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 …… 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。