智能卡 COS 产品密码检测准则

Cipher Test Criteria for Smart Card COS

国家密码管理局商用密码检测中心

2009 年 4 月

目　　次

智能卡 COS 产品密码检测准则

1 适用范围

本准则规定了智能卡 COS 产品的密码检测内容，适用于政府采购法规定范围内的智能卡 COS 产品密码检测。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

《智能 IC 卡及智能密码钥匙密码应用接口规范》 国家密码管理局

《随机性检测规范》 国家密码管理局

3 术语和定义、缩略语

3.1 术语和定义

3.1.1 对称密码算法 Symmetric Cryptographic Algorithm

加密密钥与解密密钥相同，或容易由其中任意一个密钥推导出另一个密钥，称该密码算法为对称密码算法。

3.1.2 非对称密码算法 Asymmetric Cryptographic Algorithm

加解密使用不同密钥的密码算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）必须保密，且由公钥求解私钥是计算不可行的。

3.1.3 杂凑算法 Hash Function

杂凑算法又称为散列算法、哈希算法或数据摘要算法，是能够将一个任意长的比特串映射到一个固定长的比特串的一类函数。

3.2 缩略语

COS　　Chip Operating System 芯片操作系统

4 检测内容

4.1 密码算法的正确性和一致性检测

智能卡 COS 产品使用的密码算法的正确性和一致性应满足：

（1）对称密码算法的正确性和一致性

智能卡 COS 产品中使用的对称密码算法，其运算结果应与标准数据和算法的标准运算结果相符。

（2）非对称密码算法的正确性和一致性

智能卡 COS 产品中使用的非对称密码算法，其运算结果应与标准数据和算法的标准运算结果相符。

（3）杂凑算法的正确性和一致性

智能卡 COS 产品中使用的杂凑算法，其运算结果应与标准数据和算法的标准运算结果相符。

4.2 密码性能检测

智能卡 COS 产品密码性能检测内容包括：

（1）对称密码算法运算速率

（2）非对称密码算法运算速率

（3）杂凑算法运算速率

4.3 随机数质量检测

智能卡 COS 产品生成和使用的随机数应符合《随机性检测规范》的要求。

4.4 素性检测

智能卡 COS 产品非对称密码算法所使用的素数应满足素性要求。

4.5 接口函数检测

智能卡 COS 产品的接口函数符合《智能 IC 卡及智能密码钥匙密码应用接口规范》第 7 章“接口函数原型”的规定。

4.6 安全性检测

智能卡 COS 产品的安全性符合《智能 IC 卡及智能密码钥匙密码应用接口规范》第 8 章“设备的安全要求”的规定。

5 文档要求

5.1 系统框架结构

以结构图的形式，说明整个智能卡 COS 产品的框架结构，包括智能卡 COS 产品的各子系统的构成、各子系统的功能和各子系统的实现原理，并附以详细的文字说明。

详细描述智能卡 COS 产品的安全机制、密码体制和密钥管理。

5.2 密码子系统框架结构

详细描述与密码实现和使用相关的身份鉴别、数据完整性、数据保密性等子系统框图和软件流程图。

5.3 源代码

开发者应提供与密码实现和使用相关的源代码，并提供源代码的说明文档。

5.4 不存在隐式通道的声明

开发者应提供智能卡 COS 产品中涉及密码的部分不存在隐式通道的声明文件。

5.5 密码自测试或自评估报告

开发者应提供智能卡 COS 产品的密码自测试或自评估报告。