ICS 35.040
L 80
备案号:38314—2013

GM

中华人民共和国密码行业标准

GM/T 0016—2012

智能密码钥匙密码应用接口规范

Smart token cryptography application interface specification

2012-11-22 发布　　2012-11-22 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 给出的规则进行编写。

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。

本标准由国家密码管理局提出并归口。

本标准的附录 A 为规范性附录。

本标准起草单位：北京海泰方圆科技有限公司、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、项莉、雷继业、胡鹏、赵再兴、段晓毅、刘玉峰、刘伟丰、陈吉、何永福、李高锋、黄东杰、王建承、汪雪林、赵李明。

本标准凡涉及密码算法相关内容，按照国家有关法规实施。

智能密码钥匙密码应用接口规范

1 范围

本标准规定了基于PKI密码体制的智能密码钥匙密码应用接口，描述了密码应用接口的函数、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 0006 密码应用标识规范

GM/T 0009 SM2密码算法使用规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

应用 application

包括容器、设备认证密钥和文件的一种结构，具备独立的权限管理。

3.2

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。

3.3

设备 device

本标准中将智能密码钥匙统称为设备。

3.4

设备认证 device authentication

智能密码钥匙对应用程序的认证。

3.5

设备认证密钥 device authentication key

用于设备认证的密钥。

3.6

设备标签 label

设备的别名，可以由用户进行设定并存储于设备内部。

3.7

消息鉴别码 message authentication code；MAC

消息鉴别算法的输出。