ICS 35.240.15
L 64

中华人民共和国国家标准

GB/T 29271.4—2019

识别卡　集成电路卡编程接口
第4部分:应用编程接口(API)管理

Identification cards—Integrated circuit card programming interfaces—Part 4:Application programming interface (API) administration

(ISO/IEC 24727-4:2008,MOD)

2019-08-30 发布　　2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 29271《识别卡　集成电路卡编程接口》分为以下六个部分：

——第1部分：体系结构；

——第2部分：通用卡接口；

——第3部分：应用接口；

——第4部分：应用编程接口(API)管理；

——第5部分：测试规程；

——第6部分：实现互操作的鉴别协议的注册管理规程。

本部分为GB/T 29271的第4部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用重新起草法修改采用ISO/IEC 24727-4:2008《识别卡　集成电路卡编程接口　第4部分：应用编程接口(API)管理》。

本部分与ISO/IEC 24727-4:2008的技术性差异及其原因如下：

——关于规范性引用文件，本部分做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第2章“规范性引用文件”中，具体调整如下：

- 增加引用了GB/T 16649.15 (GB/T 16649.15—2010，ISO/IEC 7816-15:2004，IDT)(见5.8，7.5和第8章)；
- 用等同采用国际标准的GB/T 29271.1代替了ISO/IEC 24727-1(见5.1、第7章和8.1)；
- 用等同采用国际标准的GB/T 29271.2代替了ISO/IEC 24727-2(见第5章、第6章、第8章、附录A和附录F)；
- 用修改采用国际标准的GB/T 29271.3代替了ISO/IEC 24727-3(见第5章、第6章、第7章、第8章、附录A、附录F、附录H、附录I和附录L)；
- 将参考文献ISO/IEC 19784-1:2006移至规范性引用文件，并用等同采用国际标准的GB/T 30267.1—2013代替(见7.5)；
- 增加引用了ISO/IEC 24727-2:2008/Amd 1:2014(见5.8)；
- 增加引用了ISO/IEC 7816-15:2004/Amd 2:2008(见8.1、G.2.16和G.4.1)；
- 将国际标准中出现的ISO/IEC 24727-5移至规范性引用文件(见5.1和图1)。

——增加缩略语ACD、ACR、AR、DID、GCI、ICC、IFD、Kenc、Kmac、PCD和SAL。

本部分还做了下列编辑性修改：

——纳入国际标准技术勘误ISO/IEC 24727-4 COR 1:2011的内容(见附录B的B.1、B.2、B.3、附录C的C.1、C.2、附录D和附录E)；

——纳入国际标准修正单ISO/IEC 24727-4/Amd 1:2014的内容(见5.8、第8章、附录F～附录L)；

——图统一从图1开始编号，不再采用原图标序号；

——表统一从表1开始编号，不再采用原表序号；

——调整了缩略语顺序；

——将国际标准中出现的悬置段编号并加标题，并依序调整下文的条标题编号；

——附录D的第一句“ISO24727-4-IFDAPI{iso(1) standard(0) iso24727(24727) part4(4) ifdapi(74)}”，改为“GB/T 29271.4-IFDAPI{1.2.156.5006.29271.4.74}”；

——附录D的第8行“ISO24727-COMMON{iso(1) standard(0) iso24727(24727)”，改为

“GB/T 29271-COMMON{1.2.156.5006.29271}”；

——附录D的第11、12行中的“revMajISO24727-4-IFDAPI” “revMinISO24727-4-IFDAPI”，改为“revMajGBT29271-4-IFDAPI”“revMinGBT29271-4-IFDAPI”；

——附录E的第一句“ISO24727-4-TCAPI{iso(1) standard(0) iso24727(24727) part4(4) tcapi(73)}”，改为“GB/T 29271.4-TCAPI{1.2.156.5006.29271.4.73}”；

——附录E的第8行“ISO24727-COMMON{iso(1) standard(0) iso24727(24727)}”，改为“GB/T 29271-COMMON {1.2.156.5006.29271}”；

——附录I的I.2.2.3.1的第一句中的“G.2”，改为“I.2.2.3”；

——附录I的I.2.2.3.3的倒数第7行“iso(1) standard(0) iso24727(24727) part3(3) annex-a(0)”，改为“1.2.156.5006.29271.3.0”；

——附录I表I.1中的“CARD-APPLICATION myservice”，改为“CARD-APPLICATION myservice”；

——附录J的第4行“ISO/IEC 24727-4-PE {iso(1) standard(0) iso24727(24727) part4(4) clause(8.1.3)}”，改为“GB/T 29271.4-PE {1.2.156.5006.29271.4 clause(8.4)} ”；

——附录J的第9行“ISO24727-COMMON{iso(1) standard(0) iso24727(24727)}”，改为“GB/T 29271.4-COMMON {1.2.156.5006.29271}”；

——附录K的K.1的标题修改为“示例”，删除“摘自欧盟标准CEN/TS 15480-3”；

——删除了参考文献。

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、北京智芯微电子科技有限公司、楚天龙股份有限公司、上海一芯智能科技有限公司、深圳赛西信息技术有限公司、紫光同芯微电子有限公司、北京握奇数据系统有限公司、飞天诚信科技股份有限公司、大唐微电子技术有限公司、中电智能卡有限责任公司、北京中电华大电子设计有限责任公司、红天智能科技(天津)有限公司、金邦达有限公司、东信和平科技股份有限公司、中国科学院自动化研究所、北京眼神智能科技有限公司、上海复旦微电子集团股份有限公司、上海密特印制有限公司。

本部分主要起草人：曹国顺、付青琴、蒋曲明、高伟、苏爱民、盛敬刚、秦日臻、白婧、朱鹏飞、张树蕊、原爱阳、李斌、夏立佳、李丹、邴志刚、张璋、徐平江、徐木平、钟陈、张汉就、王厚金、余晖、史春腾、邵兴、吴行宇、张晓良、庞振江。

引　言

GB/T 29271 定义了一组集成电路卡(ICC)和外部应用之间交互的编程接口,包括多部门使用的通用服务。ICC 的组织和操作符合 GB/T 16649.4—2010。

GB/T 29271 与不同应用领域之间有互操作要求的 ICC 应用相关。

GB/T 9387.1:1998 用作客户端应用到卡端应用连接的分层结构。也就是说,应用接口假定存在这样的协议栈:通过它可以利用命令来交换卡片间的信息和事务。传送这些命令的报文结构在 GB/T 16649 中定义。应用接口访问的命令的语义参考应用协议数据单元(APDU,在 GB/T 29271.2 中有描述)及以下标准:

——GB/T 16649.4—2010　识别卡　集成电路卡　第 4 部分:用于交换的结构、安全和命令

——GB/T 16649.8—2002　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 16649.9—2010　识别卡　集成电路卡　第 9 部分:用于卡管理的命令

GB/T 29271 的目标是最大化软件工具的适用性和解决方案空间,为支持卡片的客户端应用程序提供应用程序接口支持。该工作包括:当卡片变得更强大、同级伙伴存在以及将来应用的时候,支持卡片系统的演进,从而使得对符合 GB/T 29271 标准要求的已有方案的影响最小。

符合本部分,可以实现 GB/T 29271.3 和 GB/T 29271.2 的互操作实现。本部分没有定义实施细节;可假定符合可接受的安全策略。具体的安全策略不在 GB/T 29271 的范围之内。

识别卡　集成电路卡编程接口
第4部分:应用编程接口(API)管理

1　范围

GB/T 29271定义了一组集成电路卡(ICC)和外部应用之间交互的编程接口,包括多部门使用的通用服务。

GB/T 29271的本部分规定了客户端应用和卡端应用之间的连接和安全机制。本部分规定API管理符合GB/T 29271标准的独立于服务和独立于实现的模块,包括安全性,可以对ICC的特定卡端应用发出操作请求,以便在与数据模型和内容发现操作耦合时,卡端应用可以被各种客户端应用使用。

本部分适用于ICC和外部应用的连接,以便各种客户端应用可以采用统一接口调用卡端应用。

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 15852.1—2008　信息技术　安全技术　消息鉴别码　第1部分:采用分组密码的机制(ISO/IEC 9797-1:1999,IDT)

GB/T 16649.4—2010　识别卡　集成电路卡　第4部分:用于交换的结构、安全和命令(ISO/IEC 7816-4:2005,IDT)

GB/T 16649.15　识别卡　集成电路卡　第15部分:密码信息应用(GB/T 16649.15—2010,ISO/IEC 7816-15:2004,IDT)

GB/T 29271.1　识别卡　集成电路卡编程接口　第1部分:体系结构(GB/T 29271.1—2012,ISO/IEC 24727-1:2007,IDT)

GB/T 29271.2　识别卡　集成电路卡编程接口　第2部分:通用卡接口(GB/T 29271.2—2012,ISO/IEC 24727-2:2008,IDT)

GB/T 29271.3　识别卡　集成电路卡编程接口　第3部分:应用接口(GB/T 29271.3—2014,ISO/IEC 24727-3:2008,MOD)

GB/T 30267.1—2013　信息技术　生物特征识别应用程序接口　第1部分:BioAPI规范(ISO/IEC 19784-1:2006,IDT)

ISO/IEC 7816-3:2006　识别卡集成电路卡　第3部分:带触点的卡　电信号和传输协议(Identification cards—Integrated circuit cards—Part 3: Cards with contacts—Electrical interface and transmission protocols)

ISO/IEC 7816-15:2004/Amd 2:2008　识别卡　集成电路卡　第15部分:密码信息应用　修改单2:2008(ISO/IEC 7816-15:2004　Identification cards—Integrated circuit cards—Part 15:Cryptographic information application/Amd 2:2008)

ISO/IEC 24727-2:2008/Amd 1:2014　识别卡　集成电路卡编程接口　第2部分:通用卡接口 修改单1:2014(ISO/IEC 24727-2:2008　Identification cards—Integrated circuit card programming interfaces—Part 2:Generic card interface/Amd 1:2014)