ICS 35.240.15
A 11

中华人民共和国国家标准

GB/T 16791.1—1997
idt ISO 9992-1:1990

金融交易卡　集成电路卡与卡接受设备之间的报文　第1部分：概念与结构

Financial transaction cards—Messages between the integrated circuit card and the card accepting device—Part 1:Concepts and structures

1997-05-26发布　　1998-03-01实施

国家技术监督局　发布

前　言

本标准等同采用国际标准 ISO 9992-1:1990《金融交易卡——集成电路卡与卡接受设备之间的报文——第 1 部分:概念与结构》。

GB/T 16791 在总标题"金融交易卡　集成电路卡和卡接收设备之间的报文"下,由以下部分构成:

——第 1 部分:概念与结构

——第 2 部分:功能、报文(命令和响应)、数据元和结构

本标准的附录 A 是提示的附录。

本标准在引用标准中与 ISO 9992-1 略有差异,原因是在 ISO 9992-1 中引用的 ISO 7812:1987《识别卡——发卡者标识符编号体系和注册程序》已在 1993 年经修订后被划分为两部分,即 ISO/IEC 7812-1:1993《识别卡——发卡者标识——第 1 部分:编号体系》和 ISO/IEC 7812-2:1993《识别卡——发卡者标识——第 2 部分:申请和注册程序》,并已都被等同采用为国家标准,相应国家标准编号为 GB/T 15694.1—1995和 GB/T 15694.2—1996。因此,在引用该标准时按新标准加以标注。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会归口管理。

本标准起草单位:中国人民银行、中国工商银行、中国标准化与信息分类编码研究所。

本标准主要起草人:刘钟、孟桂清、王珈、王云生、卢小冰、房庆、陆书春、聂舒。

ISO 前言

ISO(国际标准化组织)是一个世界范围的国家团体(ISO 成员团体)标准化联盟。通过 ISO 技术委员会的活动来推动国际标准化工作。对已成立技术委员会的工作感兴趣的每个成员团体都有权参与该委员会的工作。与 ISO 有联系的官方或非官方的各国际组织也参与委员会的工作。ISO 和 IEC(国际电工技术委员会)在电工技术标准的所有领域密切合作。

技术委员会制定的国际标准草案将被分发给各成员团体进行表决。作为一项国际标准发布至少需要 75%以上的参加投票的成员团体的投票赞成。

国际标准 ISO 9992-1 由“银行及相关金融业务技术委员会”ISO/TC 68 制定。

ISO 9992 在总标题“金融交易卡——集成电路卡和卡接收设备之间的报文”下,由以下部分构成:

——第 1 部分:概念与结构;

——第 2 部分:功能、报文(命令和响应)、数据元和结构。

本标准的附录 A 仅提供参考信息。

中华人民共和国国家标准

金融交易卡 集成电路卡与卡接受设备之间的报文 第1部分:概念与结构

GB/T 16791.1—1997
idt ISO 9992-1:1990

Financial transaction cards—Messages between the integrated circuit card and the card accepting device—Part 1:Concepts and structures

引言

GB/T 16791 的本部分所定义的概念基于如下考虑:

GB/T 16791 的本部分与第 2 章引用的已有标准兼容,其目的在于为未来集成电路卡(ICC)技术的使用提供灵活性。

GB/T 16791 的本部分支持 ICC 的单一应用或多种应用。当 ICC 具有多种应用时,可能出现相同服务类型(例如电子支票簿)的多种应用。在 ICC 生命周期内的任何时间,应遵从 GB/T 16790 规定的安全性原则,在得到发卡机构同意的情况下,可以在卡中增加应用项目。在卡生命周期内的任何时间,按照业务参与方之间商定的处理方法,可在逻辑上从 ICC 中删除某项应用。

1 范围

GB/T 16791 的本部分适合于将金融机构发行的集成电路卡在交换环境下的零售金融应用中使用。它明确规定了:

——金融交换所要求的功能;

——在集成电路卡(ICC)与卡接受设备(CAD)之间,实现这些功能的报文结构和类型;

——在 ICC 与 CAD 之间进行交换时,可能使用或将要使用的数据元标识和定义。

本标准建立了 ICC 和 CAD 交换报文的概念。因此,必须对 ICC 中数据的逻辑结构进行说明。

GB/T 16791 的本部分对多种报文进行了定义,用以支持鉴别的安全性要求(例如:卡鉴别、CAD 鉴别、持卡人身份验证)。它不规定或推荐任何方法或处理过程。安全技术依据 GB/T 16790 的规定实现。

GB/T 16791 的本部分与 CAD 的性能(可连接或不可连接,有人值守或无人值守)和状态(联机或脱机)无关。

GB/T 16791 的本部分不定义实现应用的方法。

GB/T 16791 的本部分基于数据的逻辑结构,提供了 CAD 对 ICC 中的数据进行逻辑引用所用方法的准则。它不定义 ICC 中数据的物理结构。

2 引用标准

下列标准所包含的条文,通过在本标准中引用而构成为本标准的条文。本标准出版时,所示版本均为有效。所有标准都会被修订,使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 14504—93 银行卡(eqv ISO 4909:1987)

国家技术监督局 1997-05-26 批准　　1998-03-01 实施

GB/T 14916—94 识别卡 物理特性(idt ISO 7810:1985)

GB/T 15694.1—1995 识别卡 发卡者标识 第1部分:编号体系(idt ISO/IEC 7812-1:1993)

GB/T 15694.2—1996 识别卡 发卡者标识 第2部分:申请和注册程序 (idt ISO/IEC 7812-2:1993)

GB/T 16649.3—1996 识别卡 带触点的集成电路卡 第3部分:电子信号和传输协议 (idt ISO 7816-3:1989)

GB/T 16790.1—1997 金融交易卡 使用集成电路卡的金融交易系统的安全结构 (idt ISO 10202-1:1991)

ISO 7813:1987 识别卡——金融交易卡

ISO 7816-4[1] 识别卡——带触点的集成电路卡——第4部分:行业间命令(ISO/IEC 1/17/4 正在进行研究)

3 定义

本标准采用下列定义。

3.1 应用数据文件(ADF) Application Data File

支持一项或多项服务的文件。

3.2 卡接受设备(CAD) Card Accepting Device

用于与集成电路卡接口的设备。

3.3 命令 command

一个请求或通知报文,它启动一个动作,并且引发一个响应。

3.4 公共数据文件(CDF) Common Data File

一个强制性文件,它包含存储在ICC中的公共数据元,用以标识卡、发卡者和持卡人。

3.5 文件 file

ICC中的数据元和(或)程序代码的有组织的集合。

3.6 功能 function

由一个或多个命令及其相关动作完成的处理过程,用于实现一个交易的全部或部分。

3.7 集成电路卡(ICC) Intergrated Circuit Card

嵌入一个或多个集成电路的ID-1型卡(见GB/T 14916)。

3.8 报文 message

一个从CAD传输到ICC或从ICC传输到CAD的有序字符序列。

3.9 主帐号(PAN) Primary Account Number

一个被制定用以标识发卡者和持卡人的号码。它由发卡者标识号、个人帐户标识和一个附带的校验数字组成。

注:此号码等效于按GB/T 15694.1和GB/T 15694.2规定的标识号码。还可参见GB/T 14504。

3.10 个人识别号(PIN) Personal Identification Number

用户拥有的、用来验证其身份的代码或口令。

3.11 响应 response

处理所接收到的命令后返送给发起方的一个报文。

4 概念和结构

4.1 ICC中数据的逻辑结构

1) 将要出版。

逻辑数据结构能使 ICC 以最小的数据重复支持相互独立的服务。这些服务可以由不同的应用提供者提供。

公共数据文件(CDF)中包含 ICC 支持的所有服务都可能使用的数据(例如:PAN,卡的终止日期)。一个 ICC 中,只能有一个 CDF。发卡者应对 CDF 的存在、内容和使用负责。

存储在 ICC 中服务于商业交易的数据包含在 CDF 和(或)应用数据文件(ADF)中。在一个 ICC 中,可以存在一个或多个 ADF,以适应不同的金融或非金融服务。

ICC 中可以包含不带 ADF 的 CDF。

4.2 ICC 和 CAD 之间的交互作用

ICC 和 CAD 通过报文交互作用。这些报文(即命令及其响应)用于完成交易的部分或全部功能。

附录 A 用图示说明下面所述各种关系。

4.2.1 交易与功能之间的关系

一笔交易(例如:提取现金、购物、更改 PIN)由一个或多个功能(例如:持卡人身份验证、CAD 鉴别、交易的记录)构成。

GB/T 16791 的第 2 部分规定了用于国际金融交换的各个功能,在国际金融交换中可强制或推荐使用这些功能。可以增加一些附加的功能以支持由双方协议定义的活动。

4.2.2 功能与报文之间的关系

在 4.3.1 中描述的功能可用一对或多对报文来完成。这些报文是命令(例如:读、写)和其响应(例如:确认、数据)。在处理一条命令并产生一个决定或动作后,接收方应给发送方返回一个响应。

GB/T 16791 的第 2 部分规定了用来完成每个功能的命令和响应。

ISO 7816-4 描述了通用命令,GB/T 16791 的第 2 部分描述了金融 ICC 的专用命令。

4.3 数据访问属性

4.3.1 读访问属性

三类读访问定义如下:

公共读访问(PR):数据可不受任何限制地被 CAD 读取。

条件读访问(CR):只有满足特定的判断条件后,数据才能够被读取。

禁止读访问(NR):数据永远不能被 CAD 读取。

4.3.2 写访问属性

三类写访问定义如下:

自由写访问(FW):数据可以不受任何限制地增加、修改或删除。

条件写访问(CW):只有满足特定的判断条件后,数据才可以增加、修改或删除。

一次写访问(OW):数据一经写入,不能变更或修改。

4.4 与当前技术的兼容性

主帐号(PAN)应永远存放在 CDF 中(见 GB/T 15694、ISO 7813 和 GB/T 14504)。

如果 ICC 还包含着一个凸印的 PAN 和(或)按 ISO 7813 编码的磁条,CDF 中的国际交换 PAN 应与凸印的和(或)在磁条上编码的 PAN 一致。

附 录 A
（提示的附录）
交易、功能和报文之间的关系

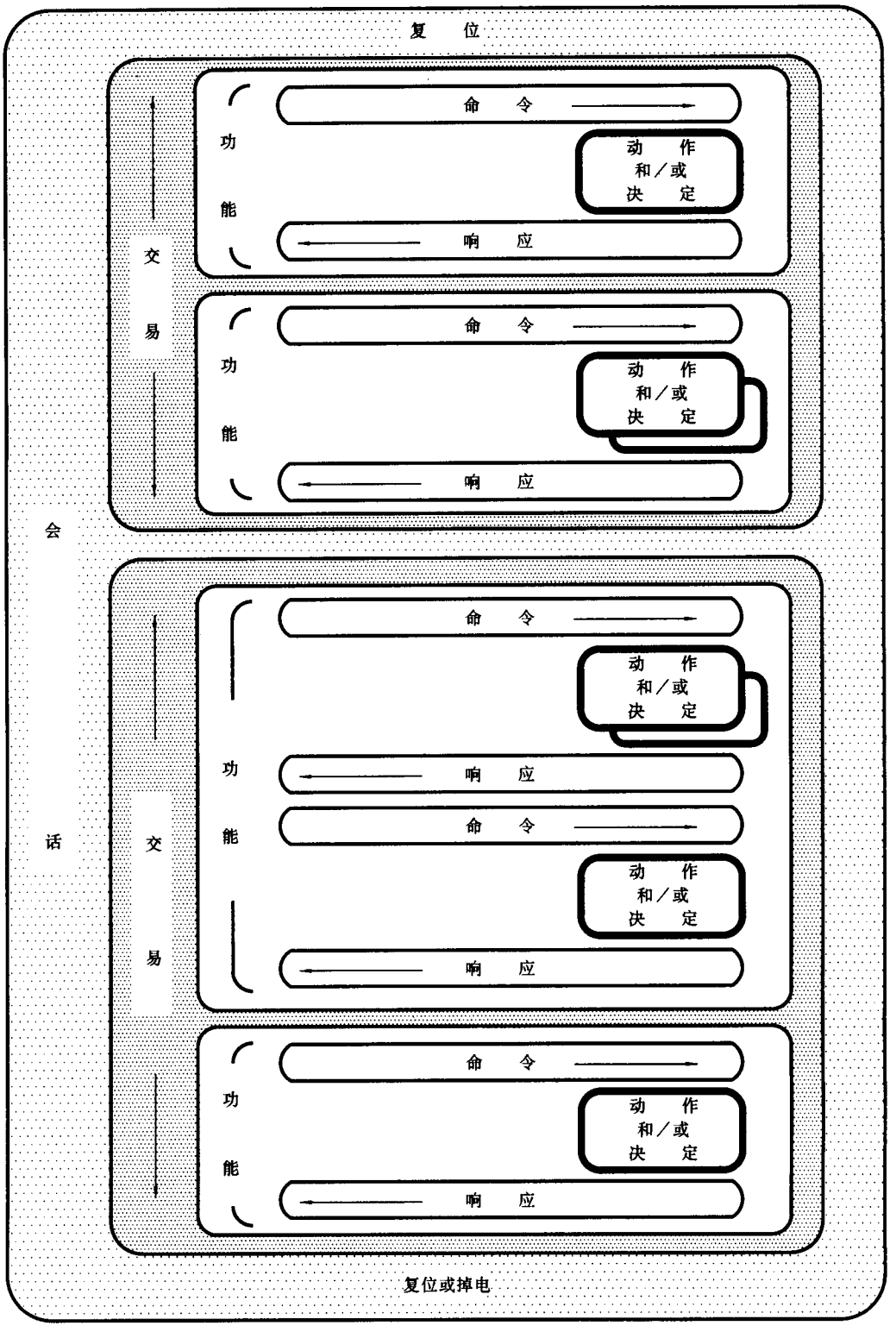

图 A1

A1 关于ICC关系的表示方法

图A1显示了一个会话的各组成部分之间的关系，这个会话通过将ICC插入CAD来启动，并通过将ICC移出CAD而终止。

图A1并不意味着报文流是单一方向的(从CAD到ICC)，也不意味着将来的技术将受到这些界限(例如：整个交易可能只需一个命令和响应就可以完成)的限制。

图A1标出了三级关系：

a) 由引起单一动作或决定、并随后跟有响应的单一命令所构成的功能可表示为：

F=[C1+A1/D1+R1]

b) 由多组命令、动作或决定和响应所组成的功能可表示为：

F=[(C1+A1+R1)+(C2+D2+R2)……+(C5+D5+R5)]

c) 由具有多个动作和决定的单一命令和响应组成的功能可表示为：

F=[C1+(A1+D2+A3)+R1]

其中，F表示功能；

C1、C2等表示命令；

A1、A2等表示动作；

D1、D2等表示决定；

R1、R2等表示响应。

中 华 人 民 共 和 国
国 家 标 准
金融交易卡 集成电路卡与卡接受设备之间的报文
第1部分:概念与结构
GB/T 16791.1—1997
*
中国标准出版社出版
北京复兴门外三里河北街16号
邮政编码:100045
电 话:68522112
中国标准出版社秦皇岛印刷厂印刷
新华书店北京发行所发行 各地新华书店经售

*
开本 880×1230 1/16 印张 3/4 字数 12 千字
1997年12月第一版 1998年3月第二次印刷
印数 501—1 500
*
书号:155066·1-14403 定价10.00元
*
标 目 325—25

GB/T 16791.1-1997