ICS 35.040
L 80
备案号:58553—2017

GM

中华人民共和国密码行业标准

GM/T 0048—2016

智能密码钥匙密码检测规范

Cryptography test specification for cryptographic smart token

2016-12-23 发布　　2016-12-23 实施

国家密码管理局　　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：北京握奇智能科技有限公司、飞天诚信科技股份有限公司、北京海泰方圆科技有限公司、北京华大智宝电子系统有限公司、国家密码管理局商用密码检测中心、上海格尔软件股份有限公司、北京创原天地科技有限公司。

本标准主要起草人：汪雪林、李大为、陈国、朱鹏飞、蒋红宇、陈保儒、邓开勇、罗鹏、林春、雷银花、韩琳。

智能密码钥匙密码检测规范

1 范围

本标准规定了智能密码钥匙密码检测环境、检测内容和检测方法。

本标准适用于智能密码钥匙密码检测，也可用于指导智能密码钥匙的研制和使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 32915 信息安全技术 二元序列随机性检测方法

GM/T 0006 密码应用标识规范

GM/T 0017—2012 智能密码钥匙密码应用接口数据格式规范

GM/T 0027 智能密码钥匙技术规范

GM/T 0028 密码模块安全技术要求

GM/T 0039 密码模块安全检测要求

3 术语和定义

以下术语和定义适用于本文件。

3.1

智能密码钥匙 cryptographic smart token

实现密码运算、密钥管理功能，提供密码服务的终端密码设备。

3.2

命令 command

向智能密码钥匙发出的一条信息，该信息启动一个操作或请求一个应答。

3.3

响应 response

智能密码钥匙处理完成收到的命令报文后，返回给应用接口的报文。

3.4

消息鉴别码 message authentication code

又称消息认证码，是消息鉴别算法的输出。

3.5

管理员 PIN administrator PIN

管理员的口令，为 ASCII 字符串。

3.6

用户 PIN user PIN

用户的口令，为 ASCII 字符串。

3.7

应用　application

包括容器、设备认证密钥和文件的一种结构，具备独立的权限管理。

3.8

容器　container

特指密钥容器，是一个用于存放非对称密钥对和会话密钥的逻辑对象。

3.9

设备认证　device authentication

智能密码钥匙对应用程序的认证。

3.10

设备认证密钥　device authentication key

用于设备认证的密钥。

3.11

设备标签　label

设备的别名，可以由用户进行设定并存储于设备内部。

3.12

SM2 算法　SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为 256 比特。

3.13

SM3 算法　SM3 algorithm

一种密码杂凑算法，其输出为 256 比特。

3.14

SM4 算法　SM4 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

3.15

验证设备　verify equipment

用于密码算法基准运算的检测仪器或设备。

3.16

参考数据　reference data

用于判断密码算法实现正确性的一组数据，包括源数据和目标数据。

3.17

RSA 算法　Rivest-Shamir-Adleman algorithm；RSA

一种基于大整数因子分解问题的公钥密码算法。

4　缩略语

下列缩略语适用于本文件：

API　Application Program Interface 应用编程接口，简称应用接口

CBC　Cipher Block Chaining(分组密码的)密码分组链接(工作模式)

ECB　Electronic Codebook(分组密码的)电子密码本(工作模式)

ID　Identifier 标识符

MAC　Message Authentication Code 消息鉴别码

5 检测环境

5.1 检测环境拓扑图

智能密码钥匙检测环境参考拓扑图如图 1 所示。

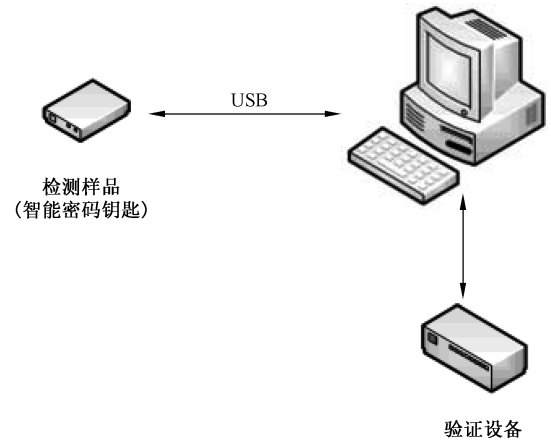

图 1 智能密码钥匙检测环境参考拓扑图

注：本标准只定义基于 USB 通讯接口的检测环境和检测方法，其他通讯接口由设备提供商提供相应的检测仪器和检测软件。

5.2 检测仪器

检测仪器见表 1。

表 1 检测仪器列表

仪器名称	备注
检测用 PC	用于运行操作系统及检测软件
验证设备	用于密码算法的基准运算，作为验证用的智能密码钥匙或其他设备

5.3 检测软件

检测软件见表 2。

表 2 检测软件列表

软件名称	备注
检测平台软件	用于执行检测的软件工具
操作系统	用于运行检测平台软件的操作系统

6 检测内容

6.1 功能检测

智能密码钥匙功能检测的目的是检测智能密码钥匙实现和运行的正确性。功能检测包括下列 6 个

方面的检测：

——设备管理；
——访问控制；
——应用管理；
——文件管理；
——容器管理；
——密码服务。

6.2 性能检测

智能密码钥匙性能检测的目的是检测智能密码钥匙文件操作和密码算法运算的效率。性能检测包括下列4个方面的检测：

——文件读写性能；
——对称算法性能；
——非对称算法性能；
——杂凑算法性能。

6.3 安全性检测

智能密码钥匙安全检测的目的是检测智能密码钥匙在设计和实现过程中的安全性，具体包括：规格，接口，角色、服务和鉴别，软件和固件安全，运行环境，物理安全，非入侵式攻击安全，敏感安全参数管理，自测试，生命周期保障，以及对其他攻击的缓解。

智能密码钥匙的安全性应满足GM/T 0028，并按照GM/T 0039对其安全性进行检测和评估。

7 检测方法

7.1 功能检测

7.1.1 设备管理

7.1.1.1 设置设备标签

检测目的：

验证是否能正确设置或修改设备的标签。

检测条件：

检测样品处于出厂状态。

检测过程：

a) 正常情况检测
   1) 步骤1：发送GM/T 0017—2012所规定的GetDevInfo指令，获取设备信息，记录其响应中的设备标签；
   2) 步骤2：发送GM/T 0017—2012所规定的SetLabel指令，设置设备标签，所设置的名称应与步骤1中所记录的设备标签不同；
   3) 步骤3：再次发送GM/T 0017—2012所规定的GetDevInfo指令，获取设备信息，其响应中的设备标签名称应与步骤2中设置的名称相同。
b) 异常情况检测
   1) 设备标签名称长度超过GM/T 0017—2012所规定的最大长度，应不成功；
   2) 设备标签长度为0，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.1.2 获取设备信息

检测目的：

验证是否能正确获取设备的一些特征信息，包括设备标签、厂商信息、支持的算法等。

检测条件：

检测样品处于出厂状态。

检测过程：

本检测项作为 7.1.1.1 的一部分进行检测。

7.1.2 访问控制

7.1.2.1 设备认证

检测目的：

验证设备是否能正确对应用程序进行认证。

检测条件：

检测样品处于出厂状态，当前设备认证密钥已知。

检测过程：

a) 正常情况检测

1) 步骤 1：发送 GM/T 0017—2012 所规定的 EnumApplication 指令，获取当前应用列表；
2) 步骤 2：发送 GM/T 0017—2012 所规定的 DevAuth 指令，使用正确的设备认证密钥；
3) 步骤 3：发送 GM/T 0017—2012 所规定的 CreateApplication 指令，创建一个应用，应用名称应与步骤 1 所获应用列表中的名称不同；
4) 步骤 4：发送 GM/T 0017—2012 所规定的 EnumApplication 指令，应成功，获取的当前应用列表中含有步骤 3 所创建的应用名称。

b) 异常情况检测

1) 使用错误的设备认证密钥，应不成功；
2) 发送 GM/T 0017—2012 所规定的 DevAuth 指令，使用错误的设备认证密钥，重复操作，直到响应“认证锁定”状态码；再次执行正常情况检测，应不成功；
3) 执行正常情况检测，跳过其中的步骤 2，应不成功；
4) 执行正常情况检测，在步骤 2 之后，清除安全状态，继续执行应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.2.2 修改设备认证密钥

检测目的：

验证是否能正确修改设备认证密钥。

检测条件：

检测样品处于出厂状态，当前设备认证密钥已知。

检测过程：

a) 正常情况检测

1) 步骤 1：发送 GM/T 0017—2012 所规定的 ChangeDevAuthKey 指令，使用正确的原设备

认证密钥，且新设备认证密钥应与原设备认证密钥不同；

2） 步骤 2：使用新设备认证密钥执行设备认证，应成功。

b） 异常情况检测

1） 使用错误的原设备认证密钥，应不成功；

2） 发送 GM/T 0017—2012 所规定的 DevAuth 指令，使用错误的设备认证密钥，重复操作，直到响应“认证锁定”状态码；再次执行正常情况检测，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.2.3 获取 PIN 信息

检测目的：

验证是否能正确获取指定应用下的 PIN 信息，包括最大重试次数、当前剩余重试次数，以及当前 PIN 是否为出厂默认 PIN。

检测条件：

检测所需的应用已存在，且用户 PIN 和管理员 PIN 为出厂默认 PIN。

检测过程：

a） 正常情况检测

1） 获取用户 PIN 信息：

——步骤 1：发送 GM/T 0017—2012 所规定的 GetPinInfo 指令，获取用户 PIN 信息，响应报文应与 GM/T 0017—2012 的规定相符；

——步骤 2：发送 GM/T 0017—2012 所规定的 ChangePIN 指令，修改用户 PIN；

——步骤 3：发送 GM/T 0017—2012 所规定的 VerifyPIN 指令，使用错误的用户 PIN；

——步骤 4：再次发送 GM/T 0017—2012 所规定的 GetPinInfo 指令，获取用户 PIN 信息。

2） 获取管理员 PIN 信息：

——步骤 1：发送 GM/T 0017—2012 所规定的 GetPinInfo 指令，获取管理员 PIN 信息，响应报文应与 GM/T 0017—2012 的规定相符；

——步骤 2：发送 GM/T 0017—2012 所规定的 ChangePIN 指令，修改管理员 PIN；

——步骤 3：发送 GM/T 0017—2012 所规定的 VerifyPIN 指令，使用错误的管理员 PIN；

——步骤 4：再次发送 GM/T 0017—2012 所规定的 GetPinInfo 指令，获取管理员 PIN 信息。

b） 异常情况检测

无。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.2.4 修改 PIN

检测目的：

验证是否能正确修改指定应用的管理员 PIN 或用户 PIN。

检测条件：

检测样品存在至少一个用户 PIN 未锁定、创建文件需要验证用户 PIN 的应用，应用名称和用户 PIN 已知；存在至少一个管理员 PIN 未锁定、创建文件需要验证管理员 PIN 的应用，应用名称和管理员 PIN 已知。

检测过程：

a) 正常情况检测

1) 修改用户 PIN：

——步骤 1：发送 GM/T 0017—2012 所规定的 ChangePIN 指令，使用正确的原用户 PIN，且新用户 PIN 应与原用户 PIN 不同；

——步骤 2：使用新用户 PIN 校验用户 PIN，应成功。

2) 修改管理员 PIN：

——步骤 1：发送 GM/T 0017—2012 所规定的 ChangePIN 指令，使用正确的原管理员 PIN，新管理员 PIN 应与原管理员 PIN 不同；

——步骤 2：使用新管理员 PIN 校验管理员 PIN，应成功。

b) 异常情况检测

1) 使用错误的原用户 PIN，应不成功；

2) 修改用户 PIN 成功后；再使用修改前的用户 PIN 作为原用户 PIN 修改用户 PIN，应不成功；

3) 发送 GM/T 0017—2012 所规定的 VeryfyPIN 指令，使用错误的用户 PIN 验证，重复操作，直到响应“PIN 码锁定”状态码；再次修改用户 PIN，应不成功；

4) 使用错误的原管理员 PIN 修改管理员 PIN，应不成功；

5) 修改管理员 PIN 成功后；再使用修改前的管理员 PIN 作为原管理员 PIN 修改管理员 PIN，应不成功；

6) 发送 GM/T 0017—2012 所规定的 VeryfyPin 指令，使用错误的管理员 PIN 验证，重复操作，直到响应“PIN 码锁定”状态码；再次修改管理员 PIN，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.2.5 校验 PIN

检测目的：

验证是否能正确校验指定应用的管理员 PIN 或用户 PIN。

检测条件：

检测样品存在至少一个用户 PIN 未锁定、创建文件需要验证用户 PIN 的应用，应用名称和用户 PIN 已知；存在至少一个管理员 PIN 未锁定、创建文件需要验证管理员 PIN 的应用，应用名称和管理员 PIN 已知。

检测过程：

a) 正常情况检测

1) 校验用户 PIN：

——步骤 1：选择一个用户 PIN 未锁定、创建文件需要验证用户 PIN 的应用，发送 GM/T 0017—2012 所规定的 EnumFiles 指令，获取当前文件列表；

——步骤 2：发送 GM/T 0017—2012 所规定的 VerifyPIN 指令，验证用户 PIN，使用正确的用户 PIN；

——步骤 3：发送 GM/T 0017—2012 所规定的 CreateFile 指令，创建一个文件，文件名应与当前文件列表中的名称不同，文件大小应不超过设备当前可用空间的大小；

——步骤 4：发送 GM/T 0017—2012 所规定的 EnumFiles 指令，应成功，所获取的当前文件列表中包含步骤 3 所使用的文件名称。

2） 校验管理员 PIN：

——步骤 1：选择一个管理员 PIN 未锁定、创建文件需要验证管理员 PIN 的应用，发送 GM/T 0017—2012 所规定的 EnumFiles 指令，获取当前文件列表；

——步骤 2：发送 GM/T 0017—2012 所规定的 VerifyPIN 指令，验证管理员 PIN，使用正确的管理员 PIN；

——步骤 3：发送 GM/T 0017—2012 所规定的 CreateFile 指令，创建一个文件，文件名应与当前文件列表中的名称不同，文件大小应不超过设备当前可用空间的大小；

——步骤 4：发送 GM/T 0017—2012 所规定的 EnumFiles 指令，应成功，获取的文件列表中包含步骤 3 所使用的文件名称。

b） 异常情况检测

1） 使用错误的用户 PIN 校验用户 PIN，应不成功；

2） 发送 GM/T 0017—2012 所规定的 VeryfyPIN 指令，使用错误的用户 PIN 验证，重复操作，直到响应“PIN 码锁定”状态码；再次校验正确的用户 PIN ，应不成功；

3） 使用错误的管理员 PIN 执行校验管理员 PIN ，应不成功；

4） 发送 GM/T 0017—2012 所规定的 VeryfyPIN 指令，使用错误的管理员 PIN 验证，重复操作，直到响应“PIN 码锁定”状态码；再次校验正确的管理员 PIN，应不成功；

5） 校验用户 PIN/管理员 PIN 成功后清除安全状态，后续操作应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.2.6 解锁 PIN

检测目的：

验证是否能正确解锁指定应用已锁定的用户 PIN。

检测条件：

检测样品管理员 PIN 未锁定、创建文件需要验证用户 PIN 的应用存在，应用名称、管理员 PIN 和用户 PIN 已知。

检测过程：

a） 正常情况检测

1） 步骤 1：发送 GM/T 0017—2012 所规定的 VeryfyPIN 指令，使用错误的用户 PIN 验证，重复操作，直到响应“PIN 码锁定”状态码；

2） 步骤 2：发送 GM/T 0017—2012 所规定的 UnblockPIN 指令，使用正确的管理员 PIN，新用户 PIN 与原用户 PIN 不同；

3） 步骤 3：使用新用户 PIN 作为正确的用户 PIN，执行校验用户 PIN 检测，应取得预期结果。

b） 异常情况检测

1） 在步骤 2 使用错误的管理员 PIN，应不成功；

2） 发送 GM/T 0017—2012 所规定的 VeryfyPIN 指令校验管理员 PIN，使用错误的管理员 PIN，重复操作，直到响应“PIN 码锁定”状态码；再解锁用户 PIN，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.2.7 清除应用安全状态

检测目的：

验证是否能正确清除指定应用的安全状态。

检测条件：

检测样品处于出厂状态，安全状态已满足。

检测过程：

本检测项作为 7.1.2.5 的一部分进行检测。

7.1.3 应用管理

7.1.3.1 创建应用

检测目的：

验证是否能正确在设备上创建应用。

检测条件：

检测样品处于出厂状态，安全状态已满足。

检测过程：

a) 正常情况检测

1) 步骤 1：发送 GM/T 0017—2012 所规定的 EnumApplication 指令，查找样品中已存在的应用；
2) 步骤 2：发送 GM/T 0017—2012 所规定的 CreateApplication 指令，使用与已存在的应用不相同的应用名称和正确的应用参数；
3) 步骤 3：发送 GM/T 0017—2012 所规定的 EnumApplication 指令，样品应存在步骤 2 创建的应用。

b) 异常情况检测

1) 安全状态不满足，应不成功；
2) 创建的应用空间大于设备剩余空间，应不成功；
3) 错误配置的应用参数，应不成功；
4) 创建相同名称的应用，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.3.2 枚举应用

检测目的：

验证是否能正确枚举设备上存在的所有应用。

检测条件：

检测所需的应用已存在。

检测过程：

本检测项作为 7.1.3.1 的一部分进行检测。

7.1.3.3 删除应用

检测目的：

验证是否能正确删除设备上的应用。

检测条件：

检测所需的应用已存在，安全状态已满足。

检测过程：

a) 正常情况检测

1） 步骤1：发送 GM/T 0017—2012 所规定的 DeleteApplication 指令，删除检测应用；
2） 步骤2：发送 GM/T 0017—2012 所规定的 EnumApplication 指令，返回已存在的所有应用名称，样品中应不含有步骤1删除的应用。

b） 异常情况检测
1） 安全状态不满足，应不成功；
2） 删除样品中不含有的应用，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.3.4 打开应用

检测目的：

验证是否能正确打开设备上的应用。

检测条件：

检测所需的应用已存在，且未打开。

检测过程：

a） 正常情况检测
1） 步骤1：发送 GM/T 0017—2012 所规定的 OpenApplication 指令，打开检测应用；
2） 步骤2：发送 GM/T 0017—2012 所规定的 VerifyPin 指令，使用正确的用户口令；
3） 步骤3：发送 GM/T 0017—2012 所规定的 CreateFile 指令，使用正确的文件属性信息，应执行成功。

b） 异常情况检测
1） 打开样品中不含有的应用，应不成功；
2） 应用已打开，再次打开该应用，应不成功；
3） 已有打开的应用，再打开新的应用，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.3.5 关闭应用

检测目的：

验证是否能正确关闭设备上的已打开的应用。

检测条件：

检测所需的应用已打开。

检测过程：

a） 正常情况检测
1） 步骤1：发送 GM/T 0017—2012 所规定的 CloseApplication 指令，命令报文包括已打开的应用 ID；
2） 步骤2：发送 GM/T 0017—2012 所规定的 VerifyPin 指令，使用正确的用户口令，应执行不成功。

b） 异常情况检测
关闭检测样品中不含有的应用，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.4 文件管理

7.1.4.1 创建文件

检测目的：

验证是否能正确在指定应用下创建文件。

检测条件：

检测所需的应用打开，安全状态已满足。

检测过程：

a) 正常情况检测

1) 步骤1：发送GM/T 0017—2012所规定的EnumFiles指令，查找应用中已存在的文件；
2) 步骤2：发送GM/T 0017—2012所规定的CreateFile指令，使用与已存在的文件不相同的文件名，应返回成功；
3) 步骤3：发送GM/T 0017—2012所规定的EnumFiles指令，应用中应存在步骤2创建的文件。

b) 异常情况检测

1) 安全状态不满足时，应建立文件失败；
2) 应用不存在，应建立文件失败；
3) 建立文件与已有文件同名，应建立文件失败；
4) 文件大小超出设备剩余空间，应建立文件失败。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.4.2 删除文件

检测目的：

验证是否能正确删除指定应用下的文件。

检测条件：

检测所需的应用打开，文件已存在，安全状态已满足。

检测过程：

a) 正常情况检测

1) 步骤1：发送GM/T 0017—2012所规定的EnumFiles指令，查找应用中已存在的文件；
2) 步骤2：发送GM/T 0017—2012所规定的DeleteFile指令，使用步骤1查找到的文件名、应用ID进行检测，应返回成功；
3) 步骤3：发送GM/T 0017—2012所规定的EnumFiles指令，应用中不存在步骤2删除的文件。

b) 异常情况检测

1) 安全状态不满足时，应不成功；
2) 应用ID不存在，应不成功；
3) 文件名不存在，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.4.3 枚举文件

检测目的：

验证是否能正确枚举指定应用下存在的所有文件。

检测条件：

检测所需的应用打开，文件已存在。

检测过程：

本检测项作为 7.1.4.1 的一部分进行检测。

7.1.4.4 获取文件信息

检测目的：

验证是否能正确获取指定应用下指定文件的属性信息。

检测条件：

检测所需应用已打开，安全状态已满足。

检测过程：

a） 正常情况检测

1） 步骤 1：发送 GM/T 0017—2012 所规定的 CreateFiles 指令，建立文件；

2） 步骤 2：发送 GM/T 0017—2012 所规定的 GetFileInfo 指令，使用正确的应用 ID 和文件名进行检测，应返回成功，得到文件的属性信息；

3） 步骤 3：对比属性信息中的文件大小、读权限和写权限信息，应与建立文件时一致。

b） 异常情况检测

1） 应用 ID 不存在，应不成功；

2） 文件名不存在，应不成功；

3） 安全状态不满足，应不成功；

4） 期望长度与文件属性信息结构长度不一致，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.4.5 读文件

检测目的：

验证是否能正确从指定文件的指定位置读取指定长度的数据。

检测条件：

检测所需应用已打开，安全状态已满足。

检测过程：

本检测项和 7.1.4.6 一同进行检测。

7.1.4.6 写文件

检测目的：

验证是否能正确向指定文件的指定位置写入指定长度的数据。

检测条件：

检测所需应用已打开，安全状态已满足。

检测过程：

a） 正常情况检测

1） 步骤1：发送GM/T 0017—2012所规定的WriteFile指令，向文件写入特定内容；
2） 步骤2：发送GM/T 0017—2012所规定的ReadFile指令，使用步骤1的偏移长度，从文件读取特定内容；
3） 步骤3：将步骤1写入的内容同步骤2读取内容进行比对，内容信息应一致。

b） 异常情况检测
1） 应用ID不存在，应不成功；
2） 文件名不存在，应不成功；
3） 安全状态不满足，应不成功；
4） 偏移值超出文件长度，应不成功；
5） 待返回长度超出通信缓冲区最大长度，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.5 容器管理

7.1.5.1 创建容器

检测目的：

验证是否能正确在指定的应用下创建容器。

检测条件：

检测所需的应用已打开，安全状态已满足。

检测过程：

a） 正常情况检测
1） 步骤1：发送GM/T 0017—2012所规定的CreateContainer指令，创建一个容器；
2） 步骤2：发送GM/T 0017—2012所规定的EnumContainer指令，返回已创建的容器名称，应用中应存在步骤1创建的容器。

b） 异常情况检测
1） 检测应用未打开，应不成功；
2） 安全状态不满足，应不成功；
3） 创建的容器空间大于应用剩余空间，应不成功；
4） 创建相同名称的容器，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.5.2 打开容器

检测目的：

验证是否能正确打开指定应用下的容器。

检测条件：

检测所需的应用已打开，容器已存在，且容器为新创建的容器。

检测过程：

a） 正常情况检测
1） 步骤1：发送GM/T 0017—2012所规定的OpenContainer指令，打开检测容器；
2） 步骤2：发送GM/T 0017—2012所规定的VerifyPin指令，使用正确的用户口令；
3） 步骤3：发送GM/T 0017—2012所规定的GenRSAKeyPair或GenECCKeyPair指令，应执行成功。

b） 异常情况检测

1） 检测应用未打开，应不成功；

2） 打开检测应用中不含有的容器，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.5.3 关闭容器

检测目的：

验证是否能正确关闭指定应用下已打开的容器。

检测条件：

检测所需的应用和容器已打开，且容器为新创建的容器。

检测过程：

a） 正常情况检测

1） 步骤 1：发送 GM/T 0017—2012 所规定的 CloseContainer 指令，命令报文包括已打开的应用 ID 和容器 ID；

2） 步骤 2：发送 GM/T 0017—2012 所规定的 VerifyPin 指令，使用正确的用户口令；

3） 步骤 3：发送 GM/T 0017—2012 所规定的 GenRSAKeyPair 或 GenECCKeyPair 指令，应执行不成功。

b） 异常情况检测

1） 检测应用未打开，应不成功；

2） 关闭检测应用中不含有的容器，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.5.4 枚举容器

检测目的：

验证是否能正确枚举指定应用下存在的所有容器。

检测条件：

检测所需的应用已打开，容器已存在。

检测过程：

本检测项作为 7.1.5.1 的一部分进行检测。

7.1.5.5 删除容器

检测目的：

验证是否能正确删除指定应用下指定的容器。

检测条件：

检测所需的应用已打开，安全状态已满足。

检测过程：

a） 正常情况检测

1） 步骤 1：发送 GM/T 0017—2012 所规定的 DeleteContainer 指令，删除检测容器；

2） 步骤 2：发送 GM/T 0017—2012 所规定的 EnumContainer 指令，返回已存在的所有容器名称，应用中应不存在步骤 1 删除的容器。

b) 异常情况检测

1) 检测应用未打开,应不成功;

2) 安全状态不满足,应不成功;

3) 删除检测样品中不含有的容器,应不成功。

通过标准:

正常情况检测和异常情况检测均得到预期结果。

7.1.5.6 获取容器信息

检测目的:

验证是否能正确获取指定应用下的指定容器的相关信息。

检测条件:

检测所需的应用和容器已打开。

检测过程:

本检测项作为 7.1.5.8 一部分进行检测。

7.1.5.7 导入数字证书

检测目的:

验证是否能正确向当前容器内导入指定类型的数字证书。

检测条件:

检测所需的应用和容器已打开,容器内已存在检测签名密钥对和加密密钥对,安全状态已满足。

检测过程:

本检测项和 7.1.5.8 一同进行检测。

7.1.5.8 导出数字证书

检测目的:

验证是否能正确从当前容器内导出指定类型的数字证书。

检测条件:

检测所需的应用和容器已打开,容器内已存在检测签名密钥对和加密密钥对,安全状态已满足。

检测过程:

a) 正常情况检测

1) 导出签名数字证书:

——步骤 1:发送 GM/T 0017—2012 所规定的 ExportPublicKey 指令,导出签名公钥;

——步骤 2:采用步骤 1 导出的签名公钥生成签名数字证书,并发送 GM/T 0017—2012 所规定的 ImportCertificate 指令,向检测容器内导入该签名数字证书;

——步骤 3:发送 GM/T 0017—2012 所规定的 GetContainerInfo 指令,检查步骤 2 导入的签名数字证书是否存在;

——步骤 4:发送 GM/T 0017—2012 所规定的 ExportCertificate 指令,导出签名数字证书;

——步骤 5:步骤 2 导入的签名数字证书和步骤 4 导出的签名数字证书内容应一致。

2) 导出加密数字证书:

——步骤 1:发送 GM/T 0017—2012 所规定的 ExportPublicKey 指令,导出加密公钥;

——步骤 2:采用步骤 1 导出的加密公钥生成加密数字证书,并发送 GM/T 0017—2012 所规定的 ImportCertificate 指令,向检测容器内导入该加密数字证书;

——步骤3：发送GM/T 0017—2012所规定的GetContainerInfo指令，检查步骤2导入的加密数字证书是否存在；

——步骤4：发送GM/T 0017—2012所规定的ExportCertificate指令，导出加密数字证书；

——步骤5：步骤2导入的加密数字证书和步骤4导出的加密数字证书内容应一致。

b） 异常情况检测

1） 检测应用未打开，应不成功；

2） 检测容器未打开，应不成功；

3） 从检测应用中不存在的容器导出数字证书，应不成功；

4） 容器内不存在对应类型的数字证书，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.6 密码服务

7.1.6.1 生成随机数

检测目的：

验证是否能正确生成指定长度的随机数。

检测条件：

检测样品处于出厂状态。

检测过程：

a） 正常情况检测

发送GM/T 0017—2012所规定的GenRandom指令，应返回相应长度随机数。

b） 异常情况检测

无。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.6.2 生成RSA签名密钥对

检测目的：

验证是否能正确在指定的应用和容器中生成RSA签名密钥对，并输出签名公钥。

检测条件：

检测所需应用和容器已打开，安全状态已满足。

检测过程：

a） 正常情况检测

1） 步骤1：发送GM/T 0017—2012所规定的GenRSAKeyPair指令，生成模长为2 048位的签名密钥对，返回签名公钥；

2） 步骤2：发送GM/T 0017—2012所规定的RSASignData指令，用步骤1生成的密钥对预设数据进行签名，返回签名结果；

3） 步骤3：采用步骤1返回的签名公钥验证步骤2返回的签名结果，应成功。

b） 异常情况检测

1） 检测应用未打开，应不成功；

2） 检测容器未打开，应不成功；

3） 安全状态不满足，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

注：如果 RSA 支持大于 2 048 位的模长，需要一并测试。

7.1.6.3 导入 RSA 加密密钥对

检测目的：

验证是否能正确在指定应用的容器中导入 RSA 加密公私钥对。

检测条件：

检测所需应用和容器已打开，安全状态已满足，容器中已有对应的 RSA 签名密钥对，且签名公钥已导出。

检测过程：

a） 正常情况检测

1） 步骤 1：发送 GM/T 0017—2012 所规定的 ImportRSAKeyPair 指令，导入模长为 2 048 位的 RSA 加密密钥对；

2） 步骤 2：发送 GM/T 0017—2012 所规定的 ImportSessionKey 指令，会话密钥采用和步骤 1 相同的 RSA 加密公钥加密；

3） 步骤 3：发送 GM/T 0017—2012 所规定的 Encrypt 指令，对预设数据采用步骤 2 导入的会话密钥进行加密，返回数据密文；

4） 步骤 4：用预设会话密钥解密数据密文，得到数据明文；

5） 步骤 5：比对预设数据和步骤 4 得到的数据明文应一致。

b） 异常情况检测

1） 检测应用未打开，应不成功；

2） 检测容器未打开，应不成功；

3） 安全状态不满足，应不成功；

4） 数据字段参数不正确，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

注：如果 RSA 支持大于 2 048 位的模长，需要一并测试。

7.1.6.4 RSA 签名

检测目的：

验证是否能正确使用指定签名私钥，对指定数据进行数字签名，并输出签名结果。

检测条件：

检测所需应用和容器已打开，容器中已存在用于检测的模长为 2 048 位的 RSA 签名密钥对，安全状态已满足。

检测过程：

a） 正常情况检测

1） 步骤 1：发送 GM/T 0017—2012 所规定的 ExportPublicKey 指令，导出模长为 2 048 位的 RSA 签名公钥；

2） 步骤 2：发送 GM/T 0017—2012 所规定的 RSASignData 指令，对预设数据进行签名，返回签名结果；

3） 步骤 3：采用步骤 1 导出的签名公钥验证步骤 2 返回的签名结果，应成功。

b） 异常情况检测

1） 检测应用未打开，应不成功；

2） 检测容器未打开，应不成功；

3） 安全状态不满足，应不成功；

4） 数据字段参数不正确，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

注： 如果 RSA 支持大于 2 048 位的模长，需要一并测试。

7.1.6.5 RSA 验签

检测目的：

验证是否能正确使用 RSA 公钥（从外部输入）对数据进行签名验证。

检测条件：

检测所需应用已存在。

检测过程：

a） 正常情况检测

1） 步骤 1：通过检测用模长为 2 048 位的 RSA 签名密钥对，对一预设数据进行签名，得到签名结果；

2） 步骤 2：发送 GM/T 0017—2012 所规定的 RSAVerify 指令，采用和步骤 1 相同的检测用 RSA 签名公钥验证步骤 1 得到的签名结果，应成功。

b） 异常情况检测

1） 检测应用未打开，应不成功；

2） 数据字段参数不正确和不一致，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

注： 如果 RSA 支持大于 2 048 位的模长，需要一并测试。

7.1.6.6 RSA 生成并导出会话密钥

检测目的：

验证是否能正确生成会话密钥并用外部公钥加密导出。

检测条件：

检测所需应用和容器打开，安全状态已满足。

检测过程：

a） 正常情况检测

1） 步骤 1：发送 GM/T 0017—2012 所规定的 RSAExportSessionKey 指令，返回会话密钥密文；

2） 步骤 2：用外部私钥解密步骤 1 返回的会话密钥密文，得到会话密钥明文；

3） 步骤 3：发送 GM/T 0017—2012 所规定的 Encrypt 指令，对预设数据采用步骤 1 生成的会话密钥进行加密，返回数据密文；

4） 步骤 4：采用会话密钥解密步骤 3 返回的数据密文，得到数据明文；

5） 步骤 5：比对预设数据和步骤 4 得到的数据明文应一致。

b） 异常情况检测

1） 检测应用未打开，应不成功；

2） 数据字段参数不正确，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.6.7 RSA 导出会话密钥

检测目的：

验证是否能正确使用外部公钥加密导出设备中的会话密钥。

检测条件：

检测所需应用和容器打开，安全状态已满足。

检测过程：

本检测项和 7.1.6.20 一同进行检测。

7.1.6.8 RSA 外来公钥计算

检测目的：

验证是否能正确使用外部传入的 RSA 公钥对输入数据做公钥运算，并输出加密结果。

检测条件：

检测样品处于出厂状态。

检测过程：

a） 正常情况检测

1） 步骤 1：发送 GM/T 0017—2012 所规定的 ExtRSAPubKeyOperation 指令，对预设数据进行加密，返回数据密文；

2） 步骤 2：解密步骤 1 返回的数据密文，得到数据明文；

3） 步骤 3：比对预设数据和步骤 2 得到的数据明文应一致。

b） 异常情况检测

数据字段参数不正确，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.6.9 生成 SM2 签名密钥对

检测目的：

验证是否能正确在指定应用的当前容器中生成 SM2 签名密钥对，并输出签名公钥。

检测条件：

检测所需的应用和容器已打开，安全状态已满足。

检测过程：

a） 正常情况检测

1） 步骤 1：发送 GM/T 0017—2012 所规定的 GenECCKeyPair 指令，生成 SM2 签名密钥对，返回签名公钥；

2） 步骤 2：发送 GM/T 0017—2012 所规定的 ECCSignData 指令，用步骤 1 生成的密钥对对预设数据进行签名，返回签名结果；

3） 步骤 3：采用步骤 1 返回的签名公钥验证步骤 2 返回的签名结果，应成功。

b） 异常情况检测

1） 检测应用未打开，应不成功；

2） 检测容器未打开，应不成功；

3） 安全状态不满足，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.6.10 导入 SM2 加密密钥对

检测目的：

验证是否能正确向指定应用的指定容器中导入 SM2 加密密钥对。

检测条件：

检测所需的应用和容器已打开，安全状态已满足，容器中已有对应的 SM2 签名密钥对，且签名公钥已导出。

检测过程：

a） 正常情况检测

1） 步骤 1：发送 GM/T 0017—2012 所规定的 ImportECCKeyPair 指令，导入 SM2 加密密钥对；

2） 步骤 2：发送 GM/T 0017—2012 所规定的 ImportSessionKey 指令，会话密钥采用和步骤 1 相同的 SM2 加密公钥加密；

3） 步骤 3：发送 GM/T 0017—2012 所规定的 Encrypt 指令，对预设数据采用步骤 2 导入的会话密钥进行加密，返回数据密文；

4） 步骤 4：用和步骤 2 相同的会话密钥解密数据密文，得到数据明文；

5） 步骤 5：比对预设数据和步骤 4 得到的数据明文应一致。

b） 异常情况检测

1） 检测应用未打开，应不成功；

2） 检测容器未打开，应不成功；

3） 安全状态不满足，应不成功；

4） 数据字段参数不正确，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.6.11 SM2 签名

检测目的：

验证是否能正确采用指定容器中 SM2 签名私钥对输入数据进行签名，并输出签名结果。

检测条件：

检测所需的应用和容器已打开，容器中已存在用于检测的 SM2 签名密钥对，安全状态已满足。

检测过程：

a） 正常情况检测

1） 输入为待签名数据的原文：

——步骤 1：发送 GM/T 0017—2012 所规定的 ExportPublicKey 指令，导出 SM2 签名公钥；

——步骤 2：发送 GM/T 0017—2012 所规定的 ECCSignData 指令，输入为待签名数据的原文，返回签名结果；

——步骤 3：采用步骤 1 导出的签名公钥对步骤 2 返回的签名结果进行验证，应成功。

2） 输入的待签名数据为原始数据的杂凑值：

——步骤 1：发送 GM/T 0017—2012 所规定的 ExportPublicKey 指令，导出 SM2 签名公钥；

——步骤 2：发送 GM/T 0017—2012 所规定的 ECCSignData 指令，输入的待签名数据为原始数据的杂凑值，返回签名结果；

——步骤 3：采用步骤 1 导出的签名公钥对步骤 2 返回的签名结果进行验证，应成功。

b） 异常情况检测

1） 检测应用未打开，应不成功；

2） 检测容器未打开，应不成功；

3） 安全状态不满足，应不成功；

4） 检测容器中不存在对应的签名密钥对，应不成功；

5） 数据字段参数不正确，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.6.12 SM2 验签

检测目的：

验证是否能正确用 SM2 公钥（从外部输入）对数据进行签名验证。

检测条件：

检测所需的应用已存在。

检测过程：

a） 正常情况检测

1） 步骤 1：通过检测用 SM2 签名密钥对，对一预设数据进行签名，得到签名结果；

2） 步骤 2：发送 GM/T 0017—2012 所规定的 ECCVerify 指令，采用和步骤 1 相同的检测用 SM2 签名公钥验证步骤 1 得到的签名结果，应成功。

b） 异常情况检测

1） 检测应用未打开，应不成功；

2） 数据字段参数不正确或不一致，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.6.13 SM2 生成并导出会话密钥

检测目的：

验证是否能正确在指定的容器中生成会话密钥并用外部公钥加密导出。

检测条件：

检测所需的应用和容器已打开，安全状态已满足。

检测过程：

a） 正常情况检测

1） 步骤 1：发送 GM/T 0017—2012 所规定的 ECCExportSessionKey 指令，返回会话密钥密文；

2） 步骤 2：用外部私钥解密步骤 1 返回的会话密钥密文，得到会话密钥明文；

3） 步骤 3：发送 GM/T 0017—2012 所规定的 Encrypt 指令，对预设数据采用步骤 1 生成的会话密钥进行加密，返回数据密文；

4） 步骤 4：采用会话密钥解密步骤 3 返回的数据密文，得到数据明文；

5） 步骤 5：比对预设数据和步骤 4 得到的数据明文应一致。

b) 异常情况检测

1) 检测应用未打开,应不成功;

2) 检测容器未打开,应不成功;

3) 安全状态不满足,应不成功;

4) 会话密钥算法标识不正确,应不成功;

5) 数据字段参数不正确,应不成功。

通过标准:

正常情况检测和异常情况检测均得到预期结果。

7.1.6.14 SM2 导出会话密钥

检测目的:

验证是否能正确使用外部公钥加密导出指定容器中的会话密钥。

检测条件:

检测所需应用和容器打开,安全状态已满足。

检测过程:

本检测项和 7.1.6.20 一同进行检测。

7.1.6.15 SM2 外来公钥加密

检测目的:

验证是否能正确使用外部传入的 SM2 公钥对输入数据做加密运算,并输出加密结果。

检测条件:

检测样品处于出厂状态。

检测过程:

a) 正常情况检测

1) 步骤 1:发送 GM/T 0017—2012 所规定的 ExtECCEncrypt 指令,对预设数据进行加密,返回数据密文;

2) 步骤 2:解密步骤 1 返回的数据密文,得到数据明文;

3) 步骤 3:比对预设数据和步骤 2 得到的数据明文应一致。

b) 异常情况检测

数据字段参数不正确,应不成功。

通过标准:

正常情况检测和异常情况检测均得到预期结果。

7.1.6.16 SM2 生成密钥协商参数并输出

检测目的:

验证是否能正确使用 SM2 密钥协商算法,为计算会话密钥而产生协商参数,并输出临时 SM2 密钥对的公钥及密钥协商句柄。

检测条件:

检测所需的应用和容器已打开,容器中已存在用于检测的 SM2 加密密钥对。

检测过程:

本检测项和 7.1.6.18 一同进行检测。

7.1.6.17 SM2 产生协商数据并计算会话密钥

检测目的：

验证是否能正确使用 SM2 密钥协商算法，产生协商参数并计算会话密钥，并输出临时 SM2 密钥对的公钥及产生的会话密钥 ID。

检测条件：

检测所需的应用和容器已打开，容器中已存在用于检测的 SM2 加密密钥对，且其公钥已导出。

检测样品作为响应方。

检测过程：

a) 正常情况检测

1) 步骤 1：发起方生成临时 SM2 公钥；
2) 步骤 2：发送 GM/T 0017—2012 所规定的 GenerateAgreementDataAndKeyWithECC 指令，返回响应方临时 SM2 公钥及会话密钥 ID；
3) 步骤 3：发起方计算得到会话密钥；
4) 步骤 4：发送 GM/T 0017—2012 所规定的 Encrypt 指令，采用步骤 2 返回的响应方会话密钥 ID 对应的会话密钥对预设数据进行加密，返回数据密文；
5) 步骤 5：发起方采用发起方会话密钥对步骤 4 返回的数据密文进行解密，得到数据明文；
6) 步骤 6：比对预设数据和步骤 5 得到的数据明文应一致。

b) 异常情况检测

1) 检测应用未打开，应不成功；
2) 检测容器未打开，应不成功；
3) 数据字段参数不正确，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.6.18 SM2 计算会话密钥

检测目的：

验证是否能正确使用 SM2 密钥协商算法，使用自身密钥协商句柄和响应方的协商参数计算会话密钥，并输出会话密钥 ID。

检测条件：

检测所需的应用和容器已打开，容器中已存在用于检测的 SM2 加密密钥对，且其公钥已导出。

检测样品作为发起方。

检测过程：

a) 正常情况检测

1) 步骤 1：发送 GM/T 0017—2012 所规定的 GenerateAgreementDataWithECC 指令，返回发起方临时 SM2 公钥及密钥协商句柄；
2) 步骤 2：响应方生成临时 SM2 公钥，并计算得到会话密钥；
3) 步骤 3：发送 GM/T 0017—2012 所规定的 GenerateKeyWithECC 指令，返回发起方会话密钥 ID；
4) 步骤 4：发送 GM/T 0017—2012 所规定的 Encrypt 指令，采用步骤 3 返回的发起方会话密钥 ID 对应的会话密钥对预设数据进行加密，返回数据密文；
5) 步骤 5：响应方采用响应方会话密钥对步骤 4 返回的数据密文进行解密，得到数据明文；
6) 步骤 6：比对预设数据和步骤 5 得到的数据明文应一致。

b） 异常情况检测

1） 检测应用未打开，应不成功；

2） 检测容器未打开，应不成功；

3） 数据字段参数不正确，应不成功。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.6.19 导出公钥

检测目的：

验证是否能正确从指定容器中导出公钥。

检测条件：

检测所需的应用和容器已打开，容器中已存在用于检测的 RSA 加密密钥对和 SM2 加密密钥对。

检测过程：

本检测项作为 7.1.6.11 的一部分进行检测。

7.1.6.20 导入加密会话密钥

检测目的：

验证是否能正确导入密文会话密钥，对会话密钥进行加密操作的公钥为指定应用的指定容器中的加密公钥。

检测条件：

检测所需的应用和容器已打开，容器中已存在用于检测的 RSA 加密密钥对和 SM2 加密密钥对且公钥已导出，安全状态已满足。

检测过程：

a） 正常情况检测

1） 容器为 RSA 类型：

——步骤 1：发送 GM/T 0017—2012 所规定的 ImportSessionKey 指令，对预设会话密钥采用检测容器中已导出的 RSA 加密公钥加密，返回会话密钥 ID；

——步骤 2：发送 GM/T 0017—2012 所规定的 RSAExportSessionKeyEx 指令，用 RSA 外部公钥导出步骤 1 导入的会话密钥，返回会话密钥密文；

——步骤 3：用 RSA 外部私钥解密步骤 2 返回的会话密钥密文，得到会话密钥明文；

——步骤 4：比对预设会话密钥和步骤 3 得到的会话密钥应一致；

——步骤 5：发送 GM/T 0017—2012 所规定的 DestroySessionKey 指令，销毁步骤 1 导入的会话密钥。

2） 容器为 SM2 类型：

——步骤 1：发送 GM/T 0017—2012 所规定的 ImportSessionKey 指令，对预设会话密钥采用检测容器中已导出的 SM2 加密公钥加密，返回会话密钥 ID；

——步骤 2：发送 GM/T 0017—2012 所规定的 ECCExportSessionKeyEx 指令，用 SM2 外部公钥导出步骤 1 导入的会话密钥，返回会话密钥密文；

——步骤 3：用 SM2 外部私钥解密步骤 2 返回的会话密钥密文，得到会话密钥明文；

——步骤 4：比对预设会话密钥和步骤 3 得到的会话密钥应一致；

——步骤 5：发送 GM/T 0017—2012 所规定的 DestroySessionKey 指令，销毁步骤 1 导入的会话密钥。

b) 异常情况检测

1) 检测应用未打开,应不成功;
2) 检测容器未打开,应不成功;
3) 安全状态不满足,应不成功;
4) 对应的密钥对不存在,应不成功;
5) 容器空间不足,应不成功;
6) 会话密钥算法标识不支持,应不成功。

通过标准:

正常情况检测和异常情况检测均得到预期结果。

7.1.6.21 加密初始化

检测目的:

验证是否能正确进行加密操作前的参数设置。

检测条件:

用于对称加密的会话密钥已导入,参考数据(包括源数据和目标数据)已准备好。

检测过程:

本检测项作为 7.1.6.18 的一部分进行检测。

7.1.6.22 单组数据加密

检测目的:

验证是否能正确进行分组密码加密运算,包括 ECB 和 CBC 模式。

检测条件:

用于对称加密的会话密钥已导入,参考数据(包括源数据和目标数据)已准备好。

检测过程:

a) 正常情况检测

1) 步骤 1:选择至少 10 组参考数据,对各组数据依次执行步骤 2～步骤 3;
2) 步骤 2:发送 GM/T 0017—2012 所规定的 EncryptInit 指令,算法标识至少支持 GM/T 0006 所规定的 SGD_SM4_ECB 和 SGD_SM4_CBC;
3) 步骤 3:发送 GM/T 0017—2012 所规定的 Encrypt 指令,对源数据进行加密,并输出加密结果;
4) 步骤 4:步骤 3 返回的加密结果和目标数据进行比对,应完全一致。

b) 异常情况检测

无。

通过标准:

正常情况检测和异常情况检测均得到预期结果。

7.1.6.23 多组数据加密

检测目的:

验证是否能正确进行多组密码加密运算,包括 ECB 和 CBC 模式。

检测条件:

用于对称加密的会话密钥已导入,参考数据(包括源数据和目标数据)已准备好。

检测过程:

a) 正常情况检测

1） 步骤1：发送GM/T 0017—2012所规定的EncryptInit指令，算法标识至少支持GM/T 0006所规定的SGD_SM4_ECB和SGD_SM4_CBC；
2） 步骤2：依次发送GM/T 0017—2012所规定的EncryptUpdate指令，分段发送参考源数据，并输出加密结果；
3） 步骤3：发送GM/T 0017—2012所规定的EncryptFinal指令，对源数据加密结束，并输出加密结果；
4） 步骤4：步骤2和步骤3返回的加密结果和目标数据进行比对，应完全一致。

b） 异常情况检测

无。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.6.24 结束加密

检测目的：

验证是否能正确结束一次加密操作，并输出剩余加密结果。

检测条件：

用于对称加密的会话密钥已导入，参考数据（包括源数据和目标数据）已准备好。

检测过程：

本检测项作为7.1.6.23的一部分进行检测。

7.1.6.25 解密初始化

检测目的：

验证是否能正确进行解密操作前的参数设置。

检测条件：

用于对称解密的会话密钥已导入，参考数据（包括源数据和目标数据）已准备好。

检测过程：

本检测项作为7.1.6.18的一部分进行检测。

7.1.6.26 单组数据解密

检测目的：

验证是否能正确进行单组密码解密运算，包括ECB和CBC模式。

检测条件：

用于对称解密的会话密钥已导入，参考数据（包括源数据和目标数据）已准备好。

检测过程：

a） 正常情况检测
1） 步骤1：选择至少10组参考数据，对各组数据依次执行步骤2～步骤3；
2） 步骤2：发送GM/T 0017—2012所规定的DecryptInit指令，算法标识至少支持GM/T 0006所规定的SGD_SM4_ECB和SGD_SM4_CBC；
3） 步骤3：发送GM/T 0017—2012所规定的Decrypt指令，对源数据进行解密，并输出解密结果；
4） 步骤4：步骤3返回的解密结果和目标数据进行比对，应完全一致。

b） 异常情况检测

无。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.6.27 多组数据解密

检测目的：

验证是否能正确进行多组密码解密运算，包括 ECB 和 CBC 模式。

检测条件：

用于对称解密的会话密钥已导入，参考数据（包括源数据和目标数据）已准备好。

检测过程：

a） 正常情况检测

1） 步骤 1：发送 GM/T 0017—2012 所规定的 DecryptInit 指令，算法标识至少支持 GM/T 0006 所规定的 SGD_SM4_ECB 和 SGD_SM4_CBC；

2） 步骤 2：发送 GM/T 0017—2012 所规定的 DecryptUpdate 指令，对源数据的每一组分组长度的数据依次进行解密，并输出解密结果；

3） 步骤 3：依次发送 GM/T 0017—2012 所规定的 DecryptFinal 指令，分段发送参考源数据，并输出解密结果；

4） 步骤 4：步骤 2 和步骤 3 返回的解密结果和目标数据进行比对，应完全一致。

b） 异常情况检测

无。

通过标准：

正常情况检测和异常情况检测均得到预期结果。

7.1.6.28 结束解密

检测目的：

验证是否能正确结束一次解密操作，并输出剩余解密结果。

检测条件：

用于对称解密的会话密钥已导入，参考数据（包括源数据和目标数据）已准备好。

检测过程：

本检测项作为 7.1.6.27 的一部分进行检测。

7.1.6.29 密码杂凑初始化

检测目的：

验证是否能正确进行初始化密码杂凑计算操作，指定计算密码杂凑的算法。

检测条件：

参考数据，包括源数据和对应 GM/T 0017—2012 所规定算法的目标数据。

检测过程：

本检测项作为 7.1.6.18 的一部分进行检测。

7.1.6.30 单组数据密码杂凑

检测目的：

验证是否能正确对单组数据进行密码杂凑运算。

检测条件：

参考数据，包括源数据和对应 GM/T 0017—2012 所规定算法的目标数据。

检测过程：

a） 正常情况检测

1） 步骤1：选择至少10组参考数据，对各组数据依次执行步骤2～步骤3；

2） 步骤2：发送GM/T 0017—2012所规定的DigestInit指令，设置摘要算法，所使用的算法包括SM3以及样品支持的算法；

3） 步骤3：发送GM/T 0017—2012所规定的Digest指令，使用预设的参考源数据计算杂凑值，其响应中包含的杂凑值应与对应的参考结果数据相符。

b） 异常情况检测

无。

通过标准：

正常情况检测得到预期结果。

7.1.6.31 多组数据密码杂凑

检测目的：

验证是否能正确队对多组数据进行密码杂凑运算。

检测条件：

参考数据，源数据和对应GM/T 0017—2012所规定算法的结果数据。

检测过程：

a） 正常情况检测

1） 步骤1：选择至少10组参考数据，对各组数据依次执行步骤2～步骤4；

2） 步骤2：发送GM/T 0017—2012所规定的DigestInit指令，设置摘要算法，所使用的算法包括SM3以及样品支持的算法；

3） 步骤3：依次发送多条GM/T 0017—2012所规定的DigestUpdate指令，分段发送预设的参考源数据，直到全部发送完毕，条数不少于3条；

4） 步骤4：发送GM/T 0017—2012所规定的DigestFinal指令，其响应中包含的杂凑值应与对应的参考结果数据相符。

b） 异常情况检测

无。

通过标准：

正常情况检测得到预期结果。

7.1.6.32 结束密码杂凑

检测目的：

验证是否能正确结束多组数据的密码杂凑计算操作，并输出密码杂凑结果。

检测条件：

参考数据，包括源数据和对应GM/T 0017—2012所规定算法的结果数据。

检测过程：

本检测项作为7.1.6.18的一部分进行检测。

7.1.6.33 消息鉴别码运算初始化

检测目的：

验证是否能正确进行初始化消息鉴别码计算操作，设置计算消息鉴别码的所需参数。

检测条件：

参考数据，包括源数据、密钥、参数和对应 GM/T 0017—2012 所规定算法的结果数据；至少存在一个可导入密钥的应用及容器。

检测过程：

本检测项作为 7.1.6.18 的一部分进行检测。

7.1.6.34 单组数据消息鉴别码运算

检测目的：

验证是否能正确进行单组数据消息鉴别码运算。

检测条件：

参考数据，包括源数据、密钥、参数和对应 GM/T 0017—2012 所规定算法的结果数据；至少存在一个可导入密钥的应用及容器。

检测过程：

a) 正常情况检测

1) 步骤 1：选择至少 10 组参考数据，对各组数据依次执行步骤 2～步骤 3；
2) 步骤 2：导入参考数据中的密钥；
3) 步骤 3：发送 GM/T 0017—2012 所规定的 MacInit 指令，根据参考数据设置算法等参数，所使用的算法包括 SM4 以及样品支持的算法；
4) 步骤 4：发送 GM/T 0017—2012 所规定的 Mac 指令，使用预设的参考源数据计算消息鉴别码，其响应中包含的消息鉴别码应与对应的参考结果数据相符。

b) 异常情况检测

无。

通过标准：

正常情况检测得到预期结果。

7.1.6.35 多组数据消息鉴别码运算

检测目的：

验证是否能正确进行多组数据消息鉴别码运算。

检测条件：

参考数据，包括源数据、密钥、参数和对应 GM/T 0017—2012 所规定算法的结果数据；至少存在一个可导入密钥的应用及容器。

检测过程：

a) 正常情况检测

1) 步骤 1：选择至少 10 组参考数据，对各组数据依次执行步骤 2～步骤 4；
2) 步骤 2：发送 GM/T 0017—2012 所规定的 MacInit 指令，根据参考数据设置算法等参数，所使用的算法包括 SM4 以及样品支持的算法；
3) 步骤 3：依次发送多条 GM/T 0017—2012 所规定的 MacUpdate 指令，分段发送预设的参考源数据，直到全部发送完毕，条数不少于 3 条；
4) 步骤 4：发送 GM/T 0017—2012 所规定的 MacFinal 指令，其响应中包含的消息鉴别码应与对应的参考结果数据相符。

b) 异常情况检测

无。

通过标准：

正常情况检测得到预期结果。

7.1.6.36 结束消息鉴别码运算

检测目的：

验证是否能正确结束多组数据的消息鉴别码运算，并输出消息鉴别码结果。

检测条件：

参考数据，包括源数据、密钥、参数和对应 GM/T 0017—2012 所规定算法的结果数据；至少存在一个可导入密钥的应用及容器。

检测过程：

本检测项作为 7.1.6.35 的一部分进行检测。

7.1.6.37 销毁会话密钥

检测目的：

验证是否能正确销毁当前容器中指定的会话密钥。

检测条件：

检测所需的应用和容器已打开，加密会话密钥已存在，安全状态已满足。

检测过程：

本检测项作为 7.1.6.20 的一部分进行检测。

7.1.6.38 随机数质量检测

检测目的：

验证生成的随机数质量是否满足要求。

检测条件：

样品的随机数生成器能正常工作。

检测过程：

a) 步骤 1：发送 GM/T 0017—2012 所规定的生成随机数指令，采集 10^3 个随机数样本，每个样本长度选取 10^6 比特；

b) 步骤 2：对每一个样本按照 GB/T 32915 定义的检测方法进行检测，分别得到每一个随机性检测项目的 P-value 值，记录这些结果。

通过标准：

对于每一个随机性检测项目，统计 P-value 值不小于显著性水平 $\alpha=0.01$（表示该样品通过该项检测）的样品个数。如果通过的样本个数不少于 981，则随机数发生器通过此项检测；否则，未通过此项检测。

7.1.6.39 素性检测

检测目的：

验证生成的密钥对参数质量是否满足要求。

检测条件：

样品提供仅用于素性检测的扩展检测接口。

检测过程：

a) 步骤 1：发送 GM/T 0017—2012 所规定的 GenRSAKeyPair 指令，生成 1 000 对模长为 2 048 位的 RSA 密钥对参数并输出；

b) 步骤2：对此1 000对RSA密钥参数，采用概率性素数检测Miller-Rabin算法进行检测。假设样本RSA参数的位长为k比特，则存在安全参数t，使得RSA参数发生错误的概率小于等于$1/2^{80}$。

通过标准：

所有k比特的RSA参数样本均能通过最小t值的Miller-Rabin检测。

7.2 性能检测

7.2.1 文件读写性能

7.2.1.1 文件读性能检测

检测目的：

验证文件的读性能是否满足要求。

检测条件：

待读取文件已存在，且用户权限满足读要求。

检测过程：

发送GM/T 0017—2012所规定的ReadFile指令，从检测样品中读取不同长度的二进制数据，重复操作N次，测量其完成时间T。$L\times N\geqslant 20\ 480$字节，$L$分别取：64字节、128字节以及送检单位建议的长度。检测结果取平均值。

通过标准：

记录检测结果。

7.2.1.2 文件写性能检测

检测目的：

验证文件的写性能是否满足要求。

检测条件：

待读写文件已存在，且用户权限满足读要求。

检测过程：

发送GM/T 0017—2012所规定的WriteFile指令，将不同长度的数据发送给检测样品进行二进制写操作，重复操作N次，测量其完成时间T。$L\times N\geqslant 20\ 480$字节，$L$分别取：64字节、128字节以及送检单位建议的长度。检测结果取平均值。

通过标准：

记录检测结果。

7.2.2 对称算法性能

检测目的：

验证对称算法加解密性能是否满足要求。

检测条件：

加解密密钥已存在，加解密初始化已完成。

检测过程：

将不同长度的数据发送给检测样品进行加密或解密操作，重复操作N次，测量其完成时间T。用于检测的数据由检测机构选定。$L\times N\geqslant 20\ 480$字节，$L$分别取：算法分组长度，以及送检单位建议的长度。相同数据长度的检测结果取平均值。

通过标准：

性能满足 GM/T 0027 的要求。

7.2.3 非对称算法性能

检测目的：

验证非对称算法密钥对生成、数字签名、验签、加密、解密运算性能是否满足要求。

检测条件：

签名密钥对和加密密钥对已存在。

检测过程：

a) 密钥对生成性能检测

检测样品生成 N 对密钥对($N \geqslant 500$)，测量其完成时间。检测结果取平均值。

b) 数字签名和验签性能检测

将定长的数据发送给检测样品，用特定的密钥进行数字签名或签名验证操作，重复操作 N 次($N \geqslant 1\ 000$)，测量其完成时间 T。用于检测的数据和密钥由检测机构选定。检测结果取平均值。

c) 加密和解密性能检测

将定长的数据发送给检测样品，用特定的密钥进行加密或解密操作，重复操作 N 次($N \geqslant 1\ 000$)，测量其完成时间 T。用于检测的数据和密钥由检测机构选定。检测结果取平均值。

通过标准：

性能满足 GM/T 0027 的要求。

7.2.4 杂凑算法性能

检测目的：

验证密码杂凑性能是否满足要求。

检测条件：

杂凑初始化已完成。

检测过程：

将不同长度的数据发送给检测样品进行杂凑运算，重复操作 N 次，测量其完成时间 T。用于检测的数据由检测机构选定。$L \times N \geqslant 20\ 480$ 字节，L 分别取：16 字节、32 字节、64 字节、128 字节以及送检单位建议的长度。检测结果取平均值。

通过标准：

性能满足 GM/T 0027 的要求。

7.3 安全性检测

对智能密码钥匙的安全性检测和评估，按照 GM/T 0039 进行。

参 考 文 献

[1] GB/T 32907 信息安全技术 SM4 分组密码算法
[2] GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法(所有部分)
[3] GB/T 32905 信息安全技术 SM3 密码杂凑算法
[4] GM/T 0009 SM2 密码算法使用规范
[5] GM/T 0016 智能密码钥匙密码应用接口规范