

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

概述

一般性问题

- G.1 请求 CMVP 和 CAVP 提供指导
- G.2 完成测试报告：必须提供给 NIST 和 CSE 的信息
- G.3 部分验证和 FIPS 140-2 中不适用的领域
- G.4 密码模块的设计和测试
- G.5 保持软件或固件密码模块的验证合规
- G.6 同时带 FIPS 模式和非 FIPS 模式的模块
- G.7 厂家、实验室和 NIST/CSE 的关系
- G.8 重新验证要求
- G.9 FSM、安全策略、用户指南和密码官指南文件
- G.10 针对从 FIPS 140-1 转换 FIPS 140-2 的重新验证而进行的物理安全测试
- G.11 借助仿真器和模拟器的测试
- G.12 验证后质询
- G.13 验证信息格式说明
- G.14 密码算法和密钥长度转换验证
- G.15 转至 W.2
- G.16 提交报告前请求开具发票

第 1 章 密码模块规定

- 1.1 密码模块名称
- 1.2 FIPS 批准的运算模式
- 1.3 固件认定
- 1.4 密码算法验证证书捆绑
- 1.5 转至 A.1
- 1.6 转至 A.2
- 1.7 多个得到批准的运行模式
- 1.8 转至 W.13
- 1.9 混合型密码模块的定义和要求
- 1.10 转至 A.3
- 1.11 转至 D.1
- 1.12 转至 C.1
- 1.13 转至 A.4
- 1.14 转至 A.5
- 1.15 转至 A.6
- 1.16 软件模块
- 1.17 固件模块
- 1.18 PIV 参引提示
- 1.19 非批准运行模式
- 1.20 子芯片密码子系统
- 1.21 处理器算法加速器 (PAA)
- 1.22 模块计数定义

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

- 9.5 模块的开机初始化
- 9.6 执行 SP 800-56A 方案时的自测试
- 9.7 软件/固件装载测试
- 9.8 持续随机数发生器测试
- 9.9 生成密钥对时的成对一致性自测试
- 9.10 软件模块库的开机测试

第 10 章 设计保障

第 11 章 对其他攻击的抑制

- 11.1 对其他攻击的抑制

第 12 章 附录 A：文件要求归纳

第 13 章 附录 B：建议的软件开发实践规范

第 14 章 附录 C：密码模块安全策略

- 14.1 报告密码服务时的详细程度
- 14.2 报告对其他攻击的抑制时的详细程度
- 14.3 软件、固件和混合型模块的逻辑图
- 14.4 由操作员落实的防护措施
- 14.5 SP 800-90 DRBG 的关键安全参数

FIPA 140-2 附件 A：得到批准的安全功能

- A.1 SHS 算法和使用 SHS 算法的更高级密码算法的验证测试
- A.2 非 NIST 建议的非对称密钥大小和椭圆曲线的使用
- A.3 密码安全方法的厂家确认
- A.4 转至 W.7
- A.5 SP 800-38D 提出的密钥/IV 对的独一性要求
- A.6 转至 W.8
- A.7 转至 W.9
- A.8 HMAC-SHA-1-96 和压缩版 HMAC 的使用
- A.9 XTS-AES 密钥生成要求
- A.10 SP 800-38G 的厂家确认要求
- A.11 FIPS 202 定义的函数族的使用和测试要求
- A.12 SP 800-38A 附件的厂家确认要求

FIPA 140-2 附件 B：得到批准的保护轮廓

FIPA 140-2 附件 C：得到批准的随机数发生器

- C.1 转至 W.3
- C.2 转至 W.4

FIPA 140-2 附件 D：得到批准的密钥建立技术

- D.1 转至 W.10
- D.1 第 2 修订版 CAVP 有关 SP 800-56A 第 2 修订版厂家确认的要求
- D.2 可接受的密钥建立协议
- D.3 密钥建立的公钥有效性保障
- D.4 有关 SP 800-56B 厂家确认的要求
- D.5 转至 W.11
- D.6 有关 SP 800-132 厂家确认的要求
- D.7 转至 W.12

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）