



# 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 .....	V
引言 .....	VII
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	2
4 缩略语 .....	3
5 体系结构规范 .....	3
5.1 概述 .....	3
5.2 全网络栈 .....	6
5.3 忠诚栈 .....	8
5.4 不透明 ICC 栈 .....	8
5.5 远程忠诚栈 .....	9
5.6 ICC 本地栈 .....	10
5.7 远程 ICC 栈 .....	11
5.8 服务访问层扩展 .....	12
6 安全体系结构 .....	16
6.1 路径保护政策 .....	16
6.2 访问控制列表-访问控制规则(ACL-ACR)映射 .....	17
6.3 安全报文传输 .....	17
6.4 可信信道密钥管理 .....	18
7 连接组件 .....	18
7.1 概述 .....	18
7.2 操作请求和响应语义 .....	18
7.3 委托-代理(Proxy-Agent)体系结构 .....	18
7.4 可信信道接口(TC_API) .....	19
7.5 接口设备 API(IFD API) .....	23
8 GB/T 16649.15 注册实施 .....	38
8.1 概述 .....	38
8.2 GB/T 29271.3 数据结构映射 .....	39
8.3 SAL API 操作映射到 GB/T 16649.15 属性 .....	46
8.4 特定卡 APDU 映射到 GB/T 16649.15 属性 .....	51
8.5 GB/T 29271.3 数据结构存储在卡上 .....	52
附录 A (规范性附录) 路径保护机制 .....	54
附录 B (资料性附录) IFD-API:Web 服务绑定 .....	62
附录 C (资料性附录) IFD-Callback-API-Web 服务绑定 .....	93

附录 D (资料性附录) GB/T 29271.4-IFDAPI 模块	96
附录 E (资料性附录) GB/T 29271.4-TCAPI 模块	113
附录 F (资料性附录) 程序元素的增强使用	118
附录 G (资料性附录) 用于 GB/T 16649.15 数据结构处理的 API	130
附录 H (资料性附录) 轻量级服务访问层(SAL API LITE)	174
附录 I (资料性附录) 密码信息应用示例	175
附录 J (资料性附录) 转换 ASN.1 模块	186
附录 K (资料性附录) 可互操作访问存储库	187
附录 L (资料性附录) CryptoAPI(CAPI)通过程序元素访问	191
图 1 GB/T 29271 体系结构	4
图 2 GB/T 29271 栈的通用元素	5
图 3 后续数据的图例	6
图 4 卡端应用和客户端应用之间的网络连接	7
图 5 GB/T 29271.2 和 GB/T 29271.3 层的专有实现	8
图 6 不透明 ICC 栈	9
图 7 远程忠诚栈	10
图 8 ICC 本地栈	11
图 9 远程 ICC 栈配置	12
图 10 网络栈	14
图 11 委托-代理机制	18
图 12 发现鉴别协议值	43
图 13 GB/T 16649.15 信息对象和 GB/T 29271.3 数据结构之间的关系	53
图 A.1 带安全报文传输和不带安全报文传输的通信	54
图 A.2 命令头转换	55
图 A.3 在 INS 为奇数值时创建包含加密数据的 DO	55
图 A.4 创建包含密码校验和的 DO	56
图 A.5 创建包含 Le 字段的 DO	56
图 A.6 MAC 运算	57
图 A.7 创建包含状态字节的 DO	58
图 A.8 保护 CASE4 命令 APDU	59
图 A.9 保护带数据字段的响应 APDU	60
图 F.1 程序元素功能	119
图 F.2 完整互操作网络栈	120
图 F.3 当前全网络栈	122
图 F.4 建议配置	123
图 F.5 当前忠诚栈	124
图 F.6 建议忠诚栈	124
图 F.7 当前不透明 ICC 栈	125
图 F.8 建议不透明 ICC 栈	125
图 F.9 当前远程忠诚栈	126

图 F.10	建议远程忠诚栈 .....	127
图 F.11	当前远程 ICC 栈 .....	128
图 F.12	建议远程 ICC 栈 .....	128
图 I.1	基于 UML 的 eService 计算模型 (基于 GB/T 29271 对象) .....	176
图 L.1	启用 CAPI 的程序元素 .....	193
图 L.2	PKCS 11 的加密服务 .....	194
表 1	命令进程 .....	15
表 2	每个栈配置的每个类别的路径保护策略类 .....	17
表 3	可信信道 API .....	19
表 4	DataSet 映射到 ACL .....	39
表 5	CardApplication 映射到 DataContainerObjectChoice .....	40
表 6	Service 映射到 ACL .....	42
表 7	authObject 映射到 DID .....	44
表 8	Secret Key 映射到 DID .....	45
表 9	private Key 映射到 DID .....	46
表 10	SAL API 操作映射到 GB/T 16649.15 属性 .....	47
表 11	DataContainerObject 的属性 (GB/T 16649.15 DO) .....	51
表 12	EF 或 DO 识别 .....	51
表 13	EF 文件内容示例 .....	52
表 A.1	安全报文传输中各字段使用的值 .....	60
表 I.1	基于对象的 "myservice" 数据集 .....	177
表 I.2	用于卡端应用和 DataSet 对象的 GB/T 16649.15 数据对象封装 .....	178

## 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 and 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)