ICS 35.xxx
CCS xxx

团　　体　　标　　准

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

Work specification for the application innovation of information technology - Storage security technical requirements of microcomputers

（征求意见稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

目　录

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这些专利的责任。

本文件由X提出。

本文件由X归口。

本文件主要起草单位：X。

本文件主要起草人：。

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

1 范围

本文件规定了信息技术应用创新工作规范中微型计算机的存储安全技术要求。存储安全技术包括存储安全功能和存储安全保障，存储安全功能是指微型计算机对指定硬盘中的数据区有加密/解密、访问控制等安全防护能力；存储安全保障是指具有存储安全功能的微型计算机须符合 GB 42250 规定的安全保障要求，包括供应链安全、设计与开发、生产和交付、运维服务保障、用户信息保护等。

本文件中，微型计算机应符合标准 GB/T 9813.1《计算机通用规范 第 1 部分：台式微型计算机》、GB/T 9813.2《计算机通用规范 第 2 部分：便携式微型计算机》。

本文件中，微型计算机核心配置应符合 GB/T 30278《信息安全技术 政务计算机终端核心配置规范》，以满足信息技术应用创新工作的要求。

本文件适用于信息技术应用创新工作推进过程中微型计算机的设计、制造、测评和采购选型。

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 9813.1-2016 计算机通用规范 第 1 部分：台式微型计算机

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

GB/T 29240-2024 网络安全技术 终端计算机通用安全技术规范

GB/T 30278-2024 信息安全技术 政务计算机终端核心配置规范

GB 42250-2022 信息安全技术 网络安全专用产品安全技术要求

GB/T 12628-2008 硬磁盘驱动器通用规范

SJ/T 11654-2016 固态盘通用规范

GB/T 32907-2016 信息安全技术 SM4 分组密码算法

GM/T 0008-2012 安全芯片密码检测准则

GB/T 37092-2018 信息安全技术 密码模块安全要求

GB/T 17964-2021 信息安全技术 分组密码算法的工作模式

GB/T 38626-2020 信息安全技术 智能联网设备口令保护指南

3 术语和定义

GB/T 9813.1、GBT 9813.2 界定的以及下列术语和定义适用于本文件。

3.1

微型计算机 Microcomputer

本文件中，是指台式微型计算机（如GB/T 9813.1定义）、便携式微型计算机（如GB/T 9813.2定义），也称为终端计算机（如GB/T 29240定义）。

信息技术应用创新工作中，微型计算机核心配置应符合GB/T 30278《信息安全技术 政务计算机终端核心配置规范》。

3.2

存储设备 storage device

本文件中，是指应用于微型计算机的固态盘（SSD）、硬磁盘（HDD），统称为硬盘；其中，固态盘可采用UFS、SATA、PCIe/NVMe、SAS等接口类型；硬磁盘可采用SATA、SAS等接口类型。

3.3

存储安全 storage security

本文件中，是指微型计算机的存储安全功能和存储安全保障，以符合国家标准GB/T 29240-2024中安全技术的定义。

存储安全功能是指微型计算机对指定硬盘中的数据区有加密/解密、访问控制等安全防护能力，满足信息技术应用创新工作中信息安全要求。

存储安全保障是指具有存储安全功能的微型计算机须符合GB 42250规定的安全保障要求，包括供应链安全、设计与开发、生产和交付、运维服务保障、用户信息保护等，满足信息技术应用创新工作中供应链安全要求。

3.4

存储安全 App storage security management application

本文件中，是指微型计算机存储安全防护功能的管理模块（management module）或管理软件（management software）。

3.5

系统盘 system drive

是指微型计算机中安装了操作系统的逻辑盘。它可以是一个独立的物理盘，也可以是一个物理盘的硬盘分区。

通常，系统盘主要用于安装操作系统、各种应用软件，也可用于保存数据。

3.6

工作盘 work drive

本文件中，是指微型计算机中没有安装操作系统且用于存储工作数据的逻辑盘。它可以是一个独立的物理盘，也可以是一个物理盘的硬盘分区。。

通常，工作盘主要用于存储工作数据。

3.7

工作区 work zone

本文件中，是指微型计算机中，用于存储工作数据的硬盘逻辑区域。它可以是一个独立的逻辑盘，也可以是逻辑盘中的工作目录。

3.8

安全工作区 security work zone

本文件中，是指微型计算机中开启了存储安全功能的工作区。

信息技术应用创新工作中，微型计算机的安全工作区应满足 GB/T 30278《信息安全技术 政务计算机终端核心配置规范》中“6.1.4 数据保密性”的安全功能要求。

3.9

移动存储设备 portable storage device

是指 USB 闪存盘、USB 接口移动硬盘、存储卡，它们可以通过微型计算机的 USB 接口或存储卡接口等便捷地使用。

3.10

存储介质 storage media

是指用于存储信息的物理载体。存储介质主要包括电存储介质（例如与非闪存（NAND Flash））、磁存储介质（例如磁片、磁带）、光存储介质（例如光盘）等。

3.11

硬盘控制器 drive controller

是指硬盘的控制单元，用于管理、控制、维护硬盘的存储介质，提供数据的读取、写入、管理维护等基础功能。

3.12

安全芯片 security chip

是指含有密码算法、安全功能，可实现密钥管理机制的集成电路芯片，遵循 GM/T 0008 定义。

3.13

密码模块 cryptographic module

是指实现了密码算法与安全功能的硬件、软件和/或固件的集合，遵循 GB/T 37092 定义。根据其组成，密码模块可分为硬件密码模块、固件密码模块、软件密码模块以及混合密码模块。

3.14

安全等级 security level

是指安全芯片和密码模块的安全防护能力等级。对于安全芯片，GM/T 0008《安全芯片密码检测准则》定义了三个安全等级，分别是安全等级 1、安全等级 2、安全等级 3。对于密码模块，GB/T 37092 《信息安全技术 密码模块安全要求》定义了四个安全等级，分别是安全一级、安全二级、安全三级、安全四级。

本文件中，基于信息技术应用创新工作的信息安全要求，安全等级统一采用安全一级、安全二级、安全三级、安全四级。

3.15

分组密码算法工作模式 block cipher operation mode

是指分组密码算法的工作方式，主要包括电码本工作模式（ECB）、密文分组链接工作模式（CBC）、密文反馈工作模式（CFB）、输出反馈工作模式（OFB）、计数器工作模式（CTR）、带密文挪用的 XEX 可调分组密码工作模式（XTS）、带泛杂凑函数的计数器工作模式（HCTR）、分组链接工作模式（BC）、带非线性函数的输出反馈工作模式（OFBNLF）等，遵循标准 GB/T 17964 的定义。

3.16

测试文件的专用工具 software tool for particular test file

是指用于打开测试文件的专用软件工具，它至少支持编辑、保存、另存为等常规操作。

4 符号和缩略语

下列缩略语适用于本文件。

- CPU：Central Processing Unit 中央处理器
- BIOS：Basic Input Output System 基本输入输出系统
- HDD：Hard Disk Drive 硬磁盘
- SSD：Solid State Drive 固态盘
- SATA：Serial ATA 串行 ATA 接口
- PCIe：Peripheral Component Interconnect Express 高速串行计算机扩展总线
- NVMe：Non-Volatile Memory Express 高速非易失存储
- SAS： Serial Attached SCSI 串行连接 SCSI 接口
- UFS：Universal Flash Storage 通用闪存存储
- USB：Universal Serial Bus 通用串行总线
- ECB：Electronic Codebook 电码本
- CBC：Cipher Block Chaining 密码分组链接
- CTR：Counter 计数器
- XEX：Xor-Encryption-Xor 异或-加密-异或
- XTS：XEX tweakable block cipher with ciphertext stealing 带密文挪用的 XEX 可调分组密码

5 技术要求

5.1 设计要求

5.1.1 硬件要求

本文件中，微型计算机的存储安全功能在安全工作区中实现，其相关硬件主要包括存储设备、安全芯片、硬件密码模块。

5.1.1.1 微型计算机支持存储安全功能时，宜采用支持数据加密/解密功能的硬盘，用于实现数据加密/解密功能。

5.1.1.2 当硬盘支持数据加密/解密功能时，数据加密/解密功能宜集成在硬盘控制器中，如图 5.1 所示。

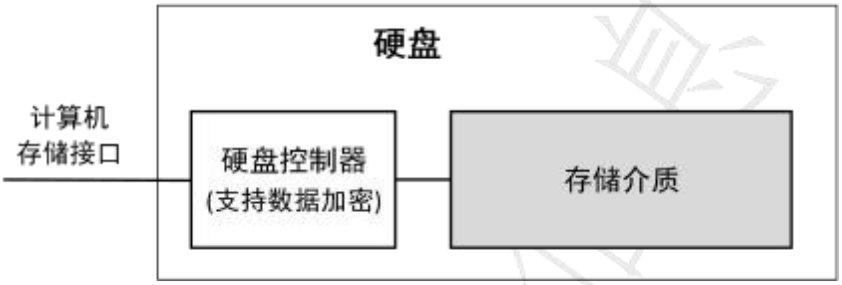

图 5.1 支持数据加密功能的硬盘示意图

5.1.1.3 微型计算机支持存储安全功能时，可选采用硬件密码模块，用于实现数据加密/解密功能。

示例：如图 5.2 所示，微型计算机在计算机存储接口上采用硬件加密模块以实现数据加密/解密功能，其中计算机存储接口可以是 PCIe、SATA、SAS、UFS 等。

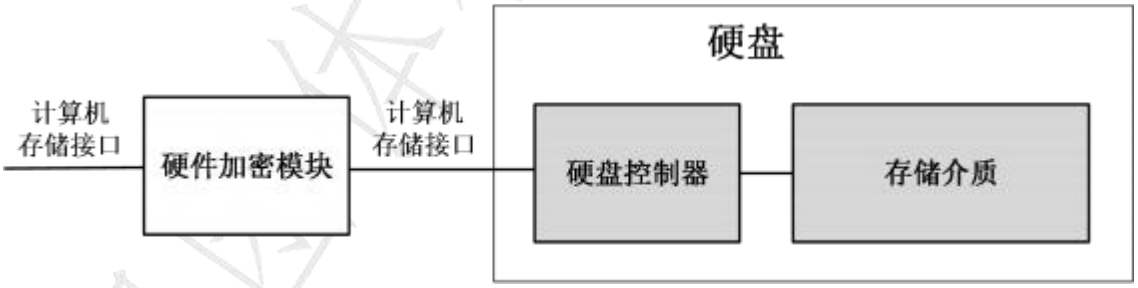

图5.2 采用硬件加密模块实现硬盘数据加密/解密

5.1.1.4 微型计算机支持存储安全功能时，可选采用支持加密/解密功能的中央处理器（CPU），用于实现数据加密/解密功能。

本文件中，支持数据加密/解密功能的硬盘控制器、硬件密码模块中的安全加密控制器、支持加密/解密功能的中央处理器（CPU）等都具有安全芯片的功能，统称为安全芯片。

5.1.2 软件要求

本文件中，存储安全功能的软件要求是指微型计算机管理与维护安全工作区的软件要求。

5.1.2.1 微型计算机支持存储安全功能时，宜支持存储安全 App，用来管理与维护安全工作区，并具有如下能力：

(1) 支持安全工作区的用户身份认证功能，具体参见 5.1.2.2 与 5.2.2.1；

(2) 支持解锁与锁定安全工作区，具体功能参见 5.2.2.3；

(3) 可选支持创建与删除安全工作区，具体功能参见 5.2.2.2。

5.1.2.2 存储安全 App 宜支持用户身份认证机制，其中用户身份认证的登录口令应符合 GB/T 38626-2020 第 7 节的要求。只有通过了身份认证，用户才能通过存储安全 App 管理与维护安全工作区。

5.1.2.3 存储安全 App 的用户身份认证功能宜具有防暴力破解登录口令的能力；如果错误登录尝试超过设定次数，则在预先设定的锁定时间内锁定登录账号的操作。

防暴力破解登录口令的示例：在连续 5 次登录口令错误后，存储安全 App 至少在 15 分钟内不接受新输入的登录口令。

5.2 功能和性能要求

本文件中，微型计算机采用安全工作区来定义和实现存储安全功能，为信息技术应用创新工作提供数据存储的信息安全防护能力。

5.2.1 安全工作区的数据加密/解密功能

5.2.1.1 微型计算机支持存储安全功能时，安全工作区宜采用安全芯片或硬件密码模块，可选采用软件密码模块或混合密码模块，用以实现数据加密/解密功能。

5.2.1.2 安全工作区的数据加密/解密功能宜采用 SM4 分组密码算法，遵循标准 GB/T 32907-2016。

5.2.1.3 安全工作区的数据加密/解密功能宜至少支持国家标准 GB/T 17964-2021 中 ECB 和 CBC 这两种工作模式，可选支持 XTS、CTR、OFB 或其他工作模式。

5.2.1.4 当安全工作区采用安全芯片实现数据加密/解密功能时，安全芯片宜通过商用密码产品认证，且至少符合标准 GMT 0008-2012 中安全一级（即安全等级 1）的要求。

5.2.1.5 当安全工作区采用密码模块实现数据加密/解密功能时，密码模块宜通过商用密码产品认证，且至少符合标准 GB/T 37092-2018 中安全一级的要求。

5.2.1.6 当安全工作区采用整机综合方式实现数据加密/解密功能时，微型计算机宜以整机方式通过商用密码产品认证，且至少符合标准 GB/T 37092-2018 中安全一级的要求。

5.2.2 安全工作区的访问控制功能

5.2.2.1 当微型计算机支持存储安全功能时，安全工作区宜在存储安全 App 协同下支持用户身份认证。

5.2.2.2 安全工作区可选支持创建、删除功能。创建之后，安全工作区才能用于保存工作数据；删除之后，安全工作区将不可访问。

5.2.2.3 安全工作区宜支持锁定、解锁功能，用来实现安全工作区的访问控制，至少要求如下：

(1) 安全工作区被锁定后，安全工作区不可访问，即微型计算机的文件系统无法访问安全工作区；

(2) 安全工作区被解锁后，安全工作区可访问，即微型计算机的文件系统能正常访问安全工作区及其工作数据；

(3) 解锁和锁定安全工作区时，安全工作区应确保用户身份认证正确，以保证管理安全。

5.2.2.4 安全工作区在如下情况宜被自动锁定：

(1) 微型计算机上电重启后；

(2) 存储安全App 退出登录后；

(3) 存储安全App 退出运行后；

(4) 如果安全工作区是通过创建方式产生，则安全工作区创建后，默认是锁定状态。

5.2.2.5 当一台微型计算机（简称归属主机）支持存储安全功能时，因特殊原因，其安全工作区迁移到其他微型计算机（简称迁移主机）后，安全工作区宜支持如下能力：

(1) 默认情况下，迁移主机中的安全工作区应处于锁定状态；

(2) 如果迁移主机与归属主机具有完全相同的存储安全功能，则迁移主机宜能使用归属主机的登录口令完成存储安全 App 的用户身份认证，实现对安全工作区的锁定、解锁功能。

5.2.2.6 微型计算机支持存储安全功能时，安全工作区所在物理硬盘宜支持安全的固件升级功能，即硬盘固件升级后应保证硬盘中工作数据没有被篡改、且能正常执行存储安全功能。

5.2.3 存储安全的性能

存储安全的性能是指微型计算机中安全工作区的数据读写性能，主要包括顺序读写速度、随机读写速度。

5.2.3.1 微型计算机开启存储安全功能后，安全工作区的数据读写速度宜不低于未开启存储安全防护功能时的 60%。

5.3 安全保障要求

5.3.1 信息技术应用创新工作中，当微型计算机采用安全芯片实现数据加密/解密功能时，安全芯片宜有《电子元器件自主可控等级评估报告》或厂家的国产自主可控承诺书，保证微型计算机存储设备的供应链安全。

5.3.2 信息技术应用创新工作中，当微型计算机采用固态盘存储工作数据时，固态盘宜有《电子元器件选用分析报告》，确保固态盘的国产化率符合信息技术应用创新工作的要求。

5.3.3 信息技术应用创新工作中，当微型计算机采用固态盘存储工作数据时，固态盘宜通过与指定微型计算机的国产处理器、国产 BIOS、以及国产操作系统的产品兼容性认证，保证微型计算机存储设备的供应链安全。

6 试验方法

本文件仅对微型计算机的存储安全防护功能规定试验方法。除此之外，微型计算机的整机试验方法应符合 GB/T 9813.1、GB/T 9813.2、GB/T 30278 的相关规定，以满足信息技术应用创新工作的要求。

6.1 试验环境

6.1.1 试验条件

未加特殊说明时，本文件的所有测试项都应在微型计算机的整机试验条件下执行，符合 GB/T 9813.1-2016、GB/T 9813.2-2016 的相关规定。

6.1.2 硬件环境

未加特殊说明时，本文件的所有测试项都应在微型计算机的整机硬件系统中执行，符合 GB/T 9813.1-2016、GB/T 9813.2-2016 的相关规定。

6.1.3 软件环境

未加特殊说明时，本文件的所有测试项都应在微型计算机的整机软件系统中执行，至少包括操作系统、存储安全 App、存储设备的测试软件工具、测试文件的专用工具。

6.1.4 测试项的预置条件

每一个测试项都应该在明确的预置条件下进行。

本文件设置了如下几种预置条件：

- 预置条件#1：
  (1) 被测微型计算机能正常工作；
  (2) 被测微型计算机中，没有安全工作区；
  (3) 被测微型计算机中，存储安全 App 已运行并成功登录。
- 预置条件#2：
  (1) 被测微型计算机能正常工作；
  (2) 被测微型计算机中，已有安全工作区；
  (3) 安全工作区已有一个测试文件 A，大小不低于 10MB；
  (4) 被测微型计算机中，存储安全 App 已运行并成功登录。
- 预置条件#2A：
  (1) 被测微型计算机能正常工作；
  (2) 被测微型计算机中，已有安全工作区；
  (3) 被测微型计算机中，普通工作区已有一个测试文件 A，大小不低于 10MB；
  (4) 被测微型计算机中，存储安全 App 已运行并成功登录。
- 预置条件#3：
  (1) 被测微型计算机能正常工作；
  (2) 被测微型计算机中，已有安全工作区；
  (3) 安全工作区已有一个测试文件 A，大小不低于 10MB；
  (4) 被测微型计算机中，存储安全 App 已运行但未登录、或者存储安全 App 未运行、或者被测计算机重启后。
- 预置条件#4：
  (1) 被测微型计算机A能正常工作；
  (2) 被测微型计算机A中，参测硬盘上已有安全工作区；
  (3) 参测硬盘中安全工作区已保存了一个测试文件A，大小不低于10MB；

(4) 被测微型计算机A中，存储安全App已运行并成功登录；

(5) 被测微型计算机B能正常工作，且与被测微型计算机A具有完全相同的存储安全防护功能；

(6) 被测微型计算机B中，存储安全App已运行并成功登录。

- 预置条件#5：

(1) 被测微型计算机能正常工作；

(2) 被测微型计算机中，参测硬盘上没有安全工作区；

(3) 被测微型计算机中，存储安全App已安装并能正常执行；

(4) 被测微型计算机中，硬盘读写性能测试工具（例如CDM、IOmeter、Fio）已安装并能正常执行。

- 预置条件#6：

(1) 被测微型计算机能正常工作；

(2) 被测微型计算机中，安全存储 App 已经安装但没有运行。

6.2 安全工作区的数据加密/解密功能的认证检查

针对安全工作区的数据加密/解密功能，检查被测微型计算机的商用密码产品认证情况，具体要求如下：

(1) 当微型计算机采用安全芯片实现数据加密/解密功能时，检查安全芯片的商用密码产品认证证书及其检测报告，要求至少符合标准 GM/T 0008-2012 中安全一级（即安全等级 1）。

(2) 当微型计算机采用密码模块实现数据加密/解密功能时，检查被测微型计算机的密码模块的商用密码产品认证证书及其检测报告，要求至少符合标准 GB/T 37092-2018 中安全一级。

(3) 当微型计算机采用整机综合方式实现数据加密/解密功能时，检查被测微型计算机的整机商用密码产品认证证书及其检测报告，要求至少符合标准 GB/T 37092-2018 中安全一级。

6.3 安全工作区的访问控制功能测试

6.3.1 安全工作区的用户身份认证

安全工作区的用户身份认证即存储安全 App 的用户认证，具体测试要求如下。

6.3.1.1 存储安全 App 的用户登录口令设置及安全性检查

本测试项目按以下预置条件和测试步骤执行。

1) 预置条件：采用预置条件#6。

2) 测试步骤：

(1) 首次运行存储安全App，它会检测到没有用户的登录口令，然后要求用户设置登录口令；

(2) 用户输入不符合规定的登录口令，确认设置操作；

(3) 重复测试步骤（2）四次，合计五种不合格的登录口令；

(4) 用户输入符合规定的登录口令，确认设置操作。

3) 预期结果：

(1) 登录口令的密码复杂度要求如下：

① 密码长度至少8个字符，不超过64个字符；

② 密码必须包含如下至少两种字符的组合:

- ✓ 至少一个小写字母;
- ✓ 至少一个大写字母;
- ✓ 至少一个数字;
- ✓ 至少一个特殊字符:`~!@#$%^&*()-_=+\|[{}];:'",<.>/? 和空格。

(2) 上述测试步骤（2）与（3）中，采用五种典型的不合规的密码设置登录口令，存储安全 App给出登录口令设置失败的具体警示，并要求重新设置;

(3) 上述测试步骤（4）中，存储安全 App 给出登录口令设置成功的提示。

4) 结果判定:

实际测试结果与上述预期结果一致，则判定为符合；其他情况判定为不符。

6.3.1.2 存储安全 App 的用户身份认证

本测试项目按以下预置条件和测试步骤执行。

1) 预置条件：采用预置条件#6。

2) 测试步骤:

(1) 运行存储安全App;

(2) 输入正确的用户登录口令进行认证。

3) 预期结果:

成功进入存储安全 App 的管理维护界面。

4) 结果判定:

实际测试结果与上述预期结果一致，则判定为符合；其他情况判定为不符。

6.3.1.3 存储安全 App 的用户登录口令防暴力破解

本测试项目按以下预置条件和测试步骤执行。

1) 预置条件：采用预置条件#6。

2) 测试步骤:

(1) 运行存储安全App;

(2) 以错误登录尝试N次、锁定时间m小时为例，连续N次输入错误的登录口令，每次登录失败后都给出提示信息，例如“登录口令错误，登录失败！”;

(3) 第N次登录失败后，在m小时内第N+1次输入登录口令（无论正确还是错误口），存储安全App拒绝登录认证，并给出警告信息，例如“连续登录失败N次，用户登录已被锁定，m小时后再尝试登录！”。

3) 预期结果:

如上述测试步骤（2）和（3）。

4) 结果判定:

实际测试结果与上述预期结果一致，则判定为符合；其他情况判定为不符。

6.3.2 安全工作区的管理

6.3.2.1 创建安全工作区

当安全工作区支持创建功能时，本测试项目按以下预置条件和测试步骤执行。

1) 预置条件：采用预置条件#1。

2) 测试步骤：

(1) 在存储安全 App 中，选择“创建安全工作区”、选择参测硬盘中的指定工作区为安全工作区（其大小不低于 1GB）、 设置安全工作区名称，确认创建操作；

(2) 在存储安全 App 中，查看已创建的安全工作区的状态。

3) 预期结果：

(1) 在上述测试步骤（1），存储安全 App 给出安全工作区创建成功的提示。

(2) 在上述测试步骤（2），存储安全 App 中查看到安全工作区已处于锁定状态.

4) 结果判定：

实际测试结果与上述预期结果一致，则判定为符合；其他情况判定为不符。

6.3.2.2 解锁安全工作区

本测试项目应按以下预置条件和测试步骤执行。

1) 预置条件：采用预置条件#2。

2) 测试步骤：

(1) 在存储安全 App 中，查看并确认安全工作区处于锁定状态；

(2) 选择“解锁安全工作区”，确认解锁操作；

(3) 在存储安全 App 中，查看安全工作区的状态；

(4) 被测微型计算机中，通过文件浏览器查看安全工作区的信息。

3) 预期结果：

(1) 上述测试步骤（3），存储安全 App查看到安全工作区已处于解锁状态。

(2) 上述测试步骤（4），文件浏览器查看到安全工作区的信息，至少包括安全工作区名称、安全工作区中测试文件 A 的基本信息。

4) 结果判定：

实际测试结果与上述预期结果一致，则判定为符合；其他情况判定为不符。

6.3.2.3 锁定安全工作区

本测试项目应按以下预置条件和测试步骤执行。

1) 预置条件：采用预置条件#2。

2) 测试步骤：

(1) 在存储安全 App 中，查看并确认安全工作区已处于解锁状态；

(2) 选择“锁定安全工作区”，确认锁定操作。

(3) 在存储安全 App 中，查看安全工作区的状态；

(4) 被测微型计算机中，通过文件浏览器查看安全工作区的信息。

3) 预期结果：

(1) 上述测试步骤（3），存储安全 App查看到安全工作区已处于锁定状态；

(2) 上述测试步骤（4），文件浏览器查看不到安全工作区的信息。

4) 结果判定：

实际测试结果与上述预期结果一致，则判定为符合；其他情况判定为不符。

6.3.2.4 删除安全工作区

当安全工作区支持删除功能时，本测试项目应按以下预置条件和测试步骤执行。

1) 预置条件：采用预置条件#2。

2) 测试步骤：

(1) 在存储安全 App 中，查看并确认安全工作区已处于锁定状态；

(2) 选择“删除安全工作区”，确认删除操作。

(3) 在存储安全 App 中，查看安全工作区的信息；

(4) 被测微型计算机中，通过文件浏览器查看安全工作区的信息。

3) 预期结果：

(1) 上述测试步骤（3），存储安全 App 中查看不到安全工作区；

(2) 上述测试步骤（4），文件浏览器中查看不到安全工作区。

4) 结果判定：

实际测试结果与上述预期结果一致，则判定为符合；其他情况判定为不符。

6.3.3 安全工作区的数据存储

本测试项目宜按以下预置条件和测试步骤执行。

1) 预置条件：采用预置条件#2A。

2) 测试步骤：

(1) 存储安全 App 中，查看并确认安全工作区已处于解锁状态；

(2) 通过文件浏览器，将普通工作区中的测试文件 A 拷贝到安全工作区中，并修改文件名为测试文件B；

(3) 运行测试文件的专用工具，打开安全工作区中的测试文件 B，修改其内容，并另存为测试文件 C，然后关闭测试文件的专用工具；

(4) 通过文件浏览器，将安全工作区中的测试文件 C 拷贝到普通工作区，并修改文件名为测试文件 D；

(5) 运行测试文件的专用工具，打开普通工作区中的测试文件 D，并检查其其内容是否与测试文件 C 一致。

3) 预期结果：

(1) 测试步骤第（2）步，测试文件 A 拷贝成功，测试文件 B 文件名修改成功；

(2) 测试步骤第（3）步，所有操作成功；

(3) 测试步骤第（4）步，测试文件 C 拷贝成功，测试文件 D 文件名修改成功；

(4) 测试步骤第（5）步，测试文件 D 的内容与测试文件 C 一致。

4) 结果判定：

实际测试结果与上述测试步骤的预期一致，则判定为符合；其他情况判定为不符。

6.3.4 安全工作区在锁定状态下的访问

6.3.4.1 安全工作区手动锁定后，安全工作区不可访问

本测试项目宜按以下预置条件和测试步骤执行。

1) 预置条件：采用预置条件#2。

2) 测试步骤：

(1) 查看并锁定安全工作区；

(2) 存储安全App中查看安全工作区中的测试文件A；

(3) 被测微型计算机中，通过文件浏览器查看安全工作区以及其中的测试文件A；

(4) 运行测试文件的专用工具，尝试打开安全工作区中的测试文件A，然后操作（包括但不限于修改、保存、另存为等）测试文件A。

3) 预期结果：

(1) 测试步骤第（2）步，存储安全App中查看不到安全工作区中的测试文件A；

(2) 测试步骤第（3）步，文件浏览器中查看不到安全工作区以及其中的测试文件A；

(3) 测试步骤第（4）步，测试文件的专用工具找不到安全工作区以及其中的测试文件A。

4) 结果判定：

实际测试结果与上述测试步骤的预期一致，则判定为符合；其他情况判定为不符。

6.3.4.2 安全工作区自动锁定后，安全工作区不可访问

本测试项目宜按以下预置条件和测试步骤执行。

1) 预置条件：采用预置条件#3。

2) 测试步骤：

(1) 被测微型计算机中，通过文件浏览器查看安全工作区以及其中的测试文件A；

(2) 运行测试文件的专用工具，尝试打开安全工作区中的测试文件A，然后操作（包括但不限于修改、保存、另存为等）测试文件A。

3) 预期结果：

(1) 测试步骤第（1）步，文件浏览器中查看不到安全工作区以及其中的测试文件A；

(2) 测试步骤第（2）步，测试文件的专用工具找不到安全工作区以及其中的测试文件A。

4) 结果判定：

实际测试结果与上述测试步骤的预期一致，则判定为符合；其他情况判定为不符。

6.3.5 安全工作区离开归属主机

本测试项目应按以下预置条件和测试步骤执行。

1) 预置条件：采用预置条件#4。

2) 测试步骤：

(1) 被测微型计算机A系统关机并关闭电源；

(2) 参测硬盘从被测微型计算机A中拆卸下来；

(3) 被测微型计算机B系统关机并关闭电源；

(4) 参测硬盘安装到被测微型计算机B中；

(5) 被测微型计算机B上电启动；

(6) 被测微型计算机B中，文件浏览器查看参测硬盘中的安全工作区；

(7) 被测微型计算机B中，运行存储安全App并成功登录，然后在存储安全App上查看安全工作区、文件浏览器查看安全工作区；

(8) 被测微型计算机B中，在存储安全App上解锁安全工作区，然后在存储安全App上查看安全工作区、文件浏览器查看安全工作区；

(9) 被测微型计算机B中，运行测试文件的专用工具，尝试打开安全工作区中的测试文件，然后操作（包括但不限于修改、保存、另存为等）测试文件。

3) 测试预期：

(1) 上述测试步骤（6），文件浏览器查看不到参测硬盘中的安全工作区；

(2) 上述测试步骤（7），存储安全App查看不到安全工作区处于锁定状态，文件浏览器查看不到安全工作区；

(3) 上述测试步骤（8），存储安全App查看到安全工作区处于解锁状态，文件浏览器查看到安全工作区及其测试文件A；

(4) 上述测试步骤（11），测试文件的专用工具正常打开和操作安全工作区中的测试文件A。

4) 结果判定：

实际测试结果与上述测试步骤的预期一致，则判定为符合；其他情况判定为不符。

6.3.6 安全工作区所在硬盘的固件升级

本测试项目按以下预置条件和测试步骤执行。

1) 预置条件：采用预置条件#2。

2) 测试步骤：

(1) 存储安全App退出用户登录并结束运行；

(2) 借助升级工具，查看参测硬盘在用固件版本信息（简称固件信息A），然后执行固件升级操作；

(3) 固件升级完成后，查看参测硬盘升级后的固件版本信息（简称固件信息B）；

(4) 检查固件信息B与新版固件的预期固件信息；

(5) 运行存储安全App，且用户成功登录；

(6) 在存储安全App中，执行“解锁安全工作区”，然后在查看安全工作区；

(7) 在存储安全App中，执行“锁定安全工作区”，然后在查看安全工作区。

3) 预期结果：

(1) 上述测试步骤（4）固件信息B与新版固件的预期固件信息一致。

(2) 上述测试步骤（6）结果与6.3.1.2节相符；

(3) 上述测试步骤（7）结果与6.3.1.3节相符。

4) 结果判定：

实际测试结果与上述预期结果一致，则判定为符合；其他情况判定为不符。

6.4 存储安全的性能测试

6.4.1 文件系统 I/O 读写性能

本测试项目应按以下预置条件和测试步骤执行。

1) 预置条件：采用预置条件#5。

2) 测试步骤：

(1) 运行存储安全App，查看并确认参测硬盘没有安全工作区，然后退出存储安全App；

(2) 运行硬盘读写性能测试工具，测试参测硬盘的读写性能，分别测试三次，记录其性能数据 Data_1-1、Data_1-2、Data_1-3，计算出平均值Data_1；然后退出测试工具；

(3) 运行存储安全App，创建安全工作区、解锁安全工作区；

(4) 运行硬盘读写性能测试工具，测试安全工作区的读写性能，分别测试三次，记录其性能数据 Data_2-1、Data_2-2、Data_2-3，计算出平均值Data_2；然后退出测试工具；

(5) 退出存储安全App；

(6) 计算安全工作区的读写性能占比：Data_2 / Data_1 *100%。

3) 预期结果：

(1) 安全工作区的读写性能占比不低于60%。

4) 结果判定：

实际测试结果与上述预期结果一致，则判定为符合；其他情况判定为不符。

6.5 安全保障的检查

6.6.1 当微型计算机采用安全芯片实现数据加密/解密功能时，检查安全芯片的电子元器件国产自主可控等级评估报告、或者包含安全芯片的整机/模块电子元器件选用分析报告、或者安全芯片厂家的国产自主可控承诺书。

6.6.2 当微型计算机采用固态盘存储工作数据时，检查固态盘的电子元器件选用分析报告、或者固态盘厂家的国产自主可控承诺书，其中重点检查固态盘的国产化率、固态盘的控制器和存储介质的国产化情况。

6.6.3 当微型计算机采用固态盘存储工作数据时，检查固态盘与指定微型计算机的国产处理器、国产 BIOS、以及国产操作系统的产品兼容性认证证书。