

ICS 35.220
L 64

YD

中华人民共和国通信行业标准

YD/T 2665-2013

通信存储介质（SSD）加密安全测试方法

The test method for security of communications solid state
disk(SSD) encryption

2013-10-17 发布

2014-01-01 实施

中华人民共和国工业和信息化部 发布

目 次

| | |
|--------------|----|
| 前 言 | II |
| 1 范围 | 1 |
| 2 规范性引用文件 | 1 |
| 3 术语、定义和缩略语 | 1 |
| 3.1 术语和定义 | 1 |
| 3.2 缩略语 | 2 |
| 4 测试概述 | 2 |
| 4.1 功能接口 | 2 |
| 4.2 测试环境 | 3 |
| 5 测试方法 | 3 |
| 5.1 缺省设置 | 3 |
| 5.2 模式选择与初始化 | 6 |
| 5.3 工作流程 | 12 |
| 5.4 身份认证 | 15 |
| 5.5 加解密算法 | 19 |
| 5.6 密钥管理 | 22 |

前 言

本标准是通信存储安全系列标准之一，该系列标准的名称及预计结构如下：

- 《IP存储网络安全技术要求》
- 《IP存储网络安全测试方法》
- 《通信虚拟磁带库（VTL）安全技术要求》
- 《通信虚拟磁带库（VTL）安全测试方法》
- 《通信存储介质（SSD）加密安全技术要求》
- 《通信存储介质（SSD）加密安全测试方法》

随着灾备相关技术和业务的发展，还将制定后续相关标准。

本标准按照GB/T1.1-2009给出的规则起草。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院。

本标准主要起草人：杨剑锋、鲁冬雪。

通信存储介质（SSD）加密安全测试方法

1 范围

本标准规定了通信存储介质（SSD）加密安全测试方法，包括设备缺省设置、启动流程、身份认证、加/解密算法、密钥管理等相关测试内容。本标准中出现的所有未指明的受测设备、加密硬盘等均特指用于通信领域的SSD类存储设备。

本标准适用于通用的通信存储介质（SSD）产品的加密安全特性的测试。不支持用户数据加密功能的SSD不适用本标准。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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。

YD/T 2390-2011 通信存储介质（SSD）加密安全技术要求

NIST SP 800-22rev1a 加密应用的随机数和伪随机数统计测试套件（A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications）

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

对称密码算法 Symmetric Cryptographic Algorithm

加密密钥与解密密钥相同，或容易由其中任意一个密钥推导出另一个密钥的密码算法。

3.1.2

杂凑算法 Hash Function

能够将一个任意长的比特串映射到一个固定长的比特串的一类函数，又称为散列算法、哈希算法或数据摘要算法。

3.1.3

用户密钥 User Key

设备日常使用过程中，用户用于身份认证的密钥。

3.1.4

主密钥 Primary Key

设备重置用户密钥时，用于用户身份认证的密钥。

3.1.5

会话密钥 Session Key

用于用户存储数据加解密的密钥。

3.1.6

加盐 Salt Encryption

即加盐加密，是一种提高密文加密强度的方法。在特定的加密算法中，按特定规则生成的盐（随机字符串）参与待加密内容的加密运算过程，最终获得加盐密文。

3.1.7

保留区 Reserved Area

用于存储SSD加解密系统所需用户密钥、主密钥、会话密钥等数据的安全区域。

3.1.8

数据区 Data Area

用于存储SSD引导和分区信息（包括引导记录、分区记录、文件分配表、文件目录等）、用户存储数据信息的区域。

3.2 缩略语

下列缩略语适用于本文件。

| | | |
|--------|---|--------------|
| DUT | Device Under Test | 被测设备 |
| eSATA: | external SATA | 外部SATA |
| mSATA | mini SATA | 迷你SATA |
| PATA | Parallel Advanced Technology Attachment | 并行高级技术附件（接口） |
| PCIe | Peripheral Component Interconnect express | 外部组件互联快速（接口） |
| SATA | Serial Advanced Technology Attachment | 串行高级技术附件（接口） |
| SSD | Solid State Disk | 固态硬盘 |
| TI | Test Interface | 测试平台接口 |
| UI | User Data Interface | 用户数据接口 |
| USB | Universal Serial BUS | 通用串行总线 |

4 测试概述

4.1 功能接口

支持本标准所述相关用户数据加密安全功能测试和验证要求的DUT，应符合YD/T 2390-2011的要求，并能提供下列两类功能接口。

(1) 用户数据接口（UI）：指在正常使用条件下，DUT用于连接用户设备（如个人计算机、工作站、服务器等），对用户数据进行读写的接口。常见用户数据接口的物理接口类型可包括SATA、mSATA、PCIe、PATA、eSATA、USB等。

(2) 测试平台接口（TI）：指在本标准规定的测试条件下，DUT用于连接测试平台实现有关测试项目所涉及对DUT状态信息、保留区数据、用户数据进行读写的接口。测试平台接口可以是基于UI接口并通过开关切换（如切换为诊断模式、测试模式等）的逻辑接口，也可以是独立设计的专用物理接口。

本标准对DUT的TI接口形式以及配套的数据读写工具（或软件）等暂不作要求。

对于不能提供TI接口的SSD安全加密存储产品，本标准鼓励研究和采用其他对保留区和数据区数据进行读写的方式（如通过破拆的方式直接读写DUT内部芯片所存储数据信息），以便依据本标准有关测试项目的要求对DUT的加密安全特性进行测试验证。

4.2 测试环境

本标准相关测试项目涉及测试环境如图1所示。

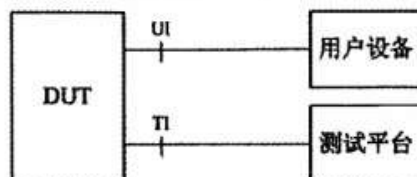


图1 测试环境配置示意

DUT为受测通信存储介质（SSD）设备，可通过UI接口、TI接口分别与用户设备和测试平台连接，其中：

（1）用户设备为具有与DUT UI接口类型相应的总线数据接口（或扩展接口）的通用型主机，且具有DUT所需的可稳定运行的操作系统环境、支持DUT驱动和管理程序的安装及使用、可保证DUT能被正常引导和加载、能正常读写DUT引导和分区信息、能正常读写数据区存储数据信息。

（2）测试平台主要用于DUT用户数据加密功能验证和测试，其安装有必要的DUT数据信息读写工具（或DUT配套的区块数据诊断、测试软件等），能支持DUT所支持的数据读写指令、数据传输协议等。

5 测试方法

5.1 缺省设置

| |
|--|
| 测试编号：1 |
| 测试项目：SSD 加密硬盘保留区的设置 |
| 测试目的：验证 SSD 加密硬盘保留区数据信息的完整性 |
| 参考要求：YD/T 2390-2011 第 5.1 节 |
| 测试步骤： 1) 连接设备测试接口和用户接口，DUT 上电； 2) 通过 TI 检查 DUT 保留区数量及数据信息完整性，验证出厂状态下保留区内模式设置模块、身份认证模块、加解密算法模块、密钥管理模块中预写入的相关程序和参数信息 |
| 预期结果： 1、DUT 出厂状态下，至少设置有 4 个保留区，各保留区数据信息均完整、有效； 2、DUT 加密系统所需的用户密钥、主密钥、会话密钥等信息均存放于保留区 |
| 判定原则：测试结果应与预期结果相符，否则不通过 |

| |
|---|
| 测试编号: 2 |
| 测试项目: 缺省会话密钥保护 |
| 测试目的: 验证 SSD 加密硬盘缺省明文会话密钥的安全性 |
| 参考要求: YD/T 2390-2011 第 5.1 节 |
| 测试步骤: 1) 连接设备测试接口和用户接口, DUT 上电; 2) 通过 TI 检查 DUT 保留区缺省的会话密钥保存状态; 3) 在 DUT 工作状态下, 通过 UI 尝试读取和修改保留区会话密钥信息 |
| 预期结果: 1、DUT 保留区中的缺省会话密钥为明文形式; 2、DUT 工作状态下, 无法读取保留区的会话密钥 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

| |
|--|
| 测试编号: 3 |
| 测试项目: 保留区数据迁移 |
| 测试目的: 验证 SSD 加密硬盘保留区数据备份和安全迁移功能 |
| 参考要求: YD/T 2390-2011 第 5.1 节 |
| 测试步骤: 1) 连接设备测试接口和用户接口, DUT 上电; 2) 通过 TI 检查 DUT 保留区数量和各备份的数据信息; 3) DUT 工作状态下通过 UI 进行保留区数据修改更新(如修改密钥), 并通过 TI 验证各保留区数据信息的一致性; 4) 模拟 DUT 中个别保留区存储单元故障, 验证检查 DUT 保留区数量和各备份的数据信息 |
| 预期结果: 1、DUT 各保留区中数据能保持同步更新; 2、DUT 保留区发生故障时, 数据可实现安全迁移, 并始终保证至少有 4 份可用的保留区 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

5.2 模式选择与初始化

| |
|--|
| 测试编号：4 |
| 测试项目：硬盘模式选择 |
| 测试目的：验证 SSD 加密硬盘支持不认证和认证两种使用模式 |
| 参考要求：YD/T 2390-2011 第 5.2、5.3 节 |
| 测试步骤： 1) 连接设备测试接口和用户接口，DUT 上电启动； 2) 验证 DUT 出厂的缺省模式状态； 3) 通过模式设置模块选择进入认证模式； 4) 验证 DUT 工作模式状态，并通过 UI 进行数据读写操作； 5) 尝试在 DUT 下电后重新启动（或尝试通过 DUT 用户软件）选择进入不认证工作模式； 6) 重复步骤 4) |
| 预期结果： 1、DUT 出厂时应缺省设置为不认证模式； 2、DUT 可在上电启动过程中（或通过 DUT 用户软件）进行模式选择，支持不认证和认证两种使用模式 |
| 判定原则：测试结果应与预期结果相符，否则不通过 |

| |
|---|
| 测试编号: 5 |
| 测试项目: 认证模式硬盘初始化 |
| 测试目的: 验证 SSD 加密硬盘由不认证模式转为认证模式的初始化流程 |
| 参考要求: YD/T 2390-2011 第 5.2、5.3 节 |
| <p>测试步骤:</p> <ol style="list-style-type: none"> 1) 连接设备测试接口和用户接口, DUT 上电启动; 2) 通过 TI 检查 DUT 保留区信息; 3) 在不认证模式下选择进入认证模式, 保留原有存储数据, 进行 DUT 初始化; 4) 设置新的用户密钥和新的主密钥, 完成 DUT 初始化; 5) 通过 TI 检查 DUT 保留区相关会话密钥、用户密钥、主密钥信息; 6) 通过 UI 进行数据读写操作, 检查 DUT 存储用户数据状态; 7) 在不认证模式下 (同步骤 2) 条件) 选择进入认证模式, 不保留原有存储数据, 进行 DUT 初始化; 8) 重复步骤 4) 到步骤 6) |
| <p>预期结果:</p> <ol style="list-style-type: none"> 1、DUT 支持模式间的正常转换, 模式转换时允许用户选择保留原有数据或放弃全部数据; 2、DUT 初始化应生成新的会话密钥, 并安全擦除保留区原有会话密钥; 3、如选择保留原有存储数据, 则应使用原有会话密钥解密全盘数据, 再使用新的会话密钥重新加密, 并保证模式转换前后存储的用户数据无损; 4、用户成功设置用户密钥和主密钥后, DUT 完成初始化, 用户数据读写功能正常; 5、DUT 保留区存放有使用用户密钥加密的会话密钥、使用主密钥加密的会话密钥、进行 128 位加盐的用户密钥杂凑值、进行 128 位加盐的主密钥杂凑值、128 位密钥加盐 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

| |
|--|
| 测试编号：6 |
| 测试项目：认证模式下硬盘数据加密 |
| 测试目的：验证 SSD 加密硬盘认证模式下全盘数据加密的有效性 |
| 参考要求：YD/T 2390-2011 第 5.2 节 |
| 测试步骤： 1) 连接设备测试接口和用户接口，DUT 上电启动； 2) 确认 DUT 处于认证模式，工作状态正常； 3) 通过 TI 检查 DUT 保留区数据信息和存储的用户数据信息； 4) 在未经身份认证的情况下，通过 UI 尝试进行数据读写操作 |
| 预期结果： 1、DUT 完成认证模式初始化后，对保留区数据和用户存储数据均进行有效地加密保护； 2、通过 TI 接口、UI 接口（未经身份认证的情况下）或其他方式（如破拆 DUT 等）均无法有效获取（直接读取或由密文快速破译解密）会话密钥、用户密钥、主密钥、用户存储数据（包括 DUT 用户分区信息、文件分配信息、目录信息、存储数据信息等） |
| 判定原则：测试结果应与预期结果相符，否则不通过 |

| |
|--|
| 测试编号: 7 |
| 测试项目: 不认证模式硬盘初始化 |
| 测试目的: 验证 SSD 加密硬盘由认证模式转为不认证模式的初始化流程 |
| 参考要求: YD/T 2390-2011 第 5.2、5.3 节 |
| <p>测试步骤:</p> <ol style="list-style-type: none"> 1) 连接设备测试接口和用户接口, DUT 上电启动; 2) 通过 TI 检查 DUT 保留区原有相关会话密钥、用户密钥、主密钥信息; 3) 在认证模式下选择进入不认证模式, 保留原有存储数据, 进行 DUT 初始化; 4) 使用有效的用户密钥和主密钥进行身份认证, 完成 DUT 初始化; 5) 通过 TI 检查 DUT 保留区相关会话密钥信息; 6) 通过 UI 进行数据读写操作, 检查 DUT 存储用户数据状态; 7) 在认证模式下 (同步骤 2) 条件) 选择进入不认证模式, 不保留原有存储数据, 进行 DUT 初始化; 8) 重复步骤 4) 到步骤 6) |
| <p>预期结果:</p> <ol style="list-style-type: none"> 1、DUT 支持模式间的正常转换, 模式转换时允许用户选择保留原有数据或放弃全部数据; 2、仅在用户身份认证成功后, 可进行 DUT 初始化; 3、DUT 应生成新的会话密钥, 并安全擦除保留区原有会话密钥、用户密钥和主密钥等信息; 4、如选择保留原有存储数据, 则应使用原有会话密钥解密全盘数据, 再使用新的会话密钥重新加密, 并保证模式转换前后存储的用户数据无损。 5、DUT 初始化完成后, 用户数据读写功能正常, 保留区仅存放有明文的会话密钥 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

| |
|--|
| 测试编号: 8 |
| 测试项目: 初始化过程中断一 |
| 测试目的: 验证 SSD 加密硬盘初始化流程会话密钥更新过程中断后的恢复 |
| 参考要求: YD/T 2390-2011 第 5.3 节 |
| <p>测试步骤:</p> <ol style="list-style-type: none"> 1) 连接设备测试接口和用户接口, DUT 上电启动; 2) 通过 TI 检查 DUT 保留区原有信息, 通过 UI 检查原有用户存储数据; 3) 在不认证模式下选择进入认证模式, 开始 DUT 初始化; 4) DUT 生成新会话密钥即中断初始化过程 (如异常下电、中断连接等); 5) DUT 重新上电 (或加载); 6) 通过 TI 检查 DUT 保留区相关信息, 通过 UI 检查 DUT 存储用户数据状态; 7) DUT 进入正常工作状态后, 在认证模式下选择进入不认证模式, 经身份认证后开始 DUT 初始化; 8) 重复步骤 4) 到步骤 6) |
| <p>预期结果:</p> <ol style="list-style-type: none"> 1、意外中断后重新上电 (或加载), DUT 提示初始化过程异常中断, 可选择恢复初始化前状态或继续初始化; 2、DUT 默认保持初始化前状态, 原有会话密钥仍保持有效; 3、DUT 至少有 4 个有效的保留区, 各保留区数据信息保持一致; 4、DUT 用户数据读写功能正常, 原有用户存储数据保持正常 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

| |
|--|
| 测试编号: 9 |
| 测试项目: 初始化过程中断二 |
| 测试目的: 验证 SSD 加密硬盘初始化流程用户数据加解密过程中断后的恢复 |
| 参考要求: YD/T 2390-2011 第 5.3 节 |
| <p>测试步骤:</p> <ol style="list-style-type: none"> 1) 连接设备测试接口和用户接口, DUT 上电启动; 2) 通过 TI 检查 DUT 保留区原有信息, 通过 UI 检查原有用户存储数据; 3) 在不认证模式下选择进入认证模式, 保留原有存储数据, 开始 DUT 初始化; 4) DUT 生成新会话密钥开始用户数据加解密后即中断初始化过程 (如异常下电、中断连接等); 5) DUT 重新上电 (或加载); 6) 通过 TI 检查 DUT 保留区相关信息, 通过 UI 检查 DUT 存储用户数据状态; 7) DUT 进入正常工作状态后, 在认证模式下选择进入不认证模式, 保留原有存储数据, 经身份认证后开始 DUT 初始化; 8) 重复步骤 4) 到步骤 6) |
| <p>预期结果:</p> <ol style="list-style-type: none"> 1、(可选) 意外中断后重新上电 (或加载), DUT 提示初始化过程异常中断, 可选择恢复初始化前状态或继续初始化; 2、DUT 默认回退到初始化前状态, 原有会话密钥仍保持有效; 3、DUT 至少有 4 个有效的保留区, 各保留区数据信息保持一致; 4、DUT 用户数据读写功能正常, 原有用户存储数据保持正常 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

5.3 工作流程

| |
|---|
| 测试编号: 10 |
| 测试项目: 不认证模式工作流程 |
| 测试目的: 验证 SSD 加密硬盘在不认证模式下的工作流程 |
| 参考要求: YD/T 2390-2011 第 5.4 节 |
| 测试步骤: 1) 连接设备测试接口和用户接口, DUT 上电; 2) 确认进入不认证模式; 3) 通过 UI 在 DUT 的数据存储区进行写入、读出用户数据的操作; 4) 通过 TI 检查硬盘控制器状态 |
| 预期结果: 1、DUT 上电进入不认证模式, 无需身份认证即可进行用户数据读写操作; 2、DUT 开启全盘加密功能, 数据区用户数据以加密形式存储; 3、用户数据读写过程使用缺省的会话密钥进行数据加解密 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

| |
|---|
| 测试编号: 11 |
| 测试项目: 认证模式工作流程 |
| 测试目的: 验证 SSD 加密硬盘在认证模式下的工作流程 |
| 参考要求: YD/T 2390-2011 第 5.5 节 |
| 测试步骤: 1) 连接设备测试接口和用户接口, DUT 上电; 2) 确认进入认证模式, 使用正确的用户密钥进行身份认证; 3) 通过 UI 在 DUT 的数据存储区进行写入、读出用户数据的操作; 4) 通过 TI 检查硬盘控制器状态; 5) DUT 下电后重新上电 (或 DUT 卸载后重新加载), 并确认进入认证模式; 6) 使用错误的用户密钥进行身份认证; 7) 检查硬盘控制器状态, 尝试通过 UI 写入、读出用户数据的操作 |
| 预期结果: 1、DUT 上电进入认证模式, 需成功通过身份认证才可进行用户数据读写操作; 2、DUT 开启全盘加密功能, 数据区用户数据以加密形式存储; 3、用户数据读写过程使用会话密钥进行数据加解密 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

| |
|--|
| 测试编号: 12 |
| 测试项目: 用户数据读写中断 |
| 测试目的: 验证 SSD 加密硬盘在正常状态下用户数据读写过程中断的处理 |
| 参考要求: YD/T 2390-2011 第 5.4、5.5 节 |
| 测试步骤: 1) 连接设备测试接口和用户接口, DUT 上电; 2) 确认进入认证模式 (或不认证模式), 检查硬盘控制器状态; 3) 在全盘加密状态下, 通过 UI 在 DUT 的数据存储区进行持续的写入用户数据的操作; 4) 随即中断 DUT 连接 (如异常下电等); 5) DUT 重新上电 (或加载), 检查硬盘控制器状态; 6) 通过 UI 验证 DUT 存储区用户数据信息 |
| 预期结果: 1、意外中断后重新上电 (或加载), DUT 工作状态保持正常; 2、DUT 存储的原有用户数据保持正常 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

5.4 身份认证

| |
|--|
| 测试编号 13 |
| 测试项目：用户密钥认证 |
| 测试目的：验证 SSD 加密硬盘身份认证模块对用户密钥的处理功能 |
| 参考要求：YD/T 2390-2011 第 6 章 |
| 测试步骤： 1) 连接设备测试接口和用户接口，DUT 上电，选择进入认证模式； 2) 使用错误的用户密钥进行身份认证； 3) 通过 TI 检查 DUT 保留区相关用户身份认证状态； 4) 使用正确的用户密钥进行身份认证； 5) 重复步骤 3) |
| 预期结果： 1、DUT 身份认证模块对用户密钥进行 128 加盐并使用杂凑算法计算杂凑值； 2、仅当输入用户密钥 128 加盐杂凑值与保留区用户密钥加盐杂凑值验证一致时，用户身份认证成功 |
| 判定原则：测试结果应与预期结果相符，否则不通过 |

| |
|--|
| 测试编号：14 |
| 测试项目：主密钥认证 |
| 测试目的：验证 SSD 加密硬盘身份认证模块对主密钥的处理功能 |
| 参考要求：YD/T 2390-2011 第 6 章 |
| 测试步骤： 1) 连接设备测试接口和用户接口，DUT 上电，选择进入认证模式； 2) 使用错误的主密钥进行身份认证； 3) 通过 TI 检查 DUT 保留区相关用户身份认证状态； 4) 使用正确的主密钥进行身份认证； 5) 重复步骤 3) |
| 预期结果： 1、DUT 身份认证模块对主密钥进行 128 加盐并使用杂凑算法计算杂凑值； 2、仅当输入主密钥 128 加盐杂凑值与保留区主密钥加盐杂凑值验证一致时，用户身份认证成功 |
| 判定原则：测试结果应与预期结果相符，否则不通过 |

| |
|---|
| 测试编号: 15 |
| 测试项目: 身份认证状态保持 |
| 测试目的: 验证 SSD 加密硬盘身份认证模块对认证结果的保持 |
| 参考要求: YD/T 2390-2011 第 6 章 |
| 测试步骤: 1) 连接设备测试接口和用户接口, DUT 上电, 选择进入认证模式; 2) 使用正确的用户密钥进行身份认证; 3) 通过 TI 检查 DUT 保留区相关用户认证状态、硬盘锁止状态信息; 4) 通过 UI 尝试进行多次写入、读出用户数据的操作; 5) DUT 下电后重新上电 (或 DUT 卸载后重新加载); 6) 通过 TI 检查 DUT 保留区相关用户认证状态、硬盘锁止状态信息; 7) 通过 UI 尝试进行写入、读出用户数据的操作 |
| 预期结果: 1、用户认证成功后, DUT 处于硬盘解锁状态; 2、身份认证模块可在掉电前一直保持正确的用户认证状态, 多次用户数据读写不需要重复认证; 3、DUT 重新上电启动 (或重新加载) 后, 需进行身份认证, 否则无法进行用户数据读写操作 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

| |
|---|
| 测试编号: 16 |
| 测试项目: 认证失败处理 |
| 测试目的: 验证 SSD 加密硬盘对身份认证失败的处理 |
| 参考要求: YD/T 2390-2011 第 6 章 |
| 测试步骤: 1) 连接设备测试接口和用户接口, DUT 上电, 选择进入认证模式; 2) 使用错误的用户密钥 (或主密钥) 进行身份认证; 3) 通过 UI 尝试对用户数据进行读写操作; 4) 通过 TI 检查 DUT 保留区相关用户认证状态、硬盘锁止状态信息; 5) 重复执行步骤 2) 到步骤 4) 至少 K 次 |
| 预期结果: 1、DUT 在认证模式下, 身份认证不成功无法进行用户数据读写操作; 2、重复认证失败 K 次后, DUT 锁止 (自动关闭电源) |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

5.5 加解密算法

| |
|--|
| 测试编号: 17 |
| 测试项目: 会话密钥加/解密 |
| 测试目的: 验证 SSD 加密硬盘加/解密算法模块对会话密钥加/解密功能 |
| 参考要求: YD/T 2390-2011 第 7 章 |
| <p>测试步骤:</p> <ol style="list-style-type: none"> 1) 连接设备测试接口和用户接口, DUT 上电启动; 2) 初始化设置用户密钥 (或更改、重置用户密钥); 3) 通过 UI 尝试进行写入、读出用户数据的操作; 4) 通过 TI 检查 DUT 保留区会话密钥状态信息; 5) 初始化设置主密钥 (或更改主密钥); 6) 重复步骤 3) 到步骤 4) |
| <p>预期结果:</p> <ol style="list-style-type: none"> 1、DUT 初始化设置用户密钥 (或主密钥) 时, 会话密钥加密模块使用用户密钥 (或主密钥) 通过对称密码算法对新的会话密钥进行加密; 2、重置用户密钥、更改用户密钥 (或主密钥) 时, 会话密钥解密模块应使用原用户密钥 (或原主密钥) 通过对称密码算法对保留区的加密会话密钥进行解密, 随后会话密钥加密模块应使用新的用户密钥 (或新的主密钥) 通过对称密码算法对会话密钥进行加密; 3、DUT 会话密钥加解密过程中用户存储数据无损 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

| |
|--|
| 测试编号: 18 |
| 测试项目: 硬盘数据加/解密 |
| 测试目的: 验证 SSD 加密硬盘加/解密算法模块对硬盘数据加/解密功能 |
| 参考要求: YD/T 2390-2011 第 7 章 |
| <p>测试步骤:</p> <ol style="list-style-type: none"> 1) 连接设备测试接口和用户接口, DUT 上电启动; 2) 进入不认证模式; 3) 通过 UI 尝试进行写入、读出用户数据的操作; 4) 通过 TI 检查 DUT 保留区信息和数据区用户数据; 5) 进入认证模式, 设置用户密钥并使用正确的用户密钥进行身份认证; 6) 重复步骤 3) 到步骤 4) |
| <p>预期结果:</p> <ol style="list-style-type: none"> 1、当 DUT 有用户数据写入时, 硬盘数据加密模块使用会话密钥通过对称密码算法对用户数据进行加密; 2、当 DUT 有用户数据读出时, 硬盘数据解密模块使用会话密钥通过对称密码算法对用户数据进行解密; 3、DUT 硬盘数据加解密过程中用户存储数据无损。 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

| |
|---|
| 测试编号: 19 |
| 测试项目: 数据加密随机性 |
| 测试目的: 验证 SSD 加密算法对用户数据进行加密的随机性 |
| 参考要求: YD/T 2390-2011 第 7 章 |
| <p>测试步骤:</p> <ol style="list-style-type: none"> 1) 连接设备测试接口和用户接口, DUT 上电启动; 2) 确认 DUT 处于认证模式, 工作状态正常; 3) 经有效身份认证, 通过 UI 进行数据读写操作; 4) 通过 TI 检查 DUT 保留区信息和数据区用户数据; 5) 对 DUT 所存储用户数据的密文进行随机性测试 |
| <p>预期结果:</p> <ol style="list-style-type: none"> 1、DUT 存储的用户数据密文应具有较好的随机性 (即密文随机性, 密文数据具有与真实随机数据相似的随机性特征); 2、DUT 存储的用户数据密文应具有较稳定的随机性特征 (即明密文独立性, 密文数据随机性变化与明文数据随机性变化不具有明显的相关性); 3、DUT 存储的用户数据密文应对相应的明文数据具有较高的敏感性 (即明文敏感性, 密文数据随明文的微小变化应表现出较大变化) |
| 判定原则: 本测试项为参考性测试, 对测试结果不作判定 |
| <p>测试说明: 常用的数据随机性特征评价指标包括频数(Frequency)、块内频数(Frequency within a Block)、游程(Runs)、块内最大游程(Longest Run of Ones within a Block)、二元矩阵线性相关度(Binary Matrix Rank)、离散傅里叶变换(Spectral Discrete Fourier Transform)、非重叠模板及重叠模板匹配(Non-periodic Templates、Overlapping Templates)、普遍性统计(Universal Statistical)、线性复杂度(Linear Complexity)、连续性(Serial)、相对熵(Approximate Entropy)、累加和(Cumulative Sums)等, 相应指标的测试和统计方法见 NIST SP 800-22rev1a</p> |

5.6 密钥管理

| |
|--|
| 测试编号: 20 |
| 测试项目: 会话密钥更新 |
| 测试目的: 验证 SSD 加密硬盘密钥管理模块的会话密钥更新处理过程 |
| 参考要求: YD/T 2390-2011 第 8 章 |
| 测试步骤: 1) 连接设备测试接口和用户接口, DUT 上电启动; 2) 通过 TI 检查 DUT 保留区会话密钥状态信息; 3) 使用用户密钥和主密钥进行身份认证; 4) 更新会话密钥; 5) 通过 TI 检查 DUT 保留区更新的会话密钥状态信息状态信息; 6) 通过 UI 检查用户存储数据信息内容 |
| 预期结果: 1、对用户密钥和主密钥均身份验证成功后, 可进行 DUT 会话密钥更新操作; 2、密钥管理模块通过随机数生成器生成新的会话密钥; 3、使用主密钥通过对称密码算法对新的会话密钥进行加密, 保存到 DUT 保留区; 4、使用用户密钥通过对称密码算法对新的会话密钥进行加密, 保存到 DUT 保留区; 5、会话密钥更新过程 DUT 中存储的用户数据无损 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

| |
|--|
| 测试编号: 21 |
| 测试项目: 主密钥更新 |
| 测试目的: 验证 SSD 加密硬盘密钥管理模块的主密钥更新处理过程 |
| 参考要求: YD/T 2390-2011 第 8 章 |
| 测试步骤: 1) 连接设备测试接口和用户接口, DUT 上电启动; 2) 通过 TI 检查 DUT 保留区主密钥、会话密钥状态信息; 3) 使用原主密钥进行身份认证; 4) 对主密钥进行更新; 5) 通过 TI 检查 DUT 保留区更新的主密钥、会话密钥状态信息; 6) DUT 下电后重新上电 (或 DUT 卸载后重新加载), 并对主密钥验证 |
| 预期结果: 1、对主密钥身份验证成功后, 可进行 DUT 主密钥更新操作; 2、对新的主密钥进行 128 加盐并使用杂凑算法计算杂凑值, 保存到 DUT 保留区; 3、使用新的主密钥通过对称密码算法对会话密钥进行加密, 保存到 DUT 保留区; 4、重新启动 (或加载) 后新的主密钥验证有效 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

| |
|--|
| 测试编号：22 |
| 测试项目：用户密钥更新 |
| 测试目的：验证 SSD 加密硬盘密钥管理模块的用户密钥更新处理过程 |
| 参考要求：YD/T 2390-2011 第 8 章 |
| <p>测试步骤：</p> <ol style="list-style-type: none"> 1) 连接设备测试接口和用户接口，DUT 上电启动； 2) 通过 TI 检查 DUT 保留区用户密钥、会话密钥状态信息； 3) 使用原用户密钥进行身份认证； 4) 对用户密钥进行更新； 5) 通过 TI 检查 DUT 保留区更新的用户密钥、会话密钥状态信息状态信息； 6) DUT 下电后重新上电（或 DUT 卸载后重新加载），并对用户密钥验证 |
| <p>预期结果：</p> <ol style="list-style-type: none"> 1、对用户密钥身份验证成功后，可进行 DUT 用户密钥更新操作； 2、对新的用户密钥进行 128 加盐并使用杂凑算法计算杂凑值，保存到 DUT 保留区； 3、使用新的用户密钥通过对称密码算法对会话密钥进行加密，保存到 DUT 保留区； 4、重新启动（或加载）后新的用户密钥验证有效 |
| 判定原则：测试结果应与预期结果相符，否则不通过 |

| |
|---|
| 测试编号: 23 |
| 测试项目: 用户密钥重置 |
| 测试目的: 验证 SSD 加密硬盘密钥管理模块的用户密钥重置处理过程 |
| 参考要求: YD/T 2390-2011 第 8 章 |
| <p>测试步骤:</p> <ol style="list-style-type: none"> 1) 连接设备测试接口和用户接口, DUT 上电启动; 2) 通过 TI 检查 DUT 保留区用户密钥、会话密钥状态信息; 3) 使用主密钥进行身份认证; 4) 对用户密钥进行重置; 5) 通过 TI 检查 DUT 保留区更新的用户密钥、会话密钥状态信息; 6) DUT 下电后重新上电 (或 DUT 卸载后重新加载), 并对用户密钥验证 |
| <p>预期结果:</p> <ol style="list-style-type: none"> 1、对主密钥身份验证成功后, 可进行 DUT 用户密钥重置操作; 2、对新的用户密钥进行 128 加盐并使用杂凑算法计算杂凑值, 保存到 DUT 保留区; 3、使用新的用户密钥通过对称密码算法对会话密钥进行加密, 保存到 DUT 保留区; 4、重新启动 (或加载) 后新的用户密钥验证有效 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

| |
|--|
| 测试编号: 24 |
| 测试项目: 用户密钥(主密钥)更新中断 |
| 测试目的: 验证 SSD 加密硬盘用户密钥(或主密钥)更新过程中断后的恢复 |
| 参考要求: YD/T 2390-2011 第 8 章 |
| <p>测试步骤:</p> <ol style="list-style-type: none"> 1) 连接设备测试接口和用户接口, DUT 上电启动; 2) 确认 DUT 处于认证模式, 工作状态正常; 3) 通过 TI 检查 DUT 保留区原有信息; 4) 经身份认证后, 通过 UI 检查原有用户存储数据; 5) 选择进行用户密钥(或主密钥)更新, 开始 DUT 初始化; 6) 输入新用户密钥(或新主密钥)后即中断密钥更新过程(如异常下电等); 7) DUT 重新上电(或加载); 8) 通过 TI 检查 DUT 保留区相关信息, 尝试以原用户密钥(或新主密钥)进行身份认证并通过 UI 检查 DUT 存储用户数据状态 |
| <p>预期结果:</p> <ol style="list-style-type: none"> 1、(可选)意外中断后重新上电(或加载), DUT 提示密钥更新过程异常中断, 可选择重新开始密钥更新; 2、DUT 默认保持密钥更新前状态, 原用户密钥(或原主密钥)仍保持有效; 3、DUT 至少有 4 个有效的保留区, 各保留区数据信息保持一致; 4、DUT 用户数据读写功能正常, 原有用户存储数据保持正常 |
| 判定原则: 测试结果应与预期结果相符, 否则不通过 |

中华人民共和国
通信行业标准
通信存储介质（SSD）加密安全测试方法
YD/T 2665-2013

*

人民邮电出版社出版发行
北京市丰台区成寿寺路11号邮电出版大厦
邮政编码：100064
宝隆元（北京）印刷技术有限公司印刷
版权所有 不得翻印

*

开本：880×1230 1/16 2014年2月第1版
印张：2 2014年2月北京第1次印刷
字数：53千字

15115·371

定价：25元

本书如有印装质量问题，请与本社联系 电话：(010)81055492