团体标准编制说明

一、项目背景

信创应用中，微型计算机存储了大量工作数据，这些数据通常都有保密要求。例如，标准《GB/T 30278-2024 信息安全技术 政务计算机终端核心配置规》中“6.1.4 数据保密性”规定，“应配置硬盘访问口令”、“应配置硬盘加密功能”。

目前，国内微型计算机有一系列的国家标准或者团体标准，如下所列，但都没有给出微型计算机数据存储安全的技术要求。这就导致信创应用难以根据现有标准为数据存储安全功能给出具体的技术要求。

(1) GB/T 9813.1-2016 计算机通用规范第 1 部分 台式微型计算机。

(2) GB/T 9813.2-2016 计算机通用规范第 2 部分 便携式微型计算机。

(3) GB/T 29240-2024 网络安全技术 终端计算机通用安全技术规范。

(4) GBT 30278-2024 信息安全技术 政务计算机终端核心配置规范。

(5) T/ZXCH 0030—2023 信息技术应用创新工作规范 微型计算机通用性要求：2024 年 1 月 2 日公布。

国际上,可信计算组织(Trusted Computing Group, TCG)制定了数据安全标准规范 TCG Opal，定义了对静态数据保护的安全策略，包括基于先进加密标准(Advanced Encryption Standard，AES)的自加密硬盘（SEDSelf-Encrypting Drive，SED）、用户权限管理、开机前身份验证等，实现了硬盘数据的自加密/解密。因此硬盘厂商通常都推出支持 AES 加/解密功能的硬盘。TCG Opal 标准体系基于 AES、面向硬盘的数据自加密，且涉及国际/国外知识产权的处理，因此并不适合于中国信创应用。

同时，与 AES 算法类似，我国已经有成熟的分组密码算法 SM4(GB/T 32907《信息安全技术 SM4 分组密码算法》)，并在数据加解密领域大量应用。目前，国内尚未发现有标准明确规定采用 SM4 加解密算法对硬盘数据加密。

因此，基于 SM4 分组密码算法，为微型计算机制定数据存储安全技术要求，这将从数据存储的角度有效阻断数据泄密的路径，从而保障数据的存储安全。

二、工作简况

2024 年 12 月 5 日,杭州市商用密码协会和信创保障中心邀请了华澜微、华为、新华三、海康、大华等五家企业召开了本标准的编制合作意向会。会上，与会单位一起讨论并修订了华澜微提交的“信创标准编制计划（初稿）”，

确定了标准名称为“信息技术应用创新工作规范 微型计算机存储安全技术要求”（暂定）、编制编制组长单位是华澜微、副组长单位是华为与海康（暂定）。

2024 年 12 月 19 日，华澜微邀请各参编单位一起召开本标准编制的启动会。会上，各参编单位讨论了华澜微提交的编制编制计划、标准草案初稿，并安排了下一步工作。

2025 年 1 月 7 日，标准编制组召开第二次会议，逐条讨论《草案初稿反馈汇总及答复》中的内容，对标准核心内容达成了统一理解；同时，安排了下一步工作。

2025 年 1 月 10 日，华澜微提交了正式标准草案 D1.0；1 月底、2 月初，各参编单位都提交了草案 D1.0 的反馈意见。

2025 年 2 月 13 日，标准编制组召开第三次会议，逐条讨论《草案 D1.0 反馈汇总与讨论结果》中的内容，对标准核心内容达成了共识。同时，会上明确华为、海康负责编写本标准的“试验方法”部分，并安排了下一步工作（如下）。

此后，草案经历了如下修改过程：

- 3 月 13 日，标准编制组召集会议讨论了草案 D2.0；
- 4 月 8 日，标准编制组召集会议讨论了草案 D2.1；
- 4 月 15 日,形成了草案 D3.0,提交编制组内部审查，并于 5 月 6 日通过了编制组全体成员的审查；

- 6 月 16 日，编制组收到了杭州市信息化管理中心的审查建议，经修订于 6 月 20 日形成了草案 D3.2；
- 8 月 20 日，因编制组调整，形成了草案 D3.3；
- 9 月 2 日，浙江省电子信息产品检验研究院组织了团体标准立项论证会；听取了专家建议，经过修订形成了草案 D3.5,即征求意见稿。

根据 2025 年 9 月 2 日的团体标准立项论证会与当前的实际进展，本标准的总体计划目标如下：

(1) 团体标准备案： 2024/12 -- 2025/8

(2) 标准立项： 2024/12 -- 2025/8

(3) 组建工作组： 2024/12 -- 2025/1

(4) 标准编写/讨论： 2025/1 -- 2025/7

(5) 征求意见阶段： 2025/8 -- 2025/9

(6) 送审阶段： 2025/9 -- 2025/10

(7) 标准报批阶段： 2025/10

三、标准编制原则和主要内容的依据

（一）编制原则

本标准按照 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，符合国家规定的标准制定的要求。

同时，本标准完成后要求在实现与市场应用方面均可落地。

（二）编制依据

本标准主要依据如下现行国内标准制定。

(1) GB/T 9813.1-2016 计算机通用规范 第 1 部分：台式微型计算机

(2) GB/T 9813.2-2016 计算机通用规范 第 2 部分：便携式微型计算机

(3) GB/T 29240-2024 网络安全技术 终端计算机通用安全技术规范

(4) GB/T 30278-2024 信息安全技术 政务计算机终端核心配置规范

(5) GB 42250-2022 信息安全技术 网络安全专用产品安全技术要求

(6) GB/T 12628-2008 硬磁盘驱动器通用规范

(7) SJ/T 11654-2016 固态盘通用规范

(8) GB/T 32907-2016 信息安全技术 SM4 分组密码算法

(9) GM/T 0008-2012 安全芯片密码检测准则

(10) GB/T 37092-2018 信息安全技术 密码模块安全

要求

(11) GB/T 17964-2021 信息安全技术 分组密码算法的工作模式

(12) GB/T 38626-2020 信息安全技术 智能联网设备口令保护指南

（三）主要内容

标准的主要技术内容：

(1) 核心部件的全国产化：包括 CPU 及周边接口芯片、操作系统、固态硬盘（主控与颗粒）。

(2) 数据的加密防护功能：

- ✓ 要求采用符合国家标准 GB/T 32907-2016 的 SM4 分组密码算法，并获得中国商用密码认证。
- ✓ 要求采用国产化的加/解密安全芯片或密码模块，包括但不限于安全加密 CPU、安全加密接口芯片、安全加密硬盘主控芯片，实现对硬盘数据的加密和解密。

(3) 数据的访问控制功能，实现对数据访问的安全防护。

(4) 符合存储安全保障要求。

（四）解决的主要问题

计算机系统、通信网络都存在安全漏洞，暴露在网络中的终端计算机容易受到安全攻击，导致用户数据被非法入侵或盗取。

本标准期望解决的主要问题是：从数据存储的角度有效阻断数据泄密的路径，建立信创应用“数据护城河”，从而保障数据的存储安全。例如微型计算机的硬盘数据“他人找不到”、“非法获得的数据不可读”。

四、主要试验（或验证）情况分析

本标准的核心内容是要求微型计算机实现可管可控的硬盘数据加密/解密功能，实现数据存储的安全防护。因此，试验方法将主要从如下几个方面开展：

- SM4 分组密码算法的认证：SM4 密码算法可以采用安全芯片、密码模块、或软件模块等多种方式实现，本标准要求通过商密认证来验证 SM4 算法的正确性。
- 可管可控的数据访问控制：本标准的目的是阻断非法获取数据的路径，本标准要求检验合法访问的数据正确性、非法访问数据时数据必须无效或乱码。
- 存储安全保障的确认：本标准要求通过检查相关硬件的国产化情况验证是否符合安全保障的要求。

五、标准中涉及专利的情况

暂无。

六、产业化情况、推广应用论证和预期达到的经济效果

本标准是现行微型计算机技术标准的补充，不是一个独立的 IT 设备标准；其核心内容是要求微型计算机采用中国 SM4 分组密码算法对硬盘数据进行芯片级的数据加/解密、对数据实施访问控制，使得微型计算机具备有效的数据存储安全防护能力。因此，其产业化过程应该是新型号信创应用微型计算机整机的产业化过程，通常不需要单独开展数据存储安全防护功能的产业化。

信创应用中，微型计算机存储了大量的工作数据，这些数据通常都有保密要求。数据存储安全防护功能弥补了现行信创应用微型计算机中数据安全功能的不足，有效阻断了非法获取数据的路径。因此，本标准规定的存储安全技术是信创应用微型计算机的一个增值功能，将有效促进微型计算机的市场推广应用。

作为一个增值功能，本标准制定的硬盘数据存储的安全技术，将会持续促进微型计算机在信创应用的市场应用，有力于提升信创应用微型计算机的业务收入。

七、与现行相关法律、法规、规章及相关标准的关系

目前，国内微型计算机的国家标准或团体标准（如下列表）都不涉及数据存储安全的技术要求。本标准是对这些国内标准在存储安全方面的技术补充，是这些国内标准

没有涉及部分的明确规定。

(1) GB/T 9813.1-2016 计算机通用规范第 1 部分 台式微型计算机。

(2) GB/T 9813.2-2016 计算机通用规范第 2 部分 便携式微型计算机。

(3) GB/T 29240-2024 网络安全技术 终端计算机通用安全技术规范：2025 年 5 月 1 日实施。

(4) GBT 30278-2024 信息安全技术 政务计算机终端核心配置规范。

(5) T/ZXCH 0030—2023 信息技术应用创新工作规范 微型计算机通用性要求。

同时，国内标准在数据加密/解密技术领域有如下标准。其中标准《GB/T 32907-2016 信息安全技术 SM4 分组密码算法》是本标准采用的数据加密/解密的密码算法标准，它是本标准的基础；其他标准也将在本标准中引用。

(1) GB/T 32907-2016 信息安全技术 SM4 分组密码算法

(2) GM/T 0008-2012 安全芯片密码检测准则

(3) GB/T 37092-2018 信息安全技术 密码模块安全要求

(4) GB/T 17964-2021 信息安全技术 分组密码算法的工作模式

八、重大意见分歧的处理依据和结果

标准制定过程中，当遇到重大意见分歧时，本标准编制组的处理依据如下：

(1) 查询和研究现有国内标准、国际标准，并以此为基础开展充分讨论；

(2) 调研行业内相关或类似的应用、技术或产品，并以此为基础开展充分讨论；

(3) 咨询行业技术专家、主流厂商，从技术、产品角度开展充分讨论；

(4) 调研行业内主要客户，从应用角度开展充分讨论。

基于上述的充分讨论，形成一个统一建议，然后提交标准编制组投票表决。以编制组的表决结果作为重大意见分歧的最终处理结果。

九、贯彻标准的要求和措施建议

本标准是对现行国内微型计算机的国家标准或团体标准在数据存储安全方面的技术补充，有效阻断了非法获取数据的路径，解决了信创应用中数据存储缺少安全防护这个痛点。

为了弥补现行国内微型计算机的国家标准或团体标准的技术缺失，本标准发布后必须在信创应用领域开展贯标，

提高信创用户在数据存储安全方面的认识，从而推动本标准的落地与大规模应用。

本标准的贯标措施有如下建议：

(1) 基于标准内容，编写贯标材料，邀请信创用户，分区域开展贯标宣传会议；

(2) 联合信创行业，将本标准的内容纳入行业应用的优选或必选或可选技术要求；

(3) 联合主要的信创应用微型计算机厂商，对本标准的应用达成行业共识。

十、其他应予说明的事项

无。

《信息技术应用创新工作规范 微型计算机存储安全技术要求》标准起草组

2025 年 9 月 15 日