安全隔离与信息交换产品

密码检测准则

Cipher Test Criteria for Secure Separation and Information Exchange Products

国家密码管理局商用密码检测中心

2009 年 4 月

目　　次

安全隔离与信息交换产品密码检测准则

1 范围

本准则规定了安全隔离与信息交换产品的密码检测内容，适用于政府采购法规定范围内的安全隔离与信息交换产品的密码检测。

2 规范性引用文件

下列文件中的条款通过本准则的引用而成为本准则的条款。凡是标注日期的引用文件，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准则，然而，鼓励根据本准则达成协议的各方研究是否可使用这些文件的最新版本。凡是不标注日期的引用文件，其最新版本适用于本准则。

GB/T 20279-2006　信息安全技术网络和终端设备隔离部件安全技术要求

《随机性检测规范》 国家密码管理局

3 术语和定义

3.1 安全隔离与信息交换产品 Secure Separation and Information Exchange Products

安全隔离与信息交换产品是指能够保证不同网络之间在网络协议终止的基础上，通过安全通道在实现网络隔离的同时进行安全数据交换的软硬件组合。

3.2 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。

3.3 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。

3.4 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。

3.5 密钥管理 Key Management

在既定安全策略指导下密钥的生成、分发、存储、使用、更新、备份、恢复、归档和销毁。

4 检测内容

4.1 密码算法的正确性和一致性检测

安全隔离与信息交换产品使用的密码算法应由密码硬件模块提供，密码硬件模块应从《商用密码通用产品名单》中选用。

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

安全隔离与信息交换产品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

安全隔离与信息交换产品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

安全隔离与信息交换产品使用的杂凑算法，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 密钥管理检测

安全隔离与信息交换产品中的密钥管理应满足：

（1） 密钥生成

安全隔离与信息交换产品能正确生成所用的各类密钥。生成的密钥应与密码算法强度相匹配。

（2） 密钥分发

密钥应按权限和密钥属性分发，防止分发过程中密钥泄漏或被篡改，并具备相应的应急处理和响应措施。

（3） 密钥存储

密钥应安全存储。对密钥存储的非授权操作应具备应急处理和响应措施。

（4） 密钥使用

密钥应按权限和密钥属性使用，并具备使用过程中的安全防护措施。

（5） 密钥更新

密钥应按照密钥属性进行更新，并在出现安全隐患时能及时更新。

（6） 密钥备份

密钥应按权限和密钥属性进行备份，并保证备份密钥的安全存储。

（7） 密钥恢复

密钥应按权限和密钥属性进行恢复。

（8） 密钥归档

密钥归档应防止密钥被非授权获取。归档的密钥只能用于确认该密钥以前提供的密码服务。

（9） 密钥销毁

安全隔离与信息交换产品应具备密钥销毁功能，销毁的密钥不能被部分或全部恢复。

4.3 随机数质量检测

安全隔离与信息交换产品生成和使用的随机数应符合《随机性检测规范》的要求。

5 文档要求

5.1 系统框架结构

以结构图的形式，说明产品的框架结构，包括安全隔离与信息交换产品的各个子系统的构成、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。

详细描述安全隔离与信息交换产品的安全机制、密码体制和密钥管理。

5.2 密码子系统框架结构

（1） 密码子系统的整体框架结构说明书

以结构图的形式，说明安全隔离与信息交换产品中密码子系统的框架结构，包括密码子系统的各个

功能模块的构成、各功能模块的功能和各功能模块的实现原理，并附以详细的文字说明。

（2） 密码子系统的功能模块流程说明书

以流程图的形式详细描述各子模块的工作原理和工作流程，详细说明各模块所调用的函数的名称和调用顺序，包括密钥生成、更新、销毁、归档等整个密钥生存周期各阶段所用到的函数，以及加密初始化函数、加密函数、解密函数、杂凑函数、签名函数、签名验证函数和加密后处理函数等。

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

开发者应提供安全隔离与信息交换产品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

开发者应提供安全隔离与信息交换产品的密码自测试或自评估报告。