ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1545—2019

信息安全技术
智能密码钥匙安全技术要求

Information security technology—
Security technical requirements for smart tokens

2019-03-04 发布　　2019-03-04 实施

中华人民共和国公安部　　发 布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、公安部第三研究所。

本标准主要起草人：付文彬、杨元原、周嵩岑、顾玮、顾健、陆臻。

信息安全技术
智能密码钥匙安全技术要求

1 范围

本标准规定了智能密码钥匙的安全功能要求、安全保障要求及等级划分要求。

本标准适用于智能密码钥匙的设计、开发及测试。

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 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB/T 18336.3—2015 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

普通用户 user

使用智能密码钥匙的最终用户。

3.2

管理员 administrator

对智能密码钥匙实施个人化、初始化、解锁等管理操作的人员。

3.3

中间件 middle ware

向其他应用程序提供软件接口，根据应用程序调用接口及传入的参数，向智能密码钥匙下发指令或指令序列，接收智能密码钥匙回送的数据，并根据回送数据向应用程序报告接口执行结果的软件。

4 缩略语

下列缩略语适用于本文件。

PIN：个人识别码(Personal Identification Number)

5 智能密码钥匙描述

智能密码钥匙是一种硬件设备，它内置安全芯片，有一定的存储空间，可以存储数字证书等用户数据，有用户的身份鉴别机制(身份鉴别信息通常是PIN，也可为指纹等)，具备密码运算功能。

本安全技术要求针对智能密码钥匙自身的软件和硬件，还包括与系统应用交互的中间件。智能密