ICS 35. xxx
CCS Lxx

团 体 标 准

T/ISC XXX—XXXX

安全可信中间件能力要求 第 1 部分 总体要求

Requirements for Secure and Trustworthy Middleware Capability Requirements
Part 1: General Requirements

xxxx－xx－xx 发布 xxxx－xx－xx 实施

中 国 互 联 网 协 会 发布

目　　次

前　　言 II
引　　言 III
安全可信中间件能力要求 第1部分 总体要求 1
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
3.1 中间件 middleware 1
3.2 应用 application 1
3.3 消息 message 1
4 符号和缩略语 1
5 安全可信总体要求 2
5.1 基础信息 2
5.2 设计研发 2
5.3 安全合规 2
5.4 运营保障 3
5.5 生态合作 3
5.6 可持续性 3

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。

本文件由中国互联网协会提出并归口。

本文件起草单位：

本文件主要起草人：

——

引　言

随着信息技术的快速发展和数字化转型的深入推进，中间件技术作为软件基础设施的重要组成部分，正被广泛应用于互联网、金融、通信、交通、医疗等多个关键领域，显著提升系统间通信效率，降低系统耦合度，增强数据处理能力，有效提升信息系统的整体性能与稳定性。

安全可信中间件往往基于自主研发的软硬件基础设施，具备高度的自主性与良好的兼容性，能够在复杂的系统环境中平稳运行。尤其针对党政、医疗、金融等对数据安全和系统可靠性要求严苛的行业，安全可信中间件提供了有效的数据安全保障机制，能够防范外部恶意攻击，保障数据的机密性、完整性和可用性，对推动重点行业的数字化转型和保障关键领域信息安全具有重要意义。

本系列标准针对中间件产品研发和行业用户应用过程中所面临的安全风险与挑战，依据现行法律法规和行业特定需求，明确安全可信中间件的技术要求和可信验证机制，建立涵盖基础环境适配、软硬件设施建设、平台功能开发的统一标准体系，规范产品研发、应用部署和服务保障等全生命周期管理活动。通过构建科学合理的安全可信体系指引和产品能力量化评估标准，为产业发展提供有力的技术支撑，促进市场可持续健康发展。本文件针对安全可信中间件总体要求进行规范。

对本文件中的具体事项，法律法规另有规定的，需遵照其规定执行。

安全可信中间件能力要求 第1部分 总体要求

1 范围

本文件规定了安全可信中间件标准体系内各类中间件都需要遵循的安全可信总体要求，涉及企业合法性、产品合规性、研发规范、技术安全、运营服务、生态适配和长期发展等多个维度。

本文件适用于从事安全可信中间件研发、应用及评价的各类机构。

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 33847—2017 信息技术 中间件术语

GB/T 28168—2025 信息技术 中间件 消息中间件技术规范

3 术语和定义

GB/T 33847—2017、GB/T 28168—2025界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 33847—2017、GB/T 28168—2025中的某些术语和定义。

3.1

中间件 middleware

位于系统软件之上，用于支持分布式应用软件，连接不同软件实体的支撑软件（2.1）。

[来源：GB/T 33847—2017，2.1]

3.2

应用 application

应用程序

通过调用开发接口，在运行过程中使用中间件系统提供功能和服务的各种程序（3.1.1）。

[来源：GB/T 28168—2025，3.1.1]

3.3

消息 message

不同的应用程序(进程或线程)之间传递或交换的信息。

注：消息的格式及内容，由该消息的提供者及接收者协商而定

[来源：GB/T 28168—2025，3.1.2]

4 符号和缩略语

下列符号和缩略语适用于本文件。

SBOM： 软件物料清单（Software Bill of Materials）

5 安全可信总体要求

5.1 基础信息

5.1.1 企业资质

企业指安全可信中间件或解决方案提供组织。

a) 组织应为在中华人民共和国境内注册的企业法人或事业法人，应能够提供真实有效的法人资质证明文件，企业成立36个月以上，企业组织机构代码证经营范围覆盖申请产品。
b) 组织最高管理者，如法定代表人、主要负责人、实际控制人、董（监）事会人员、公司高层管理人员，应具有中华人民共和国国籍。
c) 组织的资本构成应符合通过间接方式投资的外方投资者及其一致行动人的出资比例最终不超过20%。
d) 组织应具有一定年限的相关产品研发及制造经验，能够提供连续近3年（自然年）的产品认证证书、出货记录、订购合同、发票、设计开发资料等证明材料。

5.1.2 产品信息

a）应具备产品相关软件著作权或专利证书（已在国家知识产权局备案）等知识产权证明材料。
b）应具备安全可信环境下的适配测试报告（内容涵盖产品主要功能和基础性能）。

5.2 设计研发

5.2.1 研发团队

a) 应具备不少于100人规模的自有研发团队，核心成员应具备3年以上安全可信相关经验。

5.2.2 研发管理

a) 应具备覆盖需求分析、设计、开发、测试、发布的全生命周期研发管理体系。
b) 宜采用安全可信的代码签名工具，确保发布包完整性与来源可信性。
c) 应实现安全测试全生命周期覆盖，包括静态代码扫描、动态渗透测试及模糊测试，并提供测试报告。

5.2.3 环境配套

a) 应至少具备2套基于不同芯片基础架构的安全可信技术栈环境，用于产品的兼容性测试。
b) 测试环境应年度更新至主流安全可信生态最新版本。

5.3 安全合规

5.3.1 安全管理

a) 应建立安全事件分级响应机制，明确高危事件（如数据泄露）的处置流程与时限。
b) 宜建立威胁情报共享机制，实时同步行业最新漏洞信息。

5.3.2 技术合规

a) 应提供核心技术自主研发声明，以及无境外知识产权纠纷的声明文件。

b） 如涉及开源组件，应建立开源组件白名单，并明确记录所引入开源代码的来源，做好许可证风险管理。
c） 应支持数据本地化存储，确保用户数据仅存储在可控数据中心。

5.4 运营保障

5.4.1 服务保障

a） 应提供7×24小时技术支持服务，一般问题响应时间应不超过4小时，问题解决时间不超过8小时。
b） 应提供政企客户上门服务保障（提供声明文件）。
c） 应提供产品使用培训及典型问题解决说明材料。

5.5 生态合作

5.5.1 生态适配

a） 应兼容至少2家主流安全可信技术栈。
b） 宜通过权威机构组织的生态适配认证。

5.5.2 生态共建

a） 应为信创相关生态平台或组织的成员单位，并参与推进信创生态建设。
b） 宜加入至少1个国内开源社区，并贡献代码或文档。
c） 宜参与安全可信相关标准制定，年度参与数量不少于2项。
d） 宜参与开源社区漏洞众测计划，主动公开修复方案并提交漏洞库备案。

5.6 可持续性

5.6.1 可持续发展

a） 年度研发费用占比应不少于15%。
b） 应具备产品版本迭代计划，年度至少发布2版次主版本更新。
c） 应具有核心技术演进路线图，确保3年内关键技术全部实现安全可信。
d） 应承诺产品支持周期不低于5年（主要指产品安全更新、主版本更新等）。
e） 宜建立代码混淆与防逆向工程机制，保护核心算法与知识产权。