ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25057—2010

信息安全技术　公钥基础设施 电子签名卡应用接口基本要求

Information security techniques—Public key infrastructure—Specification of application interface of electronic signature card

2010-09-02 发布　　2011-02-01 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

本标准是为了配合《中华人民共和国电子签名法》的实施，在广泛征求意见的基础上，对GB/T 16649系列标准进行部分引用和扩展。

本标准的附录A为规范性附录，附录B、附录C、附录D为资料性附录。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：北京飞天诚信科技有限公司，中国电子技术标准化研究所，国家信息安全工程技术研究中心。

本标准主要起草人：于华章，周葵亮，朱鹏飞。

引　言

《中华人民共和国电子签名法》规定，电子签名是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。具有生成电子签名功能的安全客户端载体，简称电子签名卡。

数字签名是目前主要的电子签名形式之一。相应地，具有数字签名功能的集成电路卡是目前主要的电子签名卡类型之一。GB/T 16649 系列标准对集成电路卡进行了规定。然而，数字签名与电子签名的范畴并不相同，而电子签名卡也不仅限于集成电路卡。

为了避免技术细节对《中华人民共和国电子签名法》的实施造成干扰，规范电子签名卡的应用接口，制定本标准。旨在定义和规范一个能够完成电子签名应用的最小指令集合。

本标准在 GB/T 16649 系列标准的基础上进行部分引用和扩展。

本标准中给出的 SHA-1、RSA 等密码算法均为举例性说明，具体使用时均须采用国家密码管理部门批准的相应算法。

信息安全技术　公钥基础设施
电子签名卡应用接口基本要求

1　范围

本标准规定了电子签名卡的基本命令报文和相应的响应报文，以及电子签名卡的文件组织结构。

本标准适用于规范和指导电子签名卡的开发，规范和指导与电子签名卡进行通信，访问卡内文件，应用私钥生成电子签名的应用系统的开发。

本标准不适用于在电子签名卡内创建文件或使用公钥的应用系统的开发。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 16649.8　识别卡　带触点的集成电路卡　第8部分：与安全相关的行业间命令（GB/T 16649.8—2002，ISO/IEC 7816-8：1999，IDT）

ISO/IEC 7816-4：2005　识别卡　带触点的集成电路卡　第4部分：行业间交换的组织结构、安全性和命令（ISO/IEC 7816-4：2005 Identification cards—Integrated circuit cards with contacts—Part 4：Organization，security and commands for interchange）

ISO/IEC 7816-15：2004　识别卡　带触点的集成电路卡　第15部分：密码信息的应用（ISO/IEC 7816-15：2004 Identification cards—Integrated circuit cards with contact—Part 15：Cryptographic information application）

3　术语和定义

下列术语和定义适用于本标准。

3.1

应用　application

为满足特定功能所需的数据结构、数据元和程序模块。

[ISO/IEC 7816-4：2005]

3.2

电子签名卡　electronic signature card

具有生成电子签名功能的安全客户端载体，简称电子签名卡。

3.2

报文　message

应用发送给电子签名卡（或反之）的字节串，不包括传输控制字符。

3.3

命令　command

应用向电子签名卡发出的一条字节串，该信息启动一个操作或请求一个应答。

3.4

响应　response

电子签名卡处理完收到的命令报文后，返回给终端的字节串。