

密钥管理建议

第2部分：密钥管理机构最佳实践规范

内部资料
翻译：高卓

作者：**Elaine Barker**
William Barker

本出版物可从以下网址免费获得：
<https://doi.org/10.6028/NIST.SP.800-57pt2r1>

2019年5月



美国商务部

部长：**Wilbur L. Ross, Jr.**

国家标准和技术研究所

商务部副部长兼所长：**Walter Copan**

北京江南天安科技有限公司

目录

1. 介绍
 - 1.1 范围
 - 1.2 适用对象
 - 1.3 背景和缘由
 - 1.4 篇章结构
 - 1.5 术语和缩略语
 - 1.5.1 术语
 - 1.5.2 缩略语
2. 密钥管理概念
 - 2.1 密钥建立
 - 2.2 密钥管理功能
 - 2.3 密码密钥管理系统（CKMS）
 - 2.3.1 中央监控实体
 - 2.3.2 密钥处理设施
 - 2.3.3 服务代理
 - 2.3.4 客户端节点
 - 2.3.5 令牌
 - 2.3.6 公钥基础设施环境
 - 2.3.7 对称密钥环境
 - 2.3.8 分层结构和网格结构
 - 2.3.9 集中式基础设施对分散式基础设施
 - 2.3.10 可用的自动化密钥管理方案和协议
 - 2.4 CKMS 的一般设计要求
 - 2.5 信任
 - 2.6 撤销和临时停用
3. 密钥管理规划
 - 3.1 背景
 - 3.1.1 挑选 SP 800-53 控制
 - 3.1.2 IT 系统检查
 - 3.2 密钥管理规划
 - 3.2.1 密钥管理规划流程
 - 3.2.2 密钥管理规划的信息要求
4. 密钥管理规范
 - 4.1 密钥管理规范的内容
 - 4.2 密码应用
 - 4.3 通信环境
 - 4.4 密钥管理的元数据要求
 - 4.5 密钥材料生成
 - 4.6 密钥材料分发
 - 4.7 密钥信息存储

- 4.8 访问控制
- 4.9 核查和审计
- 4.10 从密钥材料遭破解、损坏或丢失事件恢复
- 4.11 密钥恢复

5. CKMS 安全策略

- 5.1 策略的内容
 - 5.1.1 策略内容的总体要求
 - 5.1.2 安全目标
 - 5.1.3 机构的责任
 - 5.1.4 CKMS SP 格式样本

5.2 策略的落实

6. CKMS 具体措施陈述

- 6.1 具体措施陈述的备选格式
 - 6.1.1 单独的具体措施陈述
 - 6.1.2 认证规范陈述
- 6.2 CKMS PS 的常见内容
 - 6.2.1 CKMS PS 与 CKMS 安全策略关联
 - 6.2.2 识别负责实体和联系信息
 - 6.2.3 密钥生成和/或证书签发
 - 6.2.4 密钥协定
 - 6.2.5 密钥处理中心之间的协定
 - 6.2.6 密钥的建立、临时停用和撤销体系
 - 6.2.7 建立密码有效期
 - 6.2.8 密钥材料的跟踪和核查
 - 6.2.9 密钥信息保护
 - 6.2.10 密钥材料的临时停用和撤销
 - 6.2.11 审计
 - 6.2.12 密钥的销毁
 - 6.2.13 密钥的备份、存档和恢复
 - 6.2.14 破解恢复
 - 6.2.15 违反策略的处罚条例
 - 6.2.16 文件

附录 A CKMS 举例

- A.1 公钥基础设施 (PKI)
 - A.1.1 中央监控中心
 - A.1.2 发证中心 (CA)
 - A.1.3 注册中心 (RA)
 - A.1.4 订户的客户端节点和令牌
 - A.1.5 PKI 的分层结构和网格结构
- A.2 密钥中心
 - A.2.1 密钥分发中心 (KDC) 架构
 - A.2.2 密钥传输中心 (KTC) 架构

附录 B 插入了密钥管理内容的安全计划模板

附录 C 密码产品开发之密钥管理规范检查列表

附录 D 参考文献

附录 E 修订历史

