

NIST特别出版物800-57第1部分  
第4修订版

---

# 密码密钥管理建议

## 第1部分：通用指南

内部资料

---

翻译：高卓

作者： Elaine Barker  
信息技术实验室计算机安全部

本出版物英文版可从以下网址免费获得：

<http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4>

2016年1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

## 执行摘要

### 1. 介绍

- 1.1 目标/目的
- 1.2 适用对象
- 1.3 适用范围
- 1.4 FIPS 和 NIST 建议（NIST 标准）的目的
- 1.5 篇章结构

### 2. 术语和缩略语

- 2.1 术语
- 2.2 缩略语

### 3. 安全服务

- 3.1 保密性
- 3.2 数据完整性
- 3.3 认证
- 3.4 授权
- 3.5 不可否认性
- 3.6 支持性服务
- 3.7 服务合成

### 4. 密码算法

- 4.1 密码算法的类别
- 4.2 密码算法的功能
  - 4.2.1 散列函数
  - 4.2.2 用于加密和解密的对称密钥算法
    - 4.2.2.1 高级加密标准（AES）
    - 4.2.2.2 三重 DEA（TDEA）
    - 4.2.2.3 运算模式
  - 4.2.3 消息认证码（MAC）
    - 4.2.3.1 使用块密码算法的 MAC
    - 4.2.3.2 使用散列函数的 MAC
  - 4.2.4 数字签名算法
  - 4.2.5 密钥建立方案
    - 4.2.5.1 离散对数密钥协定方案
    - 4.2.5.2 使用整数分解方案的密钥建立
    - 4.2.5.3 密钥建立方案的安全属性
    - 4.2.5.4 密钥加密和密钥包装
    - 4.2.5.5 密钥确认
  - 4.2.6 密钥建立协议
  - 4.2.7 随机位生成

### 5. 通用密钥管理指南

- 5.1 密钥类型和其他信息
  - 5.1.1 密码密钥

- 5.1.2 其他密码或相关信息
- 5.2 密钥的使用
- 5.3 密码有效期
  - 5.3.1 影响密码有效期的风险因素
  - 5.3.2 影响密码有效期的后果因素
  - 5.3.3 影响密码有效的其他因素
    - 5.3.3.1 通信和存储
    - 5.3.3.2 密钥的撤销和更换成本
  - 5.3.4 非对称密钥的使用期和密码有效期
  - 5.3.5 对称密钥的使用期和密码有效期
  - 5.3.6 针对具体密钥类型的密码有效期建议
  - 5.3.7 有关其他密码或相关信息的建议
- 5.4 保障
  - 5.4.1 完整性保障（完整性保护）
  - 5.4.2 域参数有效性保障
  - 5.4.3 私钥拥有权保障
- 5.5 密钥和其他密钥材料破解
- 5.6 密码算法和密钥大小选择指南
  - 5.6.1 可比算法强度
  - 5.6.2 定义适当的算法套件
  - 5.6.3 使用算法套件
  - 5.6.4 向新算法和密钥大小的转换
  - 5.6.5 安全强度降低
- 6. 密码信息的保护要求**
  - 6.1 保护和保障要求
    - 6.1.1 密码密钥的保护和保障要求归纳
    - 6.1.2 其他密码或相关信息的保护要求归纳
    - 6.1.3 密钥保障
  - 6.2 保护机制
    - 6.2.1 传输中的密码信息的保护机制
      - 6.2.1.1 可用性
      - 6.2.1.2 完整性
      - 6.2.1.3 保密性
      - 6.2.1.4 与用途或应用的关联
      - 6.2.1.5 与其他实体的关联
      - 6.2.1.6 与其他相关信息的关联
    - 6.2.2 存储中的信息的保护机制
      - 6.2.2.1 可用性
      - 6.2.2.2 完整性
      - 6.2.2.3 保密性
      - 6.2.2.4 与用途或应用的关联
      - 6.2.2.5 与其他实体的关联
      - 6.2.2.6 与其他相关信息的关联

- 6.2.3 与密码信息关联的元数据
  - 6.2.3.1 密钥的元数据
  - 6.2.3.2 相关密码信息的元数据

## 7. 密钥的状态和转换

- 7.1 预激活状态
- 7.2 活跃状态
- 7.3 暂停状态
- 7.4 失活状态
- 7.5 破解状态
- 7.6 销毁状态

## 8. 密钥管理的阶段和功能

- 8.1 运行前阶段
  - 8.1.1 用户注册功能
  - 8.1.2 系统初始化功能
  - 8.1.3 用户初始化功能
  - 8.1.4 密钥材料安装功能
  - 8.1.5 密钥建立功能
    - 8.1.5.1 非对称密钥对的生成和分发
      - 8.1.5.1.1 静态公钥的分发
        - 8.1.5.1.1.1 在 PKI 中分发信任锚公钥
        - 8.1.5.1.1.2 向注册中心或发证中心呈交
        - 8.1.5.1.1.3 常用分发方法
      - 8.1.5.1.2 临时公钥的分发
      - 8.1.5.1.3 集中生成的密钥对的分发
    - 8.1.5.2 对称密钥的生成和分发
      - 8.1.5.2.1 密钥生成
      - 8.1.5.2.2 密钥分发
        - 8.1.5.2.2.1 人工密钥分发
        - 8.1.5.2.2.2 自动密钥分发/密钥传输/密钥包装
      - 8.1.5.2.3 密钥协定
    - 8.1.5.3 其他密钥材料的生成和分发
      - 8.1.5.3.1 域参数
      - 8.1.5.3.2 初始化向量
      - 8.1.5.3.3 共享的秘密
      - 8.1.5.3.4 RBG 种子
      - 8.1.5.3.5 其他公开和秘密信息
      - 8.1.5.3.6 中间结果
      - 8.1.5.3.7 随机位/随机数
      - 8.1.5.3.8 口令
  - 8.1.6 密钥注册功能
- 8.2 运行阶段
  - 8.2.1 常规运行存储功能
    - 8.2.1.1 密码模块存储

- 8.2.1.2 可即时访问的存储介质
    - 8.2.2 运行连续性功能
      - 8.2.2.1 备份存储
      - 8.2.2.2 密钥恢复功能
    - 8.2.3 密钥变更功能
      - 8.2.3.1 密钥重设
      - 8.2.3.2 密钥更新功能
    - 8.2.4 密钥衍生方法
  - 8.3 运行后阶段
    - 8.3.1 档案存储和密钥恢复功能
    - 8.3.2 实体注销功能
    - 8.3.3 密钥注销功能
  - 8.4 销毁阶段
- 9. 问责、审计和生存**
- 9.1 问责
  - 9.2 审计
  - 9.3 密钥管理系统的生存
    - 9.3.1 密钥备份
    - 9.3.2 密钥恢复
    - 9.3.3 系统冗余/应急预案
      - 9.3.3.1 一般性原则
      - 9.3.3.2 密码和密钥管理特有的恢复问题
    - 9.3.4 破解恢复
- 10. 密码设备或应用的密钥管理规范**
- 10.1 密钥管理规范的描述/目的
  - 10.2 密钥管理规范的内容
    - 10.2.1 密码应用
    - 10.2.2 通信环境
    - 10.2.3 密钥管理成分要求
    - 10.2.4 密钥管理成分生成
    - 10.2.5 密钥管理成分分发
    - 10.2.6 密钥材料存储
    - 10.2.7 访问控制
    - 10.2.8 问责
    - 10.2.9 破解管理和恢复
    - 10.2.10 密钥恢复
- 附录 A 密码和非密码完整性和源认证机制**
- 附录 B 密钥恢复**
- B.1 用存储的密钥材料恢复
  - B.2 通过重建密钥材料恢复
  - B.3 需要密钥材料可恢复的情况
    - B.3.1 签名密钥对
      - B.3.1.1 签名私钥

- B.3.1.2 签名验证公钥
- B.3.2 对称认证密钥
- B.3.3 认证密钥对
  - B.3.3.1 认证公钥
  - B.3.3.2 认证私钥
- B.3.4 对称数据加密密钥
- B.3.5 对称密钥包装密钥
- B.3.6 随机数生成密钥
- B.3.7 对称主密钥
- B.3.8 密钥传输密钥对
  - B.3.8.1 私钥传输密钥
  - B.3.8.2 公钥传输密钥
- B.3.9 对称密钥协定密钥
- B.3.10 静态密钥协定密钥对
  - B.3.10.1 静态密钥协定私钥
  - B.3.10.2 静态密钥协定公钥
- B.3.11 临时密钥对
  - B.3.11.1 临时私钥
  - B.3.11.2 临时公钥
- B.3.12 对称授权密钥
- B.3.13 授权密钥对
  - B.3.13.1 授权私钥
  - B.3.13.2 授权公钥
- B.3.14 其他密码相关材料
  - B.3.14.1 域参数
  - B.3.14.2 初始化向量 (IV)
  - B.3.14.3 共享的秘密
  - B.3.14.4 RBG 种子
  - B.3.14.5 其他公开和秘密信息
  - B.3.14.6 中间结果
  - B.3.14.7 密钥控制信息
  - B.3.14.8 随机数
  - B.3.14.9 口令
  - B.3.14.10 审计信息
- B.4 密钥恢复系统
- B.5 密钥恢复策略
- 附录 C 参考文献
- 附录 D 版本变更 (略)