生设施的可持续管理；
7. 确保人人获得经济适用的清洁能源，如电力等可再生能源；
8. 确保充分的生产性就业和体面工作，促进持久包容和可持续经济增长；
9. 建造具备抵御灾害能力的基础设施，促进包容性可持续工业；
10. 减少国家内部之间和国家间不平等；
11. 建设包容、安全、有抵御灾害能力和可持续的城市和人类住区；
12. 采用可持续的消费和生产模式；
13. 采取紧急行动应对气候变化及影响；
14. 保护和可持续利用海洋资源；
15. 保护、恢复和促进可持续利用陆地生态系统；
16. 创建和平包容社会，建立有效、负责、包容的机构；
17. 加强执行手段，促进可持续发展的全球伙伴关系；

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_