ICS 35.040
L 80
备案号:44632—2014

GM

中华人民共和国密码行业标准

GM/T 0031—2014

安全电子签章密码技术规范

Secure electronic seal cryptography technical specification

2014-02-13 发布　　2014-02-13 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　电子签章的密码应用安全机制 …… 2
6　电子签章密码应用协议 …… 2
6.1　电子印章 …… 2
6.1.1　数据格式 …… 2
6.1.2　电子印章验证流程 …… 5
6.2　电子签章 …… 5
6.2.1　数据格式 …… 5
6.2.2　电子签章生成流程 …… 6
6.2.3　电子签章验证流程 …… 6

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、上海市数字证书认证中心有限公司、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、北京海泰方圆科技有限公司、上海格尔软件股份有限公司、吉大正元信息技术股份有限公司、上海颐东网络信息有限公司。

本标准主要起草人：刘平、马臣云、冯承勇、李述胜、程小茁、刘伟、傅大鹏、刘承、李元正、李玉峰、柳增寿、谭武征、李伟平、蒋健等。

安全电子签章密码技术规范

1 范围

本标准规定了电子印章和电子签章的数据结构、密码处理流程。

本标准适用于电子印章系统的开发和使用。

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。

GM/T 0003 SM3 密码杂凑算法

GM/T 0006 密码应用标识规范

GM/T 0009 SM2 密码算法使用规范

PKCS#1：RSA Cryptography Standard

3 术语和定义

下列术语和定义适用于本文件。

3.1

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。

3.2

电子签章 electronic seal

使用电子印章签署电子文件的过程。

3.3

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。

3.4

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档进行电子签章的软件。

3.5

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。管理员可以是单位证书或个人证书，电子印章中的图片和信息必须经制章人的数字证书进行数字签名。

3.6

签章人 electronic seal signer

电子印章系统中对文档进行签章操作的最终用户。