ICS 35.040
L 80
备案号:58554—2017

GM

中华人民共和国密码行业标准

GM/T 0049—2016

密码键盘密码检测规范

Cryptography test specification for EPP

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：深圳市证通电子股份有限公司、国家密码管理局商用密码检测中心、长城信息产业股份有限公司、上海爱信诺航芯电子科技有限公司、深圳市凯明杨科技有限公司。

本标准主要起草人：秦云川、黄洪、余思洋、张卫军、张文、朱文楚、李大为、邓开勇、罗鹏、林春、曾立志、张衡、陈锦玲、刘红明、卢雪明。

密码键盘密码检测规范

1 范围

本标准规定了密码键盘产品的安全等级划分、检测内容及检测方法、合格判定规则。

本标准适用于密码键盘产品的密码检测、检验及分级。

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 21078.1—2007 银行业务 个人识别码的管理与安全 第1部分：ATM和POS系统中联机PIN处理的基本原则和要求

GB/T 32915—2016 信息安全技术 二元序列随机性检测方法

GB/T 32918.3—2016 信息安全技术 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议

GM/Z 0001 密码术语

GM/T 0008—2012 安全芯片密码检测准则

GM/T 0028—2014 密码模块安全技术要求

GM/T 0039 密码模块安全检测要求

ISO/IEC 18032:2005 信息技术 安全技术 素数生成(Information technology—Security techniques—Prime number generation)

3 术语和定义

GB/T 21078.1—2007、GM/T 0028—2014和GM/Z 0001界定的以及下列术语和定义适用于本文件。

3.1

密码键盘 encrypting PIN Pad; EPP

用于保护PIN输入安全并对PIN进行加密的独立式密码模块。包括POS主机等设备的外接加密密码键盘和无人值守(自助)终端的加密PIN键盘。

3.2

外部认证 external authentication

密码键盘的身份认证。认证方法可以为基于随机数的单向认证或基于随机数的公钥认证。基于随机数的单向认证方法采用对称算法，基于随机数的公钥认证采用非对称算法。

3.3

上电自检检测 power-on self-test

在键盘上电时，由密码键盘自动执行的功能正确性检测。

3.4

软件/固件完整性检测 software/firmware integrity test

对密码键盘软件和固件的完整性进行的检测。

3.5

运行前条件自检检测　conditional self-test

在密码键盘运行之前，当规定的检测条件出现时，由密码键盘执行的功能正确性检测。

注：改写 GM/T 0028—2014，定义 3.12。

3.6

PIN 数据块检测　PIN block test

对密码键盘生成的 PIN 数据块正确性进行的检测。

3.7

对称密码算法加密和解密检测　symmetric cryptographic algorithm encryption and decryption test

对密码键盘中对称密码算法加密和解密进行的功能正确性检测。

3.8

MAC 检测　MAC test

对密码键盘中 MAC 算法进行的功能正确性检测。

3.9

非对称密码算法功能检测　asymmetric cryptographic algorithm test

对密码键盘中非对称密码算法的加密、解密、签名和验签的功能正确性进行的检测。

3.10

杂凑算法检测　hash algorithm compression test

对密码键盘中杂凑算法的功能正确性进行的检测。

3.11

密钥管理检测　key management test

对密码键盘中密钥分散、密钥素性和密钥协商的功能正确性进行的检测。

3.12

随机数质量检测　random quality test

对密码键盘生成的随机数质量是否合格进行的检测。

3.13

环境失效保护检测　environmental failure protection test

对密码键盘环境失效方面的要求和特性进行的检测。

注：改写 GM/T 0028—2014，定义 3.26。

3.14

密码算法稳定性检测　cryptographic algorithm stability test

对密码键盘中对称密码算法、非对称密码算法和杂凑密码算法的功能稳定性进行的检测。

3.15

蒙特卡洛检测　Monte Carlo test

采用反复随机抽样的原理对密码算法进行反复测试的方法。

3.16

算法性能检测　algorithm performance test

对密码键盘中对称密码算法、非对称密码算法和杂凑算法的性能进行的检测。

3.17

安全功能检测　security function test

用于评判密码键盘在物理安全方面的等级的评判机制。

3.18

密钥安全检测　key security test

对密码键盘在密钥存储、密钥输入与输出和密钥置零方面的安全等级进行评判的检测。

3.19

错误注入　fault induction

通过应用短暂的电压、辐射、激光或时钟偏移技术，导致硬件中的操作行为发生变化的技术。

3.20

运行环境　operational environment

密码键盘安全运行所需要的所有软件、硬件和固件的集合。

注：改写 GM/T 0028—2014，定义 3.60。

3.21

软件/固件安全检测　software/firmware security

对密码键盘的软件/固件的安全等级评判进行的检测。

3.22

安全状态

密码键盘软件/固件、硬件及身份信息方面的安全状况。

3.23

鉴别　authentication

评判密码键盘在身份鉴别方面的安全等级的评判机制。

4　缩略语

下列缩略语适用于本文件。

CBC　Cipher block Chaining 密码分组链接

EFP　Environmental Failure Protection 环境失效保护

EFT　Environmental Failure Testing 环境失效检测

MAC　Message Authentication Code 消息鉴别码

5　密码键盘安全等级

密码键盘的安全等级代表了其所具有的安全能力的高低。

本标准规定了密码键盘的依次递增的 4 个安全等级。其中安全 1 级最低，安全 4 级最高。

安全等级 1～4 级的密码键盘均应通过基本检测项目(6.1～6.8、6.10)，以及安全要求相应项目(6.9)的检测。

6　检测内容及检测方法

6.1　安全管理功能检测

6.1.1　外部认证检测

6.1.1.1　正确情况检测

检测步骤如下：

a)　导入正确的认证密钥到密码键盘；

b)　使用正确的认证密钥进行认证检测，密码键盘返回认证成功的响应；

c)　在认证前执行和密钥相关的操作，密码键盘返回不满足安全状态；

d)　如果以上步骤密码键盘均能正常响应，则正确情况检测通过。

6.1.1.2 异常情况检测

检测步骤如下：

a) 导入正确的认证密钥到密码键盘；

b) 使用错误的认证密钥进行认证检测，密码键盘返回认证失败的响应，并提示剩余认证次数，当剩余认证次数为零时，外部认证被锁定（删除密码键盘中所有密钥后自动解除锁定，或锁定24 h后自动解除锁定）；

c) 如果外部认证锁定，密码键盘进入错误状态，则异常情况检测通过。

如果正确情况检测和异常情况检测通过，则外部认证检测通过。

6.1.2 自检检测

6.1.2.1 上电自检检测

6.1.2.1.1 软件/固件完整性检测

检测内容如下：

a) 如果采用MAC进行软件/固件的完整性测试，则检测步骤如下：

1) 检测人员确认送检单位提交了MAC的计算和验证过程的测试文档；

2) 检测人员确认送检单位提交了软件/固件完整性自检测试的源代码；

3) 通过源代码和文档的审查，检测人员确认源代码实现的软件/固件完整性测试和文档描叙是否一致；

4) 如果一致，则软件/固件完整性测试通过。

b) 如果采用核准的数字签名进行软件/固件的完整性测试，则检测步骤如下：

1) 检测人员应确认送检单位提交了数字签名的计算和验证过程的测试文档；

2) 检测人员应确认送检单位提交了固件完整性自检测试的源代码；

3) 通过源代码和文档的审查，检测人员确认源代码实现的软件/固件完整性测试和文档描叙是否一致；

4) 如果一致，则软件/固件完整性测试通过。

如果密码键盘采用以上两种方法之一测试通过，则软件/固件完整性测试通过。

6.1.2.1.2 随机数自检检测

检测步骤如下：

a) 检测人员确认送检单位提交了随机数自检的自检文档和随机数自检源代码；

b) 通过文档和源代码的审查，检测人员确认源代码实现的随机数自检检测和文档描述是否一致；

c) 如果一致且随机数检测方法为GB/T 32915—2016中规定的方法，则随机数自检检测通过。

6.1.2.1.3 关键功能自检检测

检测步骤如下：

a) 检测人员应确认送检单位提交了所有关键功能描述文档和检测关键功能（包括密码算法引擎和安全状态）的自检测试文档；

b) 检测人员应确认送检单位提交了关键功能自检测试的源代码；

c) 通过文档和源代码的审查，检测人员确认源代码实现的关键功能自检测试和文档描述是否一致；

d) 如果一致，则关键功能自检测试通过。

6.1.2.2 运行前条件自检检测

6.1.2.2.1 对称密码算法自检检测

检测步骤如下：

a) 检测人员确认送检单位提交了对称密码算法(包括对称算法加密和解密)自检的自测试文档及对称密码算法自检测源代码；

b) 通过文档和源代码的审查，检测人员确认源代码实现的对称算法自检测试和文档描述是否一致；

c) 如果一致则对称算法自检测试通过。

6.1.2.2.2 非对称密码算法自检检测(可选)

非对称密码算法自检检测，根据产品对该类算法的支持情况作为可选检测项目。检测步骤如下：

a) 检测人员确认送检单位提交了非对称算法(包括非对称加解密和非对称签名验签)自检的自测试文档及非对称密码算法自检测源代码；

b) 通过文档和源代码的审查，检测人员确认源代码实现的非对称算法自检测试和文档描述是否一致；

c) 如果一致则非对称算法自检测试通过。

6.1.2.2.3 杂凑密码算法自检检测(可选)

杂凑算法自检检测，根据产品对该类算法的支持情况作为可选检测项目。检测步骤如下：

a) 检测人员确认送检单位提交了杂凑算法自检的自测试文档及杂凑算法自检测源代码；

b) 通过文档和源代码的审查，检测人员确认源代码实现的杂凑算法自检测试和文档描述是否一致；

c) 如果一致则杂凑算法自检测试通过。

6.1.3 PIN 数据块检测

6.1.3.1 PIN 数据块填充格式

送检的密码键盘应能支持附录 A 中描述的 PIN 数据块填充格式，如果密码键盘同时还支持其他 PIN 数据块填充格式，送检单位需提供 PIN 数据块填充格式说明文档。

6.1.3.2 正确情况检测

检测步骤如下：

a) 导入预定的 PIN 数据块加密密钥到密码键盘；

b) 从密码键盘输入预定的 PIN 码；

c) 设置预定的主账号；

d) 获取密文的 PIN 数据块，将密码键盘返回的密文 PIN 数据块和预期密文 PIN 数据块比对；

e) 如果比对结果一致，则正确情况检测通过。

6.1.3.3 异常情况检测

检测步骤如下：

a) 从检测平台上导入错误的 PIN 数据块加密密钥到密码键盘；

b) 从密码键盘输入正确的 PIN 码；

c) 在检测平台(能按本标准对密码键盘进行测试的上位机软件)上设定正确的主账号;
d) 从密码键盘获取密文的 PIN 数据块,将密码键盘返回的密文 PIN 数据块和预期密文 PIN 数据块比对;
e) 如果比对结果一致,则异常情况检测不通过;如果比对结果不一致,继续进行以下检测;
f) 从检测平台上导入正确的 PIN 数据块加密密钥到密码键盘;
g) 从密码键盘输入错误的 PIN 码;
h) 重复步骤 c)~d);
i) 如果比对结果一致,则异常情况检测不通过;如果比对结果不一致,继续进行以下检测;
j) 从检测平台上导入正确的 PIN 数据块加密密钥到密码键盘;
k) 从密码键盘输入正确的 PIN 码;
l) 设定错误的主账号;
m) 重复 d)步骤;
n) 如果比对结果不一致,则异常情况检测通过。

如果正确情况测试和异常情况测试通过,则 PIN 数据块测试通过。

6.2 密码算法检测

6.2.1 对称密码算法加密和解密检测

6.2.1.1 加密检测

检测步骤如下:

a) 检测机构提供明文、密钥以及测试参数等测试数据,对密码算法支持的数据长度和工作模式进行检测(填充方式采用后补“0”);
b) 用指定的密钥对测试数据进行加密运算,密码键盘返回运算结果;
c) 将密码键盘返回的运算结果与检测机构的结果进行比对;
d) 如果结果一致,则加密检测通过。

6.2.1.2 解密检测

检测步骤如下:

a) 检测机构提供密文、密钥以及测试参数等测试数据,对密码算法支持的数据长度和工作模式进行检测(填充方式采用后补“0”);
b) 用指定的密钥对测试数据进行解密运算,密码键盘返回运算结果;
c) 将密码键盘返回的运算结果与检测机构的结果进行比对;
d) 如果结果一致,则解密检测通过。如果加密检测和解密检测都通过,则对称密码算法加密和解密检测通过。

6.2.2 MAC 算法检测

6.2.2.1 MAC 计算方法

送检的密码键盘要求至少支持 CBC-MAC 算法,CBC-MAC 计算方法参见附录 B。

如果密码键盘同时还支持其他 MAC 算法,送检单位需提供 MAC 算法具体计算的说明文档。

6.2.2.2 MAC 算法检测

检测步骤如下:

a) 检测机构将测试数据发送给密码键盘；
b) 密码键盘利用检测机构提供的 MAC 参数对接收到的数据进行加密运算；
c) 将密码键盘生成的 MAC 与检测机构的 MAC 进行比对；
d) 如果一致，则 MAC 算法检测通过。

6.2.3 非对称密码算法功能检测（可选）

6.2.3.1 总则

非对称密码算法功能检测，根据产品对该类算法的支持情况来作为可选检测项目。

6.2.3.2 非对称密钥对生成检测

检测步骤如下：
a) 用密码键盘产生 10 组密钥对，然后把 10 组密钥对发送给检测机构；
b) 由检测机构判断 10 组密钥的正确性；
c) 如果密码键盘提供的 10 组密钥对都是正确的，则非对称密钥对生成检测通过。

6.2.3.3 非对称密码算法加密和解密检测

6.2.3.3.1 加密检测

检测步骤如下：
a) 用检测机构提供的公钥对测试明文进行加密运算，密码键盘返回运算结果；
b) 由检测机构判断密码键盘返回的运算结果是否正确；
c) 如果结果正确，则加密检测通过。

6.2.3.3.2 解密检测

检测步骤如下：
a) 用检测机构提供的私钥对加密结果进行解密运算，密码键盘返回运算结果；
b) 由检测机构判断密码键盘返回的结果是否正确；
c) 如果结果正确，则解密检测通过。如果加密检测和解密检测都通过，则非对称密码算法加密和解密检测通过。

6.2.3.4 非对称密码算法签名和验签检测

6.2.3.4.1 签名检测

检测步骤如下：
a) 由检测机构提供测试数据（签名者信息、待签名消息和密钥对）给密码键盘；
b) 密码键盘利用非对称密码算法对测试数据进行签名操作，密码键盘返回运算结果；
c) 检测机构用验签的方法判断已签名的结果是否正确；
d) 如果结果正确，则签名检测通过。

6.2.3.4.2 验签检测

检测内容如下：
a) 正确情况检测，检测步骤如下：
1) 将检测正确的签名结果与测试数据（签名者信息、待签名消息和密钥对）输入密码键盘；

2） 密码键盘用非对称密码算法对接收的数据进行验签；
3） 将验证结果应与预期结果相比对；
4） 如果一致，则正确情况检测通过。

b） 异常情况检测，检测步骤如下：
1） 将检测错误的签名结果与测试数据（签名者信息、待签名消息和密钥对）输入密码键盘；
2） 密码键盘用非对称密码算法对接收的数据进行验签；
3） 如果验证结果返回消息错误，验签失败，则异常情况检测通过。

如果正确情况检测和异常情况检测都通过，则验签检测通过。

6.2.3.5 密钥协商检测

检测步骤如下：

a） 检测平台与密码键盘进行密钥协商，用 GB/T 32918.3—2016 规定的方法；
b） 密码键盘加密一组已知的数据，把得到的密文送给检测平台；
c） 检测平台用秘密密钥解密接收的密文，并把解密出的明文显示出来，检测机构判断解密的明文是否正确；
d） 如果判断明文结果正确，检测通过。

6.2.4 杂凑算法数据压缩检测（可选）

杂凑算法的数据压缩检测，根据产品对该类算法的支持情况作为可选检测项目。检测步骤如下：

a） 检测机构提供测试数据给密码键盘；
b） 密码键盘利用杂凑算法对测试数据进行运算，密码键盘返回运算结果；
c） 将密码键盘返回的结果与检测机构的结果相比对；
d） 如果结果一致，则杂凑算法数据压缩检测通过。

6.3 密钥素性检测（可选）

密钥素性检测是验证非对称密码算法的密码参数是否为素数，当产品中包含对密钥有素性要求的算法时才需进行。

密钥素性检测方法按 ISO/IEC 18032:2005 规定的方法进行。

6.4 随机数质量检测

检测步骤如下：

a） 用密码键盘产生随机数，直至采集够 128 MB；
b） 用 GB/T 32915—2016 规定的方法对随机数进行检测，并判定是否通过检测。

6.5 环境失效保护检测

6.5.1 环境失效保护通用要求

环境失效保护通用要求如下：

a） 对于安全 1 级、安全 2 级的密码键盘，不要求具有环境失效保护（EFP）特性或者经过环境失效检测（EFT）；
b） 安全 3 级的密码键盘应具有 EFP 特性或经过 EFT，安全 4 级的密码键盘应具有 EFP 特性；
c） 如果温度或电压超出密码键盘的正常运行范围，则保护电路应关闭键盘，防止继续运行或立即置零所有敏感信息。

6.5.2 环境失效检测过程

按 GM/T 0028—2014 中 7.7.4.3 进行检测。

6.6 密码算法稳定性检测

6.6.1 对称密码算法稳定性检测

6.6.1.1 已知结果检测

检测步骤如下：

a) 固定密钥和初始向量，检测机构提供指定的 N($N \geq 100$)组明文与密文的测试数据对；
b) 输入测试数据(明文/密文、密钥，以及模式所需的初始向量 IV)；
c) 输出加密结果/解密结果；
d) 将加密结果/解密结果与检测机构的参考数据进行比对；
e) 加密/解密运算循环 N 次，若 N 次加密结果/解密结果都与检测机构提供的参考数据一致，则已知结果检测通过；
f) 然后检测另一长度的密钥或下一个工作模式，重复步骤 a)～e)；
g) 如果所有的密钥长度和模式都检测通过，则已知结果检测通过。

6.6.1.2 多数据块检测

检测步骤如下：

a) 由检测机构提供 N($N \geq 100$)组明文/密文数据块以及某些工作模式所需的初始向量；
b) 输入测试数据(明文/密文、密钥，以及模式所需的初始向量 IV)；
c) 输出加密结果/解密结果；
d) 将加密结果/解密结果与检测机构的参考数据进行比对；
e) 加密/解密运算循环 N 次，若 N 次加密结果/解密结果都与检测机构提供的参考数据一致，则检测通过；
f) 然后检测另一长度的密钥或下一个工作模式，测试步骤循环 a)～e)；
g) 如果所有密钥长度和工作模式的结果都与检测机构的参考数据相同，则多数据块检测通过。

6.6.1.3 蒙特卡洛检测

检测原理参见附录 C，检测步骤如下：

a) 固定密钥和初始向量，由检测机构提供 1 组明文/密文数据块；
b) 输入测试数据(明文/密文、密钥，以及模式所需的初始向量 IV)；
c) 输出加密结果/解密结果；
d) 将每一轮的加密结果/解密结果作为下一轮的明文/密文输入，加密/解密运算循环 N($N \geq 100$)次；
e) 若 N 次运算后的加密结果/解密结果与检测机构提供的参考数据一致，则检测通过；
f) 然后检测另一长度的密钥或下一个工作模式，测试步骤循环 a)～e)，直到所有的密钥长度和模式检测通过；
g) 如果所有密钥长度和工作模式的结果都与检测机构的参考数据相同，则蒙特卡洛检测通过。

6.6.2 非对称密码算法稳定性检测(可选)

6.6.2.1 总则

非对称密码算法稳定性检测，根据送检单位产品对该类算法的支持情况来作为可选检测项目。

6.6.2.2 密钥生成检测

检测步骤如下：

a) 输入检测机构给定的参数；

b) 输出公钥和私钥；

c) 检测平台判断每组密钥对的正确性；

d) 如果完成 N（$N \geq 100$）组运算且结果都正确，则密钥生成检测通过。

6.6.2.3 非对称密码算法公钥加密检测

检测步骤如下：

a) 由检测机构生成 N（$N \geq 100$）组的测试明文；

b) 输入检测机构提供的测试明文，以及公钥；

c) 输出利用公钥加密之后的密文；

d) 检测机构对结果进行反向检测；

e) 如果完成 N 组运算且结果都一致，则非对称密码算法公钥加密检测通过。

6.6.2.4 非对称密码算法私钥解密检测

检测步骤如下：

a) 输入上一节公钥加密产生的 N（$N \geq 100$）组密文，公钥对应的私钥；

b) 输出私钥解密的明文；

c) 将明文与检测机构的参考值进行比对；

d) 如果完成 N 组运算且结果都一致，则非对称密码算法私钥解密检测通过。

6.6.2.5 非对称密码算法签名检测

检测步骤如下：

a) 由检测机构提供 N（$N \geq 100$）组待签名的数据的随机数；

b) 输入待签名数据、签名者信息和密钥对，密码键盘对输入的数据进行签名；

c) 检测机构用验签的方法判断已签名的结果是否正确；

d) 如果完成 N 组运算且结果都正确，则非对称密码算法签名检测通过。

6.6.2.6 非对称密码算法验签检测

6.6.2.6.1 正确情况

检测步骤如下：

a) 由检测机构提供 N（$N \geq 100$）组正确的测试数据（如：正确的签名结果、签名者信息、待签名消息和密钥对）；

b) 输入测试数据，密码键盘对输入的数据进行验签；

c) 如果密码键盘返回 N 组正确的验签结果，则正确情况检测通过。

6.6.2.6.2 异常情况

检测步骤如下：

a) 由检测机构提供 N（$N \geq 100$）组异常的测试数据（如：异常的签名结果、签名者信息、待签名消息和密钥对）；

b) 输入测试数据，密码键盘用输入的数据进行验签；

c) 如果密码键盘返回 N 组错误的验签结果，则异常情况检测通过。

6.6.3 杂凑算法稳定性检测(可选)

杂凑算法稳定性检测，根据送检单位产品对该类算法的支持情况作为可选检测项目。检测步骤如下：

a) 由检测机构提供 N($N \geqslant 100$)组测试数据；

b) 输入测试数据；

c) 输出杂凑值；

d) 将输出的杂凑值与检测机构的数据进行比对；

e) 如果 N 次运算的杂凑值都与检测机构的数据一致，则杂凑算法稳定性检测通过。

6.7 算法性能检测

6.7.1 对称密码算法加密和解密性能检测

检测步骤如下：

a) 由检测机构确定测试数据的字节总数(字节总数≥20 480)和一组对称算法密钥；

b) 将字节总数平均分组(分组长度可以是 64 字节、128 字节或者送检单位建议的长度)，每一组的字节数为 L，总组数为 N；

c) 检测人员操作密码键盘用密钥对分好的每组数据依次进行加密运算，记录运算完成的总时间 T；

d) 用式(1)求出运算速率 S，$S_1 = S$；

$$S = \frac{8LN}{T} \qquad \cdots\cdots(1)$$

式中：

S ——每秒的运算速率，单位为比特每秒(bit/s)；

L ——测试数据的字节数；

N——测试次数；

T ——测试所耗费的总时间，单位为秒(s)。

e) 重复步骤 a)～d)两次，求出 S_2、S_3；

f) 将 S_1、S_2、S_3 求平均值得出 S'；

g) 解密性能检测步骤同步骤 a)～f)，在 c)步骤中进行解密运算；

h) 如果 S'符合《产品规格说明书》中厂商申明的参数，则对称密码算法加密和解密性能检测通过。

6.7.2 MAC 计算性能检测

检测步骤如下：

a) 由检测机构确定测试数据的字节总数(字节总数≥20 480)，一组初始化向量和一组对称算法密钥；

b) 将字节总数平均分组(分组长度可以是 64 字节、128 字节或者送检单位建议的长度)，每一组的字节数为 L，总组数为 N；

c) 检测人员操作密码键盘用密钥对分好的每组数据依次进行 MAC 运算，记录运算完成的总时间 T；

d) 用式(1)求出运算速率 S，$S_1=S$；

e) 重复步骤 a)～d)两次，得出 S_2、S_3；

f) 将 S_1、S_2、S_3 求平均值得出 S'；

g) 如果 S'符合《产品规格说明书》中厂商申明的参数，则对称密码算法 MAC 计算性能检测通过。

6.7.3 非对称密码算法性能检测(可选)

6.7.3.1 总则

非对称密码算法性能检测，根据送检单位产品对该类算法的支持情况来作为可选检测项目。

6.7.3.2 非对称密码算法加密和解密性能检测

检测步骤如下：

a) 由检测机构确定测试数据的字节总数(字节总数≥20 480)和一组非对称算法密钥对；

b) 将字节总数平均分组(分组长度可以是 64 字节、128 字节或者送检单位建议的长度)，每一组的字节数为 L，总组数为 N；

c) 检测人员操作密码键盘用公钥对分好的每组数据依次进行加密运算，记录运算完成的总时间 T；

d) 用式(1)求出运算速率 S_1；

e) 重复步骤 a)～d)两次，得出 S_2、S_3；

f) 将 S_1、S_2、S_3 求平均值得出 S'，将 S'与《产品规格说明书》中厂商申明的参数进行比对；

g) 如果 S'符合厂商申明，则非对称密码算法加密性能检测通过；

h) 解密算法性能检测重复步骤 a)～b)；

i) 检测人员操作密码键盘用私钥对分好的每组数据依次进行解密运算，记录运算完成的总时间 T；

j) 用式(1)求出运算速率 S_1；

k) 重复步骤 d)～f)；

l) 将 S_4、S_5、S_6 求平均值得出 S''，将 S''与《产品规格说明书》中厂商申明的参数进行比对；

m) 如果 S'' 符合《产品规格说明书》中厂商申明的参数，则非对称密码算法解密性能检测通过。

6.7.3.3 非对称密码算法签名和验签性能检测

检测步骤如下：

a) 由检测机构提供一组测试数据，如算法密钥对、签名者 ID、N 组($N\geq 1\ 000$)待签名数据；

b) 密码键盘用提供的数据进行 N 次签名，记录完成总时间为 T；

c) 用 N/T 得出每秒签名次数 n_1；

d) 重复步骤 a)～c)两次，得出 n_2、n_3；

e) 将 n_1、n_2、n_3 求平均值得出 n'，将 n'与《产品规格说明书》中厂商申明的参数进行比对；

f) 如果 n'与厂商申明的参数相符合，则非对称密码算法签名性能检测通过；

g) 验签性能检测重复步骤 a)～b)；

h) 用 N/T 得出每秒验签次数 n_4；

i) 重复步骤 g)～h)两次，得出 n_5、n_6；

j) 将 n_4、n_5、n_6 求平均值得出 n''，将 n''与《产品规格说明书》中厂商申明的参数进行比对；

k) 如果 n''符合《产品规格说明书》中厂商申明的参数，则非对称密码算法验签性能检测通过。

6.7.3.4 非对称密钥生成性能检测

检测步骤如下：

a) 密码键盘产生 N($N \geqslant 1\ 000$)组密钥对，检测机构记录完成总时间 T；

b) 用 N/T 得出每秒密钥对生成次数 n_1；

c) 重复步骤 a)～b)两次，得出 n_2、n_3；

d) 将 n_1、n_2、n_3 求平均值得出 n'，将 n' 与《产品规格说明书》中厂商申明的参数进行比对；

e) 如果 n' 符合《产品规格说明书》中厂商申明的参数，则非对称密钥生成性能检测通过。

6.7.3.5 非对称密码算法密钥协商性能检测

检测步骤如下：

a) 密码键盘和检测平台进行 N($N \geqslant 1\ 000$)次密钥协商，检测机构记录完成总时间 T；

b) 用 N/T 得出每秒密钥协商次数 n_1；

c) 重复步骤 a)～b)两次，得出 n_2、n_3；

d) 将 n_1、n_2、n_3 求平均值得出 n'，将 n' 与《产品规格说明书》中厂商申明的参数进行比对；

e) 如果 n' 符合《产品规格说明书》中厂商申明的参数，则非对称密钥的协商性能检测通过。

6.7.4 杂凑算法性能检测(可选)

杂凑算法性能检测，根据送检单位产品对该类算法的支持情况作为可选检测项目。检测步骤如下：

a) 由检测机构确定测试数据的字节总数，字节总数≥20 480；

b) 将字节总数平均分组(分组长度可以是 64 字节、128 字节或者送检单位建议的长度)，每一组的字节数为 L，总组数为 N；

c) 密码键盘完成 N 次杂凑运算，检测机构记录运算完成总时间 T；

d) 用式(1)求出每个数据长度的速率 S_1；

e) 重复步骤 a)～d)两次，得出 S_2、S_3；

f) 将 S_1、S_2、S_3 求平均值得出 S'，将 S' 与《产品规格说明书》中厂商申明的参数进行比对；

g) 如果 S' 符合《产品规格说明书》中厂商申明的参数，则杂凑算法性能检测通过。

6.8 设备安全性检测

密码键盘安全性测试遵照 GM/T 0039 的要求进行。

6.9 安全要求检测

6.9.1 安全功能检测

6.9.1.1 安全 1 级

检测步骤如下：

a) 检测密码键盘部件是否由产品级部件组成以及部件是否采用了标准钝化技术。如果是则继续以下检测，否则检测不通过。

b) 检测密码键盘在运行维护功能运行时密码键盘是否能被操作员按规定程序置零，或由密码键盘自动置零。如果是则继续以下检测，否则检测不通过。

c) 检测密码键盘的外壳是否为金属或硬质塑料的产品级外壳。如果是则检测通过。

6.9.1.2 安全 2 级

除了通过安全 1 级的检测，安全 2 级的密码键盘还需通过以下检测：

a) 检测密码键盘在封盖、外壳或封条上是否提供了显式的拆卸证据。如果是则继续以下检测，否则检测不通过。
b) 检测密码键盘的外壳是否在可见光谱内无法对密码键盘关键区域的内部操作进行信息收集。如果是则继续以下检测，否则检测不通过。
c) 检测密码键盘是否存在通风孔或缝，若不存在则继续以下检测。若存在通风孔或缝则检测该孔或缝是否具有特殊构造，保证无法直接观察密码键盘内部的构造或从部件进行信息收集。如果是则继续以下检测，否则检测不通过。
d) 检测密码键盘在受到移除外壳的行为后，是否变成不可工作。如果是则继续以下检测，否则检测不通过。
e) 检测密码键盘是否包含拆卸响应和置零电路，且一旦检测到拆卸行为则置零所有敏感信息。如果是则检测通过。

6.9.1.3 安全3级

除了通过安全2级的检测，安全3级的密码键盘还需通过以下检测：
a) 检测密码键盘是否具有EFP特性或经过EFT。如果是则继续以下检测，否则检测不通过。
b) 检测密码键盘在温度超出运行，存放和分发的预期温度范围时，外壳是否维持强度或硬度特征。如果是则继续以下检测，否则检测不通过。
c) 检测密码键盘是否存在封盖或者访问接口，若不存在则继续以下检测。若存在则检测密码键盘在拆卸外壳或维护访问接口时，是否立即置零敏感信息。如果是则继续以下检测，否则检测不通过。
d) 检测密码键盘是否存在通风孔或缝，若不存在则继续以下检测。若存在则检测通风孔或缝是否具有特殊的构造，保证键盘内部不被物理探测。如果是则继续以下检测，否则检测不通过。
e) 检测密码键盘是否存在封条，若不存在则检测完成。若存在则检测密码键盘的封条是否具有唯一性和可识别性。如果是则检测通过。

6.9.1.4 安全4级

除了通过安全3级的检测，安全4级的密码键盘还需通过以下检测：
a) 检测密码键盘是否具有抗移除的硬质不透明涂层或拆卸立即置零的能力。如果是则继续以下检测，否则检测不通过。
b) 检测密码键盘是否具有EFP特性。如果是则继续以下检测，否则检测不通过。
c) 检测密码键盘是否能防止错误注入攻击。如果是则继续以下检测，否则检测不通过。
d) 检测密码键盘是否封装在一种或多种拆卸检测机制的封套内且能对访问敏感信息做出响应。如果是则检测通过。

6.9.2 密钥安全检测

6.9.2.1 密钥存储

6.9.2.1.1 安全1级

无要求，无需检测，密码键盘默认达到安全1级。

6.9.2.1.2 安全2级

安全2级的密码键盘需通过以下检测：
a) 检测存储的密钥是否带有校验。如果是则继续以下检测，否则检测不通过。

b) 检测密钥是否存放在可控且专用的区域，是否不能进行非法访问。如果是则检测通过。

6.9.2.1.3 安全3级

除了通过安全2级的检测，安全3级的密码键盘还需进行以下检测：工作密钥是否以对称密码算法加密的形式存储。如果是则检测通过。

6.9.2.1.4 安全4级

同安全3级。

6.9.2.2 密钥输入与输出

6.9.2.2.1 安全1级

检测步骤如下：

a) 检测密码键盘的密钥是否可手动输入或以其他方式导入。如果是则继续以下检测，否则检测不通过。

b) 检测密码键盘的密钥是否可导出。如果是则检测不通过，否则检测通过。

6.9.2.2.2 安全2级

检测步骤如下：

a) 检测密码键盘的密钥是否支持密钥分量或密文的形式导入，且通过可信信道传输。若是则检测通过，否则检测不通过。

b) 检测密码键盘的密钥是否可导出。如果是则检测不通过，否则检测通过。

6.9.2.2.3 安全3级

检测步骤如下：

a) 密码键盘如果支持手工输入，检测手工输入的密钥是否采用知识拆分过程来产生，若是则进行步骤b)的检测，否则检测不通过；如果密码键盘支持远程更新，检测密钥是否以数字签名远程加载的方式进行导入，若是则进行步骤b)的检测，否则检测不通过；密码键盘如果支持密文导入，检测加密的密钥是否采用以上两种方式之一事先存放于密码键盘中，若是则进行步骤b)的检测，否则检测不通过。

b) 检测密码键盘除公钥外的其他所有密钥是否可导出，如果是则检测不通过，否则检通过。

6.9.2.2.4 安全4级

检测步骤如下：

a) 密码键盘如果支持手工输入，检测手工输入的密钥是否采用知识拆分过程来产生，且每个分量的输入必须通过身份认证后方可进行；若是则进行步骤b)的检测，否则检测不通过；密码键盘如果支持远程更新，检测密钥是否以安全证书远程加载的方式进行导入，若是则进行步骤b)的检测，否则检测不通过；密码键盘如果支持密文导入，加密的密钥必须采用以上两种方式之一事先存放于密码键盘中，若是则进行步骤b)的检测，否则检测不通过。

b) 检测密码键盘除公钥外的其他所有密钥是否可导出，如果是则检测不通过，否则检通过。

6.9.2.3 密钥置零

6.9.2.3.1 安全1级

无要求，无需检测，密码键盘默认达到安全1级。

6.9.2.3.2 安全2级

安全2级的密码键盘需通过以下检测：

a) 检测密码键盘未受保护的密钥和使用完毕的临时密钥是否置零，且输出完成状态指示。如果是则继续以下检测，否则检测不通过。

b) 对密码键盘进行非法操作，检测密钥是否置零。如果是则检测通过。

6.9.2.3.3 安全3级

除了通过安全2级的检测，安全3级的密码键盘还需通过以下检测：

a) 检测密码键盘的置零操作是否可中断。如果是则检测不通过，否则继续以下检测。

b) 检测密码键盘在置零操作过程中，是否可恢复已被置零数据。如果是则检测不通过，否则检测通过。

6.9.2.3.4 安全4级

同安全3级。

6.9.3 安全状态检测

6.9.3.1 软件/固件安全

6.9.3.1.1 安全1级

无要求，无需检测，密码键盘默认达到安全1级。

6.9.3.1.2 安全2级

安全2级的密码键盘需通过以下检测：

a) 通过检查键盘的《产品规格说明书》，确认检测密码键盘的固件是否能够导出。如果不能导出则继续以下检测，否则检测不通过。

b) 检测密码键盘的软件/固件是否只包含可运行的形式代码。如果是则继续以下检测，否则检测不通过。

c) 检测密码键盘的操作员是否能通过接口启动或执行调试技术。如果不能则检测通过，否则检测不通过。

6.9.3.1.3 安全3级

除了通过安全2级的检测，安全3级的密码键盘还需通过以下检测：

a) 检查生产厂家提供的《产品规格说明书》，确认固件是否以加密形式存储。如果是则继续以下检测，否则检测不通过。

b) 检测密码键盘在软件/固件更新时是否使用MAC校验或验签。如果是则检测通过。

6.9.3.1.4 安全4级

除了通过安全3级的检测，安全4级的密码键盘还需检测密码键盘在软件/固件更新时是否使用了验签。如果是则检测通过。

6.9.3.2 鉴别(可选)

6.9.3.2.1 总则

密码键盘可能需要鉴别机制以鉴别访问密码键盘的操作员，根据送检单位产品对该类功能的支持

情况来作为可选检测项目。

6.9.3.2.2 安全 1 级

无要求，无需检测，密码键盘默认达到安全 1 级。

6.9.3.2.3 安全 2 级

安全 2 级的密码键盘需检测密码键盘是否采用基于角色的鉴别以控制对密码键盘的访问。如果是则检测通过。

6.9.3.2.4 安全 3 级

除了通过安全 2 级的检测，安全 3 级的密码键盘还需检测密码键盘是否采用基于身份的鉴别以控制对密码键盘的访问。如果是则检测过。

6.9.3.2.5 安全 4 级

除了通过安全 3 级的检测，安全 4 级的密码键盘还需检测密码键盘是否采用基于身份的多因素鉴别以控制对密码键盘的访问。如果是则检测通过。

6.9.4 密码算法检测

6.9.4.1 随机数生成

6.9.4.1.1 安全 1 级

按 GM/T 0008—2012 中 5.1.1 的规定进行检测。如果符合该要求，则检测通过。

6.9.4.1.2 安全 2 级

同安全 1 级。

6.9.4.1.3 安全 3 级

按 GM/T 0008—2012 中 5.1.2 的规定进行检测。如果符合该要求，则检测通过。

6.9.4.1.4 安全 4 级

按 GM/T 0008—2012 中 5.1.3 的规定进行检测。如果符合该要求，则检测通过。

6.9.4.2 对称密码算法

6.9.4.2.1 安全 1 级

按 GM/T 0008—2012 中 5.2.1 的规定进行检测。如果符合该要求，则检测通过。

6.9.4.2.2 安全 2 级

同安全 1 级。

6.9.4.2.3 安全 3 级

按 GM/T 0008—2012 中 5.2.2 的规定进行检测。如果符合该要求，则检测通过。

6.9.4.2.4 安全4级

按GM/T 0008—2012中5.2.3的规定进行检测。如果符合该要求，则检测通过。

6.9.4.3 非对称密码算法(可选)

6.9.4.3.1 总则

非对称密码算法的安全要求，根据送检单位产品对该类算法的支持情况来作为可选检测项目。

6.9.4.3.2 安全1级

按GM/T 0008—2012中5.3.1的规定进行检测。如果符合该要求，则检测通过。

6.9.4.3.3 安全2级

同安全1级。

6.9.4.3.4 安全3级

按GM/T 0008—2012中5.3.2的规定进行检测。如果符合该要求，则检测通过。

6.9.4.3.5 安全4级

按GM/T 0008—2012中5.3.3的规定进行检测。如果符合该要求，则检测通过。

6.9.4.4 杂凑密码算法(可选)

6.9.4.4.1 总则

杂凑密码算法的安全要求，根据送检单位产品对该类算法的支持情况来作为可选检测项目。

6.9.4.4.2 安全1级

按GM/T 0008—2012中5.4.1的规定进行检测。如果符合该要求，则检测通过。

6.9.4.4.3 安全2级

同安全1级。

6.9.4.4.4 安全3级

按GM/T 0008—2012中5.4.2的规定进行检测。如果符合该要求，则检测通过。

6.9.4.4.5 安全4级

按GM/T 0008—2012中5.4.3的规定进行检测。如果符合该要求，则检测通过。

6.10 送检技术文档要求

按照检测要求提交相关文档资料，作为检测依据。文档资料应包含但不限于以下内容：

a) 密码键盘产品规格说明书；
b) 密码键盘接口说明；
c) 产品函数接口与接口示例代码(若送检单位不提供“产品函数接口与接口示例代码”，则必须提供产品通讯协议、测试工具及测试方法)；

d) 系统框架结构说明；
e) 密码子系统框架结构及功能流程说明；
f) 与密码实现和使用相关的硬件说明；
g) 送检产品所采用的密码算法清单；
h) 密码自检测或自评估报告；
i) 产品技术手册及使用说明书；
j) 生命周期保障说明；
k) 产品总体设计说明；
l) 产品安全性设计报告；
m) 对其他攻击的缓解说明；
n) 源代码及说明；
o) 产品的清晰彩照(整体照片及前后面板照，照片上要清晰显示出生产厂商的标牌、设备型号及序列号)、与密码实现和使用相关的硬件部分彩色照片(能清晰识别芯片或部件的名称、型号等标注)。

7 合格判定条件

在产品进行完所有的检测项目后，进行合格判定。只有基本检测项目(基本检测项目见表1)全部通过，才会进入安全等级判定检测。

产品通过相应安全等级要求的全部项目(见表2)的检测，判定为该产品达到相应的安全等级。

表1 基本检测项目

序号	类别	检测项目	本标准章节	单项要求	总结论
1	基本检测项目	安全管理功能检测	6.1	通过	—
2		密码算法检测	6.2		—
3		密钥素性检测	6.3		—
4		随机数质量检测	6.4		—
5		环境失效保护检测	6.5		—
6		密码算法稳定性检测	6.6		—
7		算法性能检测	6.7		—
8		设备安全性检测	6.8		—
9		送检技术文档审查	6.10		—

表2 安全等级要求检测结果及安全等级判定

序号	类别	检测项目	本标准章节	单项判定结果	总结论
1	安全要求检测项目	安全功能检测	6.9.1	通过 N 级	单项判定最低级为产品最终安全等级(如果在本标准6.1～6.9的基本测试中有某些可选项目未测，那么即使该产品的安全要求检测单项判定高于2级，该产品最终的安全等级也判定为安全2级)
		密钥安全检测	6.9.2	通过 N 级	
		安全状态检测	6.9.3	通过 N 级	
		密码算法检测	6.9.4	通过 N 级	

附 录 A
（资料性附录）
PIN 数据块填充格式

A.1 PIN 数据块填充格式

PIN 数据块填充参考 ISO 9564 格式 0，PIN 数据块格式由明文 PIN 字段和主账号字段异或组成，并由原 64 位长度扩展为 128 位，加密算法改为国家密码管理主管部门认可的对称算法。其格式如下所示。

A.2 明文 PIN 字段

前 8 字节（第 1 位到第 64 位）：

C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

后 8 字节（第 65 位到第 128 位）：

F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

注 1：C——4-bit 控制码，%B0000。

注 2：N——PIN 的长度（4-bit）。

注 3：P——4-bit 二进制 PIN 码。

注 4：P/F——4-bit 二进制 PIN 码/填充码。

注 5：F——4-bit %B1111（填充码）。

A.3 主账号字段

前 8 字节（第 1 位到第 64 位）：

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

后 8 字节（第 65 位到第 128 位）：

0	0	0	0	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12

注 1：0——4-bit 填充码，%B0000。

注 2：A1～A12——主账号的右 12 位（不包括最右边的校验位），主账号不足 12 位左补 0（主账号默认全为 0）。

附 录 B
（资料性附录）
CBC-MAC 计算方法

将待计算的数据按照 128 位一组进行分块，并在数据的最后一块添加最少的 0，使其长度等于 128 位。将数据按照 CBC 模式进行加密运算（加密算法为国家密码管理主管部门认可的对称算法），取最后一块的前 4 字节或前 8 字节作为 MAC 结果。

附 录 C
（资料性附录）
蒙特卡洛检测方法

蒙特卡洛(Monte Carlo)测试的原理是对 N($N \geqslant 100$)组伪随机数进行加密/解密运算，输入的测试数据，密钥以及模式所需的向量 IV 在每次运算时都是一个伪随机数。

在不需要向量 IV 的工作模式下，每一次运算的明文/密文输入是上一次加密/解密的结果，而每一次密钥的输入则是上一次密钥与加密/解密结果的异或值。

当密钥为 128 位时 key[i+1]=key[i] xor result[i]。

当密钥为 192 位时 key[i+1]=key[i] xor {result[i-1][63：0],result[i]}。

当密钥为 256 位时 key[i+1]=key[i] xor {result[i-1],result[i]}。