ICS 35.040
L 80
备案号：58551—2017

GM

中华人民共和国密码行业标准

GM/T 0046—2016

金融数据密码机检测规范

Test specification for financial cryptographic server

2016-12-23 发布　　2016-12-23 实施

国家密码管理局　　发布

中华人民共和国密码
行业标准
金融数据密码机检测规范
GM/T 0046—2016
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2017年5月第一版
*
书号:155066·2-31452

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：无锡江南信息安全工程技术中心、国家密码管理局商用密码检测中心、卫士通信息产业股份有限公司、兴唐通信科技股份有限公司、山东得安信息技术有限公司。

本标准主要起草人：张所成、齐传兵、李大为、邓开勇、罗鹏、李国友、刘常、肖秋林、丁余泉、刘先祥、李元正、王妮娜、孔凡玉。

金融数据密码机检测规范

1 范围

本标准规定了金融数据密码机的检测要求和检测方法。

本标准适用于金融数据密码机的检测，以及该类密码设备的研制。

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 0028 密码模块安全要求

GM/T 0039 密码模块安全检测要求

GM/T 0045—2016 金融数据密码机技术规范

GM/T 0050 密码设备管理 设备管理技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

金融数据密码机 financial cryptographic server

用于金融领域，保护金融数据安全，主要实现 PIN 加密、PIN 转加密、MAC 产生和校验、数据加解密、签名验证以及密钥管理等密码服务功能的密码设备。

3.2

对称密码算法 symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

3.3

非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm

加密和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

密码杂凑算法 HASH algorithm

又称杂凑算法、密码散列算法或哈希算法。该算法将一个任意长的比特串映射到一个固定长的比特串，且满足下列三个特性：

a) 为一个给定的输出找出能映射到该输出的一个输入是计算上困难的；

b) 为一个给定的输入找出能映射到同一个输出的另一个输入是计算上困难的；

c) 要发现不同的输入映射到同一输出是计算上困难的。