ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30274—2013

信息安全技术　公钥基础设施 电子签名卡应用接口测试规范

Information security techniques—Public Key Infrastructure—Specification of testing on application interfaces of electronic signature card

2013-12-31 发布　　2014-07-15 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 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 1
5　测试环境 …… 1
5.1　硬件 …… 1
5.2　软件 …… 2
5.3　文档 …… 2
6　测试内容 …… 2
6.1　电子签名功能测试 …… 2
6.2　算法实现正确性测试 …… 3
7　测试方法 …… 3
7.1　电子签名功能测试 …… 3
7.2　算法实现正确性测试 …… 6
附录A（资料性附录）　电子签名卡应用接口测试软件接口 …… 7
参考文献 …… 9

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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:飞天诚信科技股份有限公司、中国电子技术标准化研究院、北京数字证书认证股份有限公司、中国信息安全测评中心。

本标准主要起草人:于华章、朱鹏飞、李月新、吴彼、刘伟、赵永省、罗锋盈、上官晓丽、张翀斌、杨永生、郭涛。

信息安全技术　公钥基础设施
电子签名卡应用接口测试规范

1　范围

本标准依据 GB/T 25057—2010 定义的电子签名卡应用接口而规定了测试环境、测试内容、测试方法。

本标准适用于电子签名卡应用接口测试的策划、设计与实施。

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 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

GB/T 25064—2010　信息安全技术　公钥基础设施　电子签名格式规范

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 25057—2010 和 GB/T 25069—2010 中界定的术语和定义适用于本文件。

4　缩略语

下列缩略语适用于本文件。

FCI：文件控制信息(File Control Information)

FID：文件标识符(File ID)

MAC：消息验证码(Message Authentication Code)

PIN：个人鉴别码(Personal Identification Number)

5　测试环境

5.1　硬件

电子签名卡应用接口测试环境的拓扑结构如图 1 所示。