ICS 35.040
L 80
备案号:55613—2016

GM

中华人民共和国密码行业标准

GM/T 0045—2016

金融数据密码机技术规范

Specifications of financial cryptographic server

2016-03-28 发布　　2016-03-28 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。

本标准主要起草单位：成都卫士通信息产业股份公司、无锡江南计算机技术研究所、兴唐通信科技股份有限公司、山东得安信息技术有限公司、北京三未信安科技发展有限公司、北京江南天安科技有限公司。

本标准主要起草人：李元正、张世雄、黄锦、张所成、徐明翼、王妮娜、郑海森、高志权、李国、马晓艳。

金融数据密码机技术规范

1 范围

本标准定义了金融数据密码机的相关术语，规定了金融数据密码机功能要求、接口要求、硬件要求、业务要求、安全性要求和检测要求等内容。

本标准适用于金融数据密码机的研制、使用，也适用于指导金融数据密码机的检测。

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 4943 信息技术 设备(包括电气事务设备)的安全

GB/T 9813—2000 微型计算机通用规范

GB/T 17964 信息技术 安全技术 分组密码算法的工作模式

GM/T 0002 SM4 分组密码算法

GM/T 0003 SM2 椭圆曲线公钥密码算法

GM/T 0004 SM3 密码杂凑算法

GM/T 0005 随机性检测规范

GM/T 0006 密码应用标识规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0028 密码模块安全技术要求

JR/T 0025 中国金融集成电路(IC)卡规范

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

在金融领域内，用于确保金融数据安全，并符合金融磁条卡、IC 卡业务特点的，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，也称为主机加密机(HSM)。

3.2

对称密码算法 symmetric cryptographic algorithm

加密和解密在算法和密钥上相同或可相互推导的密码算法。

3.3

非对称密码算法 asymmetric cryptographic algorithm

使用两种相关变换和非对称密钥对的密码算法，一种是由公开密钥定义的公开变换，另一种是由私有密钥定义的私有变换。两种变换具有以下特性：给定公开密钥，得出私有密钥在计算上是不可行的。