



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

cryptographystestspecificationfor_{EPP}

2016-12-23 发布

2016-12-23 实施

国家密码管理局 发 布

目 次

前言	I
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	3
5 密码键盘安全等级	3
6 检测内容及检测方法	3
6.1 安全管理功能检测	3
6.2 密码算法检测	6
6.3 密钥素性检测（可选）	8
6.4 随机数质量检测	8
6.5 环境失效保护检测	8
6.6 密码算法稳定性检测	9
6.7 算法性能检测	11
6.8 设备安全性检测	13
6.9 安全要求检测	13
6.10 送检技术文档要求	18
7 合格判定条件	19
附录 A（资料性附录） PIN 数据块填充格式	20
附录 B（资料性附录） CBC-MAC计算方法	21
附录 C（资料性附录） 蒙特卡洛检测方法	22

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 conditionalself-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 blocktest

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 symmetriccryptographicalgorithm encryptionanddecryptiontest

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 MACtest

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 asymmetriccryptographicalgorithm 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 hashalgorithm compressiontest

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 keymanagementtest

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 qualitytest

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 failureprotectiontest

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 cryptographicalgorithm stabilitytest

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 carlotest

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 performancetest

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 securityfunctiontest

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 keysecuritytest

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 faultinduction

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 operationalenvironment

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 / firmwaresecurity

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述是否一致；
 - 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述是否一致；
 - 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测试和文档描述是否一致；
- c) 如果一致则对称算法自检测测试通过。

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（包括非对称加密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测试和文档描述是否一致；
- c) 如果一致则杂凑算法自检测测试通过。

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 $MAC_{\text{密码}}$ 与检测机构的 $MAC_{\text{检测}}$ 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。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：

<https://d.book118.com/505334113114011301>