ICS 35.240.15
L 64

中华人民共和国国家标准

GB/T 30001.4—2013

信息技术　基于射频的移动支付 第4部分：卡应用管理和安全

Information technology—Mobile payment based on radio frequency—Part 4：Card application management and security

2013-10-10 发布　　2014-05-01 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 …… Ⅰ
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　多应用安全单元管理模式 …… 2
5.1　以安全单元载体发行机构为中心的管理模式 …… 2
5.2　以多方机构合作的管理模式 …… 2
6　多通道管理 …… 2
6.1　概述 …… 2
6.2　基本逻辑通道 …… 2
6.3　辅助逻辑通道 …… 3
7　生命周期管理 …… 4
7.1　安全单元生命周期管理 …… 4
7.2　应用生命周期管理 …… 7
7.3　安全域生命周期管理 …… 9
7.4　生命周期状态的编码 …… 9
7.5　生命周期状态迁移的命令 …… 10
8　安全单元系统平台安全要求 …… 11
8.1　系统平台固有的防护机制 …… 11
8.2　系统平台存储管理 …… 11
8.3　系统平台状态管理 …… 11
8.4　安全引导 …… 11
8.5　安全恢复 …… 11
8.6　安全通讯机制 …… 12
8.7　防攻击要求 …… 12
8.8　密钥管理 …… 12
8.9　识别与认证 …… 13
9　多应用管理安全要求 …… 13
9.1　应用安全 …… 13
9.2　用户安全 …… 16
附录A（资料性附录）　多应用安全单元的安全防护措施 …… 17
参考文献 …… 19

前　言

GB/T 30001《信息技术　基于射频的移动支付》分为五个部分：

——第1部分：射频接口；

——第2部分：卡技术要求；

——第3部分：设备技术要求；

——第4部分：卡应用管理和安全；

——第5部分：射频接口测试方法。

本部分为GB/T 30001的第4部分。

本部分按照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。

本部分由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本部分起草单位：中国电子技术标准化研究院、武汉天喻信息产业股份有限公司、中国银联股份有限公司、上海复旦微电子集团股份有限公司、北京握奇数据系统有限公司、北京同方微电子有限公司、中国移动通信集团、中国电信集团公司、中国联合网络通信集团有限公司、普天信息技术研究院。

本部分主要起草人：耿力、赵波、柴洪峰、董逢华、高林、单长胜、冯敬、李洁、金倩、丁义民、李蔚、严光文。

信息技术　基于射频的移动支付
第4部分:卡应用管理和安全

1　范围

GB/T 30001的本部分规定了基于射频的移动支付卡中安全单元的多应用安全单元管理模式、多通道管理、生命周期管理、安全单元系统平台安全要求和多应用管理安全要求。

本部分适用于基于射频的移动支付卡的设计、生产和使用。

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 30001.1　信息技术　基于射频的移动支付　第1部分　射频接口

3　术语和定义

GB/T 30001.1界定的以及下列术语和定义适用于本文件。

3.1

安全单元　security element

组成基于射频的移动支付卡的主要器件,主要负责交易关键数据的安全存储和运算功能。

3.2

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。

[GB/T 16649.4—2010,定义3.3]

3.3

应用提供者　application provider

提供安全单元上应用组成部分的实体。

3.4

安全单元系统平台　system platform on security element

安全单元上负责基本功能的组件。

3.5

安全域　security domain

向应用提供者提供控制、安全和通信支持的卡上实体。

4　缩略语

下列缩略语适用于本文件。

ADF　　应用定义文件(Application Definition File)

AID　　应用标识符(Application Identifier)