

FIPS PUB 140-2

联邦信息处理标准出版物

(取代1994年1月11日发布的FIPS PUB 140-1)

密码模块安全要求

类别：计算机安全

子类别：密码

国家标准和技术研究所

信息技术实验室

Gaithersburg, MD 20899-8900

2001年5月25日



美国商务部

部长：Donald L. Evans

技术管理局

主管技术副部长：Phillip J. Bond

国家标准和技术研究所

所长：Arden L. Bement, Jr.

目录

1. 概述
 - 1.1 安全 1 级
 - 1.2 安全 2 级
 - 1.3 安全 3 级
 - 1.4 安全 4 级
2. 术语和缩略语
 - 2.1 术语
 - 2.2 缩略语
3. 功能安全目标
4. 安全要求
 - 4.1 密码模块规定
 - 4.2 密码模块端口和界面
 - 4.3 角色、服务和认证
 - 4.3.1 角色
 - 4.3.2 服务
 - 4.3.3 操作人员认证
 - 4.4 有限状态模型
 - 4.5 物理安全
 - 4.5.1 总体物理安全要求
 - 4.5.2 单芯片密码模块
 - 4.5.3 多芯片嵌入式密码模块
 - 4.5.4 多芯片单机密码模块
 - 4.5.5 环境故障保护/测试
 - 4.6 运行环境
 - 4.6.1 操作系统要求
 - 4.7 密码密钥管理
 - 4.7.1 随机数生成器 (RNG)
 - 4.7.2 密钥生成
 - 4.7.3 密钥建立
 - 4.7.4 密钥输入和输出
 - 4.7.5 密钥存储
 - 4.7.6 密钥归零
 - 4.8 电磁干扰/电磁兼容性 (EMI/EMC)
 - 4.9 自测试
 - 4.9.1 开机测试
 - 4.9.2 条件测试
 - 4.10 设计保障
 - 4.10.1 配置管理
 - 4.10.2 交付与操作
 - 4.10.3 开发
 - 4.10.4 指南文件

4.11 对其他攻击的抑制

附录 A 文件要求归纳

附录 B 建议的软件开发实践规范

附录 C 密码模块安全策略

附录 D 精选文献

附录 E 相关网址

FIPS PUB 140-2
《密码模块安全要求》之
派生测试要求

2011 年 1 月 4 日（草案）

CMVP项目成员
(NIST、CSEC 和 CMVP 实验室)

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



美国商务部
代理部长: Rebecca M. Blank

国家标准和技术研究所
副部长兼所长: Patrick Gallagher

目录

1. 密码模块规定
 2. 密码模块端口和界面
 3. 角色、服务和鉴别
 - 3.1 角色
 - 3.2 服务
 - 3.3 操作员鉴别
 4. 有限状态模型
 5. 物理安全
 - 5.1 一般性物理安全要求
 - 5.2 单芯片密码模块
 - 5.3 多芯片嵌入式密码模块
 - 5.4 多芯片单机密码模块
 - 5.5 环境故障保护/测试
 6. 运行环境
 - 6.1 操作系统要求
 7. 密码密钥管理
 - 一般性要求
 - 7.1 随机数发生器 (RNG)
 - 7.2 密钥生成
 - 7.3 密钥建立
 - 7.4 密钥输入输出
 - 7.5 密钥存储
 - 7.6 密钥归零
 8. 电磁干扰/电磁兼容性 (EMI/EMC)
 9. 自测试
 - 9.1 开机测试
 - 9.2 条件测试
 10. 设计保障
 - 10.1 配置管理
 - 10.2 交付和操作
 - 10.3 开发
 - 10.4 指南文件
 11. 对其他攻击的抑制
- 附录 A 文件归纳
- 附录 B 建议的软件开发实践规范
- 附录 C 密码模块安全策略
 - C.1 密码模块安全策略的定义
 - C.2 密码模块安全策略的目的
 - C.3 密码模块安全策略的规定
- 变更通告 (略)