10．ISO 7816-10：Electronic signals and answer to reset for synchronous cards（同步卡的电信号和复位应答）

本部分规定了在集成电路卡和接口设备（如终端）之间同步传输使用的电源、信号结构及复位应答结构。

本部分同时涵盖了信号速率、操作条件、与集成电路卡的通信。

本部分定义了 type-1 和 type-2 两种同步卡。

11．ISO 7816-11：Personal verification through biometric methods（通过生物识别方法的个人验证）

本部分规定了集成电路卡在行业间命令中使用生物识别方法验证个人的安全机制，它还定义了把卡作为生物参考数据或设备的数据结构和数据访问方法。

本标准不定义使用生物识别方法对人员的识别过程。

12．ISO 7816-12：Cards with contacts：USB electrical interface and operating procedures（带触点集成电路卡：USB 电气接口及操作规程）

本部分规定了提供 USB 接口的 IC 卡的操作条件，图 29-1 展示了 USB 接口的触点分配和此分配与 ISO/IEC7816-3 中使用的触点分配的相互关系。

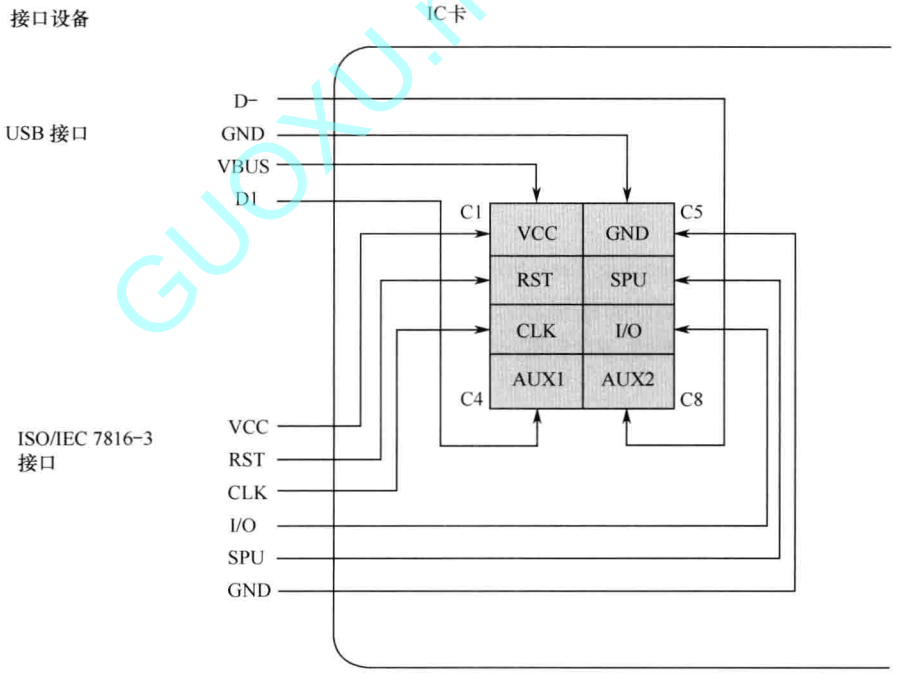

图 29-1　带有 USB 接口的 IC 卡的触点分配

13．ISO 7816-13：Commands for application management in multi-application environment（在多应用环境中用于应用管理的命令）

本部分规定了在多应用环境下用于应用管理的命令，这些命令涵盖了多应用环境下的应用的整个生命周期。可以在卡发行到持卡者手中之前或之后使用这些命令。

本规范没有涵盖卡内和/或外界的内部实现。

14．ISO 7816-15：Cryptographic information application（密码信息应用）

本部分规定了卡的一种应用，该应用包含密码功能的信息。

本部分定义了用于密码信息的通用语法和格式，以及在适当时共享该信息的机制。

本部分旨在：

- 便于运行于不同平台的各部分间的交互性（平台无关）；
- 使外部应用能利用多个制造商的产品和组件（厂商无关）；
- 使无需重写应用层的软件也能使用更先进的技术（应用无关）；
- 在维持现有的、相关的标准一致性的同时，进行必要的和可行的扩展。

本部分支持下列功能：

- 在卡中存储密码信息的多个实例；
- 使用密码信息；
- 检索密码信息，这一功能的关键因素在于“目录文件”的概念，它提供了卡上对象和这些对象实际格式之间的一个间接层；
- 适当时候，用 ISO/IEC 7816 其他部分中定义的数据对象来交叉引用密码信息；
- 不同的鉴别机制；
- 多个密码算法。

本规范没有涵盖卡内和/或外界的内部实现。

不强制要求执行本部分的所有选项。

29.3 IETF RFC 系列

在 IETF（Internet Engineering Task Force）内有 PKIX（Public-Key Infrastructure（X.509））工作组，负责与 X.509 有关的规范管理，PKIX 工作组从 1995 年 10 月 26 日开始启动，到 2013 年 10 月 31 日关闭，在近 20 年间，发布了大量 RFC 规范。

1．RFC 2459

名称：Internet X.509 Public Key Infrastructure Certificate and CRL Profile。

发布日期：1999-01。

状态：被 RFC3280 替代。

简述：介绍了应用于互联网 PKI 证书和证书撤销列表的格式和语义。描述了在互联网环境中证书路径的处理，提供密码学算法的编码规则。

2．RFC 2510

名称：Internet X.509 Public Key Infrastructure Certificate Management Protocols。

发布日期：1999-03。

状态：被 RFC4210 替代。

简述：描述了互联网 X.509 PKI 证书管理协议（CMP），定义了证书生成和管理所有相关方面的协议消息。

3．RFC 2511

名称：Internet X.509 Certificate Request Message Format。

发布日期：1999-03。

状态：被 RFC4211 替代。

简述：描述了证书请求消息格式（CRMF）。它被用来向 CA 传递一个产生 X.509 证书的请求（可能通过 RA）。请求消息一般包括公钥和有关的注册信息。

4．RFC 2527

名称：Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework。

发布日期：1999-03。

状态：被 RFC3647 替代。

简述：提供了一个帮助写作证书策略和证书业务规则的框架。特别地，此框架提供了一系列需要在证书策略和证书业务规则中进行说明的综合主题。

5．RFC 2528

名称：Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm（KEA）Keys in Internet X.509 Public Key Infrastructure Certificates。

发布日期：1999-03。

简述：描述了 X.509 v3 证书中包含 KEA（密钥交换算法）密钥的格式和语义。说明了公钥信息和密钥用途扩展项的内容。

6．RFC 2559

名称：Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2。

发布日期：1999-04。

状态：被 RFC3494 替代。

简述：描述了访问 PKI 信息库以获取信息和管理这些信息的需求，它基于 LDAP 协议，定义了使用和更新证书编码和证书撤销列表的协议框架。

7．RFC 2560

名称：X.509 Internet Public Key Infrastructure Online Certificate Status Protocol（OCSP）。

发布日期：1999-06。

状态：被 RFC6960 替代，由 RFC6277 更新。

简述：在线证书状态查询协议，描述了无需证书撤销列表就可以决定一张数字证书当前状态的协议。

8．RFC 2585

名称：Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP。

发布日期：1999-05。

简述：描述了使用 FTP（File Transfer Protocol）和 HTTP（Hypertext Transfer Protocol）协议获取证书和证书撤销列表（CRLs）的方法。

9. RFC 2587

名称：Internet X.509 Public Key Infrastructure LDAPv2 Schema。

发布日期：1999-06。

状态：被 RFC4523 替代。

简述：描述了以支持在 LDAPv2 环境中使用 PKI 而定义的最小 schema（语法）。

10. RFC 2797

名称：Certificate Management Messages over CMS。

发布日期：2000-04。

状态：被 RFC5272 替代。

简述：定义了使用 CMS 进行证书管理的协议，以满足基于 CMS 和 PKCS10 进行证书服务的接口需求，以及满足基于 SMIMEV3 使用 DH（Diffie-Hellman）公钥并用 DSA 签名的证书注册请求。

11. RFC 3029

名称：Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols。

发布日期：2001-02。

简述：描述了通用数据验证和证书服务器及与之进行通信的协议，数据验证和证书服务器可以认为是受信任的第三方机构，用来构建不可否认服务。

12. RFC 3161

名称：Internet X.509 Public Key Infrastructure Time-Stamp Protocol（TSP）。

发布日期：2001-08。

状态：被 RFC5816 更新。

简述：描述了发送到时间戳机构的请求数据格式和返回的响应数据格式，并说明了安全需求。

13. RFC 3279

名称：Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List（CRL）Profile。

发布日期：2002-05。

状态：被 RFC4055、RFC4491、RFC5480、RFC5758 更新。

简述：描述了应用于 X.509 公钥证书和证书撤销列表的算法和算法标识符。

14. RFC 3280

名称：Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List（CRL）Profile。

发布日期：2002-05。

状态：被 RFC5280 替代，被 RFC4325、RFC4630 更新。

简述：替代 RFC2549。描述了 X.509 v3 证书和 X.509 v2 的证书撤销列表（CRL）在互

联网的使用。详细描述了 X.509 v3 证书格式、证书标准扩展，增加了与互联网相关的两项扩展，并指定了必要证书扩展。详细描述了 X.509 v2 的证书撤销列表格式和必要扩展。

15. RFC 3281

名称：An Internet Attribute Certificate Profile for Authorization。

发布日期：2002-05。

状态：被 RFC5755 替代。

简述：描述了基于授权的属性证书。

16. RFC 3379

名称：Delegated Path Validation and Delegated Path Discovery Protocol Requirements。

发布日期：2002-09。

简述：描述了公钥证书的委托路径验证（DPV）和委托路径发现（DPD）需求，以及 DPV 和 DPD 的管理策略需求。

17. RFC 3628

名称：Policy Requirements for Time-Stamping Authorities（TSAs）。

发布日期：2003-11。

简述：定义了基准时间戳策略需求，时间戳机构使用公钥证书发布时间戳标记，时间戳可精确到 1 秒或更小。

18. RFC 3647

名称：Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework。

发布日期：2003-11。

简述：替代 2527，增加了更多内容。提供了一个帮助写作证书策略和证书业务规则的框架。特别是此框架提供了一系列需要在证书策略和证书业务规则中进行说明的综合主题。

19. RFC 3709

名称：Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates。

发布日期：2004-02。

状态：被 RFC6170 更新。

简述：描述了包含可视化信息（如图片、声音等）的证书扩展项。

20. RFC 3770

名称：Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol（PPP）and Wireless Local Area Networks（WLAN）。

发布日期：2004-05。

状态：被 RFC4334 替代。

简述：定义了两项 EAP（Extensible Authentication Protocol）扩展密钥用途，且包含 WLAN（Wireless LAN）系统服务标识的证书扩展项。