

NIST 特别出版物 800-111

NIST

**National Institute of
Standards and Technology**
Technology Administration
U.S. Department of Commerce

最终用户设备

存储加密技术指南

国家标准和技术研究所的建议

**Karen Scarfone
Murugiah Souppaya**

计算机安全

国家标准和技术研究所
信息技术实验室
计算机安全处

Gaithersburg, MD 20899-8930

2007年11月



美国商务部
部长: Carlos M. Gutierrez

国家标准和技术研究所
代所长: James M. Turner

目录

执行摘要

1 介绍

- 1.1 权限
- 1.2 目的和适用范围
- 1.3 适用对象
- 1.4 篇章结构

2 存储安全概述

- 2.1 文件存储的基本概念
- 2.2 存储安全的需要
- 2.3 存储的安全控制

3 存储加密技术

- 3.1 存储加密技术的常见类型
 - 3.1.1 全盘加密
 - 3.1.2 虚拟盘加密和卷加密
 - 3.1.3 文件/文件夹加密
- 3.2 存储加密技术提供的保护
- 3.3 不同存储加密技术的比较
 - 3.3.1 用例 1: 共用一台手提电脑
 - 3.3.2 用例 2: 计算机间转移文件
 - 3.3.3 用例 3: 与合同商共享数据
 - 3.3.4 用例 4: 携带手提电脑出差
 - 3.3.5 用例 5: 携带双引导手提电脑出差
- 3.4 存储加密技术管理

4 存储加密技术的规划和执行

- 4.1 识别需要
- 4.2 设计方案
 - 4.2.1 密码
 - 4.2.2 认证
- 4.3 执行和测试草案
- 4.4 配备方案
- 4.5 管理方案

附录 A 最终用户设备存储加密的可替代方案

附录 B 术语表

附录 C 缩略语

附录 D 工具和资源