ICS 35.040
L 80
备案号：58552—2017

GM

中华人民共和国密码行业标准

GM/T 0047—2016

安全电子签章密码检测规范

Cryptography test specification for secure electronic seal

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 …… 2
5　检测内容 …… 2
5.1　检测对象 …… 2
5.2　数字签名算法检测 …… 2
5.3　电子印章数据检测 …… 2
5.4　电子印章验证检测 …… 2
5.5　电子签章数据检测 …… 3
5.6　电子签章验证检测 …… 3
6　检测方法 …… 4
6.1　数字签名算法检测 …… 4
6.2　电子印章数据检测 …… 4
6.3　电子印章验证检测 …… 4
6.4　电子签章数据检测 …… 5
6.5　电子签章验证检测 …… 5
7　送检技术文档要求 …… 7
8　合格判定条件 …… 7

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：北京数字认证股份有限公司、国家密码管理局商用密码检测中心、兴唐通信科技有限公司、上海市数字证书认证中心有限公司、上海格尔软件股份有限公司、卫士通信息产业股份有限公司。

本标准主要起草人：刘伟、李大为、邓开勇、罗鹏、肖秋林、马爱良、李冬、朱亚飞、陈曦、韩琳、阎夏强、张周群、傅大鹏等。

安全电子签章密码检测规范

1 范围

本标准规范了安全电子签章的密码检测内容、检测要求、检测方法以及合格判定准则。

本标准适用于按照 GM/T 0031—2014 研制的安全电子签章系统密码技术的检测。

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 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法

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 0031—2014 安全电子签章密码应用技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子文件 electronic document

在数字设备及环境中形成，以数码形式存储于磁带、磁盘、光盘等载体，依赖计算机等数字设备阅读、处理，并可在通信网络上传送的文件。本文中签章原文指电子文件。

3.2

电子印章 electronic stamp

一种由制作者签名的包括持有者信息和图形化内容的数据，可用于签署电子文件。

3.3

电子签章 electronic seal

使用电子印章签署电子文件的过程。

3.4

电子签章数据 electronic seal data

电子签章过程产生的包含电子印章信息和签名信息的数据。

3.5

电子印章系统 electronic seal system

包含电子印章管理系统和电子签章软件，其中电子印章管理系统包括印章管理员管理、电子印章制作与管理、电子印章验证服务以及安全审计等功能。电子签章软件是使用电子印章对各类电子文件进行电子签章的软件。

3.6

制章人 electronic stamp maker

电子印章系统中具有签署和管理电子印章信息权限的管理员。管理员的数字证书可以是单位证书