

NIST特别出版物800-152

内部资料

翻译：高卓

# 美国联邦密码密钥 管理系统轮廓

作者： Elaine Barker  
Miles Smid  
Dennis Branstad

本出版物可从以下网址免费获得：

<http://dx.doi.org/10.6028/NIST.SP.800-152>

2015年10月



美国商务部

部长：Penny Pritzke

国家标准和技术研究所

副部长兼所长：Willie May

北京江南天安科技有限公司

# 目录

1. 介绍
  - 1.1 “轮廓”用语
  - 1.2 适用范围
  - 1.3 适用对象
  - 1.4 篇章结构
2. “轮廓”的基础
  - 2.1 “轮廓”的主题、要求、扩充和特性
  - 2.2 密码密钥管理的基本原理
  - 2.3 密钥、元数据、可信关联和捆绑
  - 2.4 FCKMS 的功能
  - 2.5 CKMS 设计
  - 2.6 CKMS 轮廓
  - 2.7 FCKMS 轮廓
  - 2.8 “框架”与“轮廓”的区别
  - 2.9 支持安全电子邮件应用的分布式 CKMS 举例
  - 2.10 模块、设备和组件
3. 联邦 CKMS 的目标
  - 3.1 为网络、应用和用户 提供密钥管理
  - 3.2 在 FCKMS 中充分利用商业现货产品
  - 3.3 标准合规
  - 3.4 易用
    - 3.4.1 适应用户的能力和喜好
    - 3.4.2. 用户界面的设计原则
  - 3.5 性能和可扩展性
  - 3.6 知识产权
4. 安全策略
  - 4.1 信息管理策略
  - 4.2 信息安全策略
  - 4.3 CKMS 和 FCKMS 安全策略
  - 4.4 FCKMS 模块安全策略
  - 4.5 密码模块安全策略
  - 4.6 其他相关安全策略
  - 4.7 策略的相互关系
  - 4.8 个人问责
  - 4.9 匿名化、不可关联性和不可观察性
    - 4.9.1 匿名化
    - 4.9.2 不可关联性
    - 4.9.3 不可观察性
  - 4.10 法律法规
  - 4.11 安全域

- 4.11.1 数据交换的条件
- 4.11.2 保护保障
- 4.11.3 FCKMS 安全策略的等效性和兼容性
- 4.11.4 第三方共享
- 4.11.5 多层级安全域
- 4.11.6 升级和降级
- 4.11.7 FCKMS 安全策略变更

## 5. 角色和责任

## 6. 密码算法、密钥和元数据

- 6.1 密码算法和密钥
  - 6.1.1 密钥类型、长度和强度
  - 6.1.2 密钥保护
  - 6.1.3 密钥保障
- 6.2 密钥元数据
  - 6.2.1 元数据元素
  - 6.2.2 被要求的密钥和元数据信息
- 6.3 密钥的生命周期状态和转换
- 6.4 针对密钥和元数据的管理功能
  - 6.4.1 生成密钥
  - 6.4.2 注册拥有者
  - 6.4.3 激活密钥
  - 6.4.4 失活密钥
  - 6.4.5 撤销密钥
  - 6.4.6 暂停和重新激活密钥
  - 6.4.7 更新公钥证书
  - 6.4.8 密钥衍生或密钥更新
  - 6.4.9 销毁密钥和元数据
  - 6.4.10 关联密钥和元数据
  - 6.4.11 修改元数据
  - 6.4.12 删除元数据
  - 6.4.13 列出密钥元数据
  - 6.4.14 将运算密钥和元数据保存到密码模块之外
  - 6.4.15 备份密钥及其元数据
  - 6.4.16 存档密钥和/或元数据
  - 6.4.17 恢复密钥和/或元数据
  - 6.4.18 建立密钥
  - 6.4.19 密钥和关联元数据输入密码模块
  - 6.4.20 密钥和关联元数据从密码模块输出
  - 6.4.21 验证公钥域参数
  - 6.4.22 验证公钥
  - 6.4.23 验证公钥认证路径
  - 6.4.24 验证对称密钥
  - 6.4.25 验证对称密钥拥有权

- 6.4.26 验证私钥（或密钥对）
- 6.4.27 验证私钥所有权
- 6.4.28 通过密钥执行密码功能
- 6.4.29 管理信任锚库
- 6.5 被保存的密码密钥和/或元数据的安全
- 6.6 密钥建立过程中的密码密钥和/或元数据的安全
  - 6.6.1 密钥传送
  - 6.6.2 密钥协议
  - 6.6.3 密钥确认
  - 6.6.4 密钥建立协议
- 6.7 限制对密钥和元数据管理功能的访问
  - 6.7.1 访问控制系统（ACS）
  - 6.7.2 限制明文密钥从密码模块的输入输出
  - 6.7.3 控制人工输入
  - 6.7.4 多方控制
  - 6.7.5 密钥分解
- 6.8 破坏恢复
  - 6.8.1 密钥破解
  - 6.8.2 元数据破解
  - 6.8.3 密码和元数据撤销
  - 6.8.4 密码模块破解
  - 6.8.5 计算机系统破坏恢复
  - 6.8.6 网络安全控制和破坏恢复
  - 6.8.7 人为安全破坏恢复
  - 6.8.8 物理安全破坏恢复
- 7. 互操作性和转换**
- 8. 安全控制**
  - 8.1 物理安全控制
  - 8.2 操作系统和设备安全控制
    - 8.2.1 操作系统的安全
    - 8.2.2 单个 FCKMS 设备的安全
    - 8.2.3 恶意软件保护
    - 8.2.4 审计和远程监测
  - 8.3 网络安全控制机制
  - 8.4 密码模块控制
  - 8.5 联邦 CKMS 安全控制的挑选和评价流程
- 9. 测试和系统保障**
  - 9.1 CKMS 和 FCKMS 测试
  - 9.2 第三方测试
  - 9.3 互操作性测试
  - 9.4 自测试
  - 9.5 可扩展性测试
  - 9.6 功能测试和安全测试

- 9.7 环境测试
- 9.8 易用性测试
- 9.9 开发、交付和维护保障
  - 9.9.1 配置管理
  - 9.9.2 安全交付
  - 9.9.3 开发和维护环境安全
  - 9.9.4 缺陷补救能力

## **10. 灾害恢复**

- 10.1 设施毁坏
- 10.2 公用服务中断
- 10.3 通信和计算中断
- 10.4 FCKMS 硬件故障
- 10.5 系统软件故障
- 10.6 密码模块故障
- 10.7 密钥和元数据损坏和丢失

## **11. 安全评价**

- 11.1 全面安全评价
  - 11.1.1 第三方测试审查和测试结果验证
  - 11.1.2 系统设计的架构审查
  - 11.1.3 功能和安全测试
  - 11.1.4 渗透测试
- 11.2 定期安全审查
- 11.3 增量安全评价
- 11.4 保持安全水平不变

## **12. 技术挑战**

**附录 A 参考文献**

**附录 B 术语表**