

NIST特别出版物800-57第3部分  
第1修订版

内部资料  
高卓翻译

---

**密码密钥管理建议**  
**第3部分：针对具体应用的**  
**密钥管理指南**

作者： Elaine Barker  
Quynh Dang

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.800-57pt3r1>

2015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

1. 介绍
  - 1.1 目的
  - 1.2 要求的用语
  - 1.3 一般性协议考虑
    - 1.3.1 强制执行对可选执行
    - 1.3.2 密码协商
    - 1.3.3 单用途或多用途密钥
    - 1.3.4 算法和密钥大小转换
2. 密钥管理基础设施 (PKI)
  - 2.1 描述
  - 2.2 安全和合规问题
    - 2.2.1 建议的密钥大小和算法
  - 2.3 采购指南
    - 2.3.1 CA/RA 软件和硬件
    - 2.3.2 OCSP 响应器
    - 2.3.3 密码模块
    - 2.3.4 密钥恢复服务器
    - 2.3.5 依赖方的软件
    - 2.3.6 客户端软件
  - 2.4 针对系统安装人员/管理员的建议
    - 2.4.1 证书发放
    - 2.4.2 证书撤销请求
    - 2.4.3 证书撤销列表的生成
    - 2.4.4 分发证书和 CRL 的 PKI 资源库
    - 2.4.5 OCSP 响应器
    - 2.4.6 备份和存档
    - 2.4.7 依赖方的集成和配置
  - 2.5 用户 (订户) 指南
3. 互联网协议安全 (IPsec)
  - 3.1 描述
  - 3.2 安全和合规问题
    - 3.2.1 密码算法
    - 3.2.2 附加建议
  - 3.3 采购指南
  - 3.4 针对系统安装人员的建议
  - 3.5 针对系统管理员的建议
  - 3.6 针对最终用户的建议
4. 传输层安全 (TLS)
5. 安全/多用途互联网邮件扩展 (S/MIME)
  - 5.1 描述

- 5.2 安全和合规问题
- 5.3 采购指南
- 5.4 针对系统安装人员的建议
- 5.5 针对系统管理员的建议
- 5.6 针对最终用户的建议
- 6. Kerberos**
  - 6.1 描述
  - 6.2 安全和合规问题
  - 6.3 采购指南
  - 6.4 针对系统安装人员的建议
  - 6.5 针对系统管理员的建议
  - 6.6 针对最终用户的建议
- 7. 无线电发射密钥重设 (OTAR) 密钥管理消息 (KMM)**
  - 7.1 描述
  - 7.2 安全和合规问题
    - 7.2.1 密码算法
    - 7.2.2 消息认证和密码有效期
    - 7.2.3 密钥的使用
    - 7.2.4 备份
    - 7.2.5 密钥重设
    - 7.2.6 随机位发生器
  - 7.3 采购指南
  - 7.4 针对系统安装人员的建议
  - 7.5 针对系统管理员的建议
  - 7.6 针对最终用户的建议
- 8. 域名系统安全扩展 (DNSSEC)**
  - 8.1 描述
    - 8.1.1 DNS 数据认证
    - 8.1.2 DNS 交易认证
    - 8.1.3 DNS 密码算法/方案、模式和组合
    - 8.1.4 有关密钥大小的特殊考虑
    - 8.1.5 有关 NSEC3 的特殊考虑
  - 8.2 安全和合规问题
  - 8.3 采购指南
  - 8.4 针对系统安装人员的建议
    - 8.4.1 针对系统安装人员的建议 (权威服务器)
    - 8.4.2 针对系统安装人员的建议 (缓存递归服务器)
    - 8.4.3 针对系统安装人员的建议 (客户端系统)
  - 8.5 针对系统管理员的建议
    - 8.5.1 针对系统管理员的建议 (权威服务器)
    - 8.5.2 针对系统管理员的建议 (缓存递归服务器)
    - 8.5.3 针对系统管理员的建议 (客户端系统)
  - 8.6 针对最终用户的建议

## **9. 加密文件系统（EFS）**

### **9.1 描述**

9.1.1 被要求的密钥数量

9.1.2 对用于文件加密的对称密钥的访问

### **9.2 安全和合规问题**

### **9.3 采购指南**

### **9.4 针对系统安装人员的建议**

### **9.5 针对系统管理员的建议**

### **9.6 针对最终用户的建议**

## **10. 安全壳（SSH）**

### **10.1 描述**

10.1.1 传输层协议（SSH-TLP）

10.1.2 用户认证协议（UAP）

10.1.3 连接协议（CP）

### **10.2 安全和合规问题**

10.2.1 TLP 问题

10.2.2 UAP 问题

### **10.3 采购指南**

### **10.4 针对系统安装人员的建议**

### **10.5 针对系统管理员的建议**

### **10.6 针对最终用户的建议**

## **附录 A 术语表**

## **附录 B 缩略语**

## **附录 C 最终用户新手入门**

## **附录 D 参考文献**

## **附录 E 修订版的更改**