ICS 35.040
L 80

中华人民共和国国家标准

GB/T 35291—2017

信息安全技术
智能密码钥匙应用接口规范

Information security technology—
Cryptography token application interface specification

2017-12-29 发布　　2018-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准依据 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。

本标准由全国信息安全标准化委员会(SAC/TC 260)提出并归口。

本标准起草单位:北京海泰方圆科技股份有限公司、北京握奇智能科技有限公司、北京大明五洲科技有限公司、恒宝股份有限公司、深圳市明华澳汉科技股份有限公司、武汉天喻信息产业股份有限公司、北京飞天诚信科技股份有限公司、华翔腾数码科技有限公司。

本标准起草人:刘平、郭宝安、石玉平、柳增寿、胡俊义、管延军、赵再兴、刘伟丰、何永福、李高锋、汪雪林、赵李明、蒋红宇、王烨。

引　言

本标准的目标是为公钥密码基础设施应用体系框架下的智能密码钥匙设备制定统一的应用接口标准，通过该接口调用智能密码钥匙，向上层提供基础密码服务。为该类密码设备的开发、使用及检测提供标准依据和指导，有利于提高该类密码设备的产品化、标准化和系列化水平。

本标准未包含标识算法 SM9 相关的应用接口。

信息安全技术
智能密码钥匙应用接口规范

1 范围

本标准规定了基于PKI密码体制的智能密码钥匙应用接口，描述了密码相关应用接口的函数、数据类型、参数的定义和设备的安全要求。

本标准适用于智能密码钥匙产品的研制、使用和检测。

2 规范性引用文件

下列文件对于本标准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 33560 信息安全技术 密码应用标识规范

GM/T 0022 IPSec VPN技术规范

GM/T 0024 SSL VPN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

容器 container

密码设备中用于保存密钥所划分的唯一性存储空间。

3.2

设备认证 device authentication

智能密码钥匙对应用程序的认证。

3.3

设备认证密钥 device authentication key

用于设备认证的密钥。

3.4

设备标签 label

由用户设定并存储于设备内部的用于对设备进行标识的字符串。

4 缩略语

下列缩略语适用于本文件。

API 应用编程接口(Application Programming Interface)

MAC 消息鉴别码(Message Authentication Code)

PIN 个人身份识别码(Personal Identification Number)