

《安全可靠智能云平台能力分级方法》 标准编制说明

标准起草组

2026 年 05 月 27 日

1、 标准范围。

本规范旨在定义安全可信智能云平台能力分级方法，帮助企业明确安全可信智能云平台的综合能力评价体系，从安全可信特性、平台基础能力和性能三个维度构建分级评价框架，涵盖基础资质、设计研发、安全合规、运营保障、生态合作、可持续性等安全可信要求，以及基础环境、基础设施、基础服务、运维与安全等平台能力要求，并明确能力等级定义与等级划分方法。

随着人工智能技术与云计算深度融合，智能云平台已成为数字经济时代的关键基础设施。在技术快速迭代与应用深度拓展的同时，安全、可信、可控、可靠成为智能云服务发展的核心诉求。当前，我国智能云产业发展面临核心技术自主水平不足、安全风险防范体系不完善、产业生态协同性不高等挑战，亟需建立统一、规范的能力分级标准，引导产业健康有序发展。基于自主基础软硬件构建的安全可信智能云平台，以安全可信技术栈兼容、数据安全、模型安全等关键能力为核心，是推动数字政府、金融、能源等关键行业数字化转型的重要支撑。

2、 工作简况。

本项目计划名称为“安全可信智能云平台能力分级方法”。由中国互联网协会归口。由中国信息通信研究院牵头研制。

本文件起草单位包括中国信息通信研究院、阿里云计算有限公司、中国铁塔股份有限公司、中国航空结算有限责任公司、华为云计算技术有限公司、腾讯云计算（北京）有限责任公司、联通数字科技有限公司、上海云轴科技股份有限公司、浪潮云信息技术股份公司、京东云计算有限公司、中移（苏州）软件技术有限公司、天翼云科技有限公司。

本文件主要起草人：姬海南、龚斌、吴子龙、冯毅、孙海骅、王鑫、梁超、白洋洋、韩冬、王石、刘晓军、何波、程维。

本文件于2026年5月在中国互联网协会通过立项申请。

起草组于2026年6月召开线上讨论会，汇报讨论标准的研制情况。会上各企业根据产品的共同需求及差异性进行讨论，对标准中的相关内容提出合理建议，最终形成符合在线文档行业要求的标准文件。

3、 标准编制原则和确定标准主要内容的依据：

编制原则：

- 标准性要求，充分借鉴国内相关标准规范，并结合我国实际情况，力求该标准的可执行性和规范性更强；
- 实用性要求，依据现行法律法规和行业特定需求，明确安全可信智能云平台在安全可信特性与技术能力双维度的评价要求及可信验证机制，建立涵盖基础资质、研发合规、安全运营、生态建设的全要素评价体系，规范平台研发、部署应用、服务保障等全生命周期活动，具有充分的技术先进性和实用性；
- 可行性要求，结合当前主流技术栈和企业技术储备现状，制定分层级、可落地的技术要求；
- 有效性要求，考虑到技术的发展与扩充需求，故全面考虑标准架构和兼容性，满足未来标准发展与扩充需求。

4、 主要试验（或验证）的分析、综述报告。

本标准的技术内容聚焦安全可信智能云平台的全维度能力分级方法构建，经过对各方场景业务及技术方案的调研与分析，通过对各参与方不同平台产品在技术与需求方面的深入讨论，重点就基础设施性能、平台调度性能、AI服务性能等关键指标的分级阈值进行了充分论证，得到了符合行业要求的通用技术文档。最终形成的标准文件得到各参与方的认可和验证，标准可为从事安全可信智能云平台研发、运营及能力评价的各类机构提供参考。

5、 标准在起草过程中遇到的问题及解决办法：重大分歧意见的处

理经过和依据：有无重要技术问题需要说明。

在标准起草过程中遇到的问题通过项目组内部协调和讨论已经解决。无重大分歧意见。没有重要技术问题需要说明。

6、 与国外标准的关系：包括：采用国际标准和国外先进标准的程度，与国外标准主要技术内容的差异（可引用标准前言的内容）：

本标准无对应的国际标准或国外标准。

7、 修订标准时，说明与标准前一版本的重大技术变化，并列出的新、旧版本的有关条款（可引用标准前言的内容）：废止/代替现行有关标准的建议：

本标准为第一版制定标准。

8、 说明标准与其他标准或文件的关系（可引用标准前言的内容），特别是与有关的现行法律、法规和强制性国家标准的关系：

本标准注重与GB/T 46350—2025《信息技术 云计算 智能云服务通用要求》等国家标准的衔接，同时聚焦安全可信特性，强化了安全可信技术栈兼容、数据安全、模型安全等关键能力要求，旨在推动构建安全可信的智能云服务生态。

9、 标准作为强制性标准或推荐性标准的建议：

建议本文件作为推荐性团体标准发布实施。

10、 贯彻国家标准的要求和措施建议（包括组织措施、技术措施、过渡办法等内容）：标准发布后，对国内外业界可能产生的影响。

本标准的发布与实施可协调产业共识，促进行业健康发展，形成产品统一要求和考量，从而为该类产品的未来能力发展和普及奠定技术保障。

11、 标准是否涉及知识产权的情况说明；如标准中含有自主知识产权，说明产品研发程度、产业化基础及进程。

本文件不涉及知识产权的问题。

12、 其他应予说明的事项。

无。