FIPS PUB 140-2
之密码模块验证体系
实施指南

内部资料

翻译：高卓

（美国）国家标准和技术研究所

加拿大通信安全组织

初版：2003 年 3 月 28 日
最新更新：2017 年 2 月 6 日

北京江南天安科技有限公司

目录

第 2 章　密码模块端口和接口

2.1　可信路径

第 3 章　角色、服务和鉴别

3.1　受权角色

3.2　路由器的绕过能力

3.3　软件模块的鉴别机制

3.4　多操作员鉴别

3.5　密码模块服务的文件要求

第 4 章　有限状态模型

第 5 章　物理安全

5.1　带风扇、通风孔或通风缝的安全 2 级密码模块的不透明和探测防范

5.2　测试防拆封封条

5.3　物理安全的前提假设

5.4　安全 3 级：硬涂层测试方法

5.5　物理安全 3 级 EFP/EFT 增强

第 6 章　运行环境

6.1　单操作员模式和多操作员并行

6.2　运行环境要求对 JAV 智能卡的适用性

6.3　操作系统通用准则要求修正

6.4　得到批准的完整性技术

第 7 章　密码密钥管理

7.1　转至 D.2

7.2　使用 IEEE 802.11i 密钥派生协议

7.3　转至 C.2

7.4　开机测试密钥归零

7.5　密钥建立方法的强度

7.6　转至 W.6

7.7　密钥建立和密钥输入输出

7.8　后处理在密钥生成方法中的使用

7.9　关键安全参数的规程化归零

7.10 SP 800-108 的密钥派生功能在 FIPS 模式下的使用

7.11 转至 W.6

7.12 RSA 签名算法的密钥生成

7.13 转至 W.1

7.14 熵警示

7.15 熵评价

7.16 保护存储的密钥和 CSP 的可接受算法

7.17 一次性可编程存储器归零

第 8 章　电磁干扰/电磁兼容性

第 9 章　自测试

9.1　密钥杂凑算法的已知答案测试

9.2　嵌入式密码算法的已知答案测试

9.3　完整性测试技术所用算法的已知答案测试

9.4　密码算法的已知答案测试

D.8 密钥协定方法

D.9 密钥传输方法

D.10 有关 SP 800-56C 厂家确认的要求

D.11 受支持工业协议的标注

D.12 有关 SP 800-133 厂家确认的要求

已撤销的指南章节（略）

变更一览（略）