

GUANGZHOU SHI SHE HUI BAO ZHANG KA DE FA XING YU YUN YONG

广州市社会保障卡的 发行与应用

GUANGZHOU SHI SHE HUI BAO

胡勇 编著

.1

中山大学出版社

广州市 社会保障卡的发行与应用

胡 勇 编著

中山大学出版社
·广州·

版权所有 翻印必究

图书在版编目(CIP)数据

广州市社会保障卡的发行与应用/胡勇编著. —广州:中山大学出版社, 2003.10

ISBN 7-306-02177-X

I. 广… II. 胡… III. 社会保障-智能卡-研究-广州市
IV. D632.1

中国版本图书馆 CIP 数据核字(2003)第 085368 号

责任编辑:吴相辉 舒宝明 封面设计:刘 强 责任校对:方 园
责任技编:黄少伟

中山大学出版社出版发行

(地址:广州市新港西路 135 号 邮编:510275)

电话:020-84111998、84037215)

广东新华发行集团股份有限公司经销

广州市番禺区市桥印刷厂印刷

(地址:广州市番禺区市桥环城西路 201 号 邮编:511400)

850 毫米×1168 毫米 32 开本 3.875 印张 100 千字

2003 年 10 月第 1 版 2003 年 10 月第 1 次印刷

定价:15.00 元

如发现因印装质量问题影响阅读,请与承印厂联系调换

序

随着社会主义市场经济建设的快速发展,逐步完善中的我国社会保障体系在保障人民生活、维护社会稳定、促进经济发展等方面发挥着越来越大的作用。作为完善社会保障体系重要任务之一的社会保障信息化建设,在促进社会保障事业的健康发展,提高社会保障的服务质量、效率等方面,也正在发挥着越来越大的作用。

改革开放以来,人员流动日益频繁,社会保障对象急剧增加,建设我国统一的劳动力市场和统一的社会保障体系就成为经济发展、社会进步的必然。而实践以人为本的管理理念,建立有利于人的流动的社会保障体系,促进社会保障管理和服务的社会化,需要用新的手段来铺路搭桥。智能卡等新技术的出现,正好适应了这种公共政务信息共享和尊重个体的需求。社会保障卡的发行,使社会保障对象(参保人员)在全国范围内均可享受相应的社会保障成为可能。从长远看,社会保障卡将逐步成为社会保障服务社会化的主要手段之一。

自1999年劳动和社会保障部正式下发了《社会保障卡建设总体规划》以来,社会保障卡工程通过摸索、总结,现已进入抓落实、抓应用、抓管理的阶段。社会保障卡的应用正逐步走向有序,并向大规模应用发展。

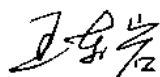
作为行业性大卡,为了保证总体规划目标的实现,劳动和社会保障部制发了一系列关于“中华人民共和国社会保障卡”的技术标准和管理规范。广东省针对社会保障

卡的发行和应用也制定了相关的标准和规范。广州市还提出了“四个统一”，即：采用统一的业务标准规范，统一的计算机技术标准规范，统一的网络互联技术标准规范，统一的社会保障卡系统标准规范。这“四个统一”的提出，为社会保障卡的顺利发行与有效应用提供了进一步的保证。

无论建设者还是使用者，对新技术的应用和推广都有一个认识过程。《广州市社会保障卡的发行与应用》一书的出版对加快这个认识过程非常有帮助。如何理解和掌握社会保障卡系统建设的相关技术和管理思想，本书作了详细的论述，这对那些准备或正在进行社会保障卡系统建设的领导和工程技术人员都有着具体的指导作用。

本书结构完整，条理清晰，内容全面，可操作性强，对各地社会保障卡的发行与应用都具有一定的参考价值。

在本书即将付梓出版之际，我希望广州市社会保障卡的发行与应用能有效地推动广州市社会保障信息系统工程建设，为我国社会保障事业信息化建设作出重要贡献。



国家劳动和社会保障部

二〇〇三年十月二日

前 言

随着我国社会主义市场经济体制的建立和逐步完善,社会劳动保障事业也随着经济的发展而迅速发展。社会保障关系到千家万户的温饱,也直接影响到社会的长治久安和繁荣昌盛。由于社会保障业务和范围的不断增长,过去的手工处理模式已远远不能满足为广州市几百万人口提供社会保障业务的需要。因此,利用计算机技术和现代通信技术,建设社会劳动保障信息管理系统已成为积极推进社会保障事业的必要措施。

利用智能 IC 卡一卡多用的优势,把各种社会劳动保障业务数据集于一卡之中,以代替现有手工填写的各种证册,也是各地正积极推行的一种新的应用手段——社会保障卡的应用。对各社会保障业务部门来说,可以凭卡鉴别持卡人的身份并方便而可靠地获取持卡人的信息资料,避免了手工输入信息造成的错误,也提高了工作效率,同时解决了各部门业务系统间由于同一信息的多次输入带来的数据标准化、信息比对与交互的问题;对参保人来说,可以持卡参加各种社会保障服务,由于卡中记录各项保险费的缴纳和保险金的领用等情况(个人账户),持卡人不仅可以随时查询到卡中个人的各项记录状况,而且还可以通过卡和网络系统,查询到有关个人的更详细的资料或有关的国家政策与法规。同时,由于卡中存放了个人保险账户(账号和保险费用余额),因此,社会保障卡还可以作为一种支付工具,用于支付持卡人的医疗费等各项费用,为参保人提供了更为简单快捷的服务。

社会保障卡在社保领域作为信息存储载体和传递媒体正被广泛认同和使用。随着全国社保制度改革的深入和各地网络建设的进展,社会保障卡将在人们生活中起到越来越重要的作用,特别是国家劳动和社会保障部有关《社会保障(个人)卡规范》和《社会保障(个人)卡安全要求》的制定发布,使社会保障卡在全国范围内通用成为了可能,并且社会保障卡将是社保服务社会化的主要手段。

本书将从社会保障卡建设的角度,以广州市为例来阐述社会保障卡的发行及应用。由于社会保障卡的发行涉及到多个环节,每个环节处理不好,都将会影响到卡的发行甚至应用,为此,第一章至第四章将侧重这方面的描述,以期读者对卡及其卡的发行过程有所了解和获得基本的解决思路或方案。然后,在第五章至第七章说明社会保障卡的各种管理系统和在各个社会保障业务系统中的应用。最后,在第八章谈了社会保障卡在建设工程实施中的一些考虑。

本书在写作过程中得到了国家劳动和社会保障部王东岩先生、广州市信息中心谢学宁先生和广州市劳动和社会保障局张秋红女士等的帮助和指导,在此一并表示衷心的感谢。

作者限于水平和条件,书中一定有不少错误或疏漏之处,敬请读者和专家指正。

胡 勇

2003年6月

目 录

第一章 IC卡简介	(1)
1.1 IC卡定义	(1)
1.2 IC卡的分类	(1)
1.3 智能IC卡的特点	(4)
1.4 智能IC卡的主要功能	(4)
1.5 智能IC卡芯片操作系统	(5)
第二章 社会保障卡系统概述	(7)
2.1 社会保障卡系统的建设目标	(8)
2.2 社会保障卡系统的建设思路	(8)
2.3 社会保障卡系统的建设原则	(9)
2.4 社会保障卡系统的功能	(10)
2.4.1 总体功能	(11)
2.4.2 具体功能	(11)
2.5 社会保障卡系统的技术性能	(12)
2.5.1 接口能力	(12)
2.5.2 性能指标	(13)
2.6 社会保障卡管理中心	(13)
2.6.1 广州市社会保障卡管理中心的功能	(14)
2.6.2 广州市社会保障卡管理中心的定位	(14)
2.6.3 广州市社会保障卡管理中心的职能	(14)
2.6.4 社会保障卡管理中心与其他部门的关系	(15)
2.6.5 社会保障卡管理中心的业务范围	(16)
2.6.6 社会保障卡管理中心的接口管理	(17)

2.7 社会保障卡系统设计的标准和规范	(18)
第三章 社会保障卡的系统架构	(19)
3.1 社会保障卡系统网络结构	(20)
3.1.1 社会保障卡管理中心局域网	(20)
3.1.2 广州市社会保障卡管理中心广域网	(21)
3.2 社会保障卡系统软件结构	(22)
第四章 社会保障卡的发行	(25)
4.1 参保人基本信息的采集	(26)
4.1.1 参保人基本信息数据库的建立	(26)
4.1.2 参保人基本信息数据库的惟一权威性	(27)
4.1.3 街镇服务中心定点数据采集	(28)
4.1.4 流动式数据采集	(29)
4.1.5 已参保人群的数据采集	(29)
4.1.6 试点工程的数据采集	(30)
4.2 社会保障卡的制作	(31)
4.2.1 社会保障卡	(31)
4.2.2 社会保障卡芯片	(32)
4.2.3 社会保障卡数据结构	(32)
4.2.4 社会保障卡制作	(40)
4.3 社会保障卡的发放	(44)
4.3.1 发卡流程	(45)
4.3.2 批量卡发放	(45)
4.3.3 零散卡发放	(46)
4.3.4 社会保障卡发卡管理	(46)
4.4 社会保障卡的其他业务	(47)
4.4.1 社会保障卡的挂失	(47)
4.4.2 社会保障卡的注销	(47)
4.4.3 社会保障卡的变更	(48)
4.4.4 社会保障卡的换领	(48)

4.4.5	社会保障卡的查询	(48)
4.4.6	社会保障卡的管理	(48)
4.5	制发卡设备与场地	(49)
4.5.1	制发卡设备	(49)
4.5.2	制发卡场地	(52)
第五章	社会保障卡管理系统	(55)
5.1	社会保障卡发行与运行维护子系统	(55)
5.1.1	社会保障卡的发行软件系统	(55)
5.1.2	社会保障卡的运行维护系统	(60)
5.2	社会保障卡安全交易与结算系统	(64)
5.2.1	社会保障卡的安全交易	(64)
5.2.2	社会保障卡的交易结算	(67)
5.2.3	社会保障卡的交易清算系统	(72)
第六章	社会保障卡的安全及管理	(77)
6.1	社会保障卡的密钥与管理	(77)
6.1.1	三级密钥	(77)
6.1.2	两级管理	(78)
6.1.3	广州市社会保障卡系统密钥	(78)
6.2	社会保障卡用户的标识与认证	(79)
6.2.1	社会保障卡用户标识	(79)
6.2.2	社会保障卡用户身分认证	(81)
6.3	社会保障卡管理中心安全与管理	(82)
6.3.1	社会保障卡管理中心安全	(82)
6.3.2	社会保障卡管理中心发卡安全管理规范	(83)
6.3.3	社会保障卡数据安全	(88)
6.3.4	社会保障卡交易安全	(88)
6.3.5	黑名单管理的相关规定	(89)
6.3.6	异地交易和脱网交易的相关规定	(90)

第七章 社会保障卡在业务系统中的应用	(91)
7.1 社会保障卡的应用与功能	(91)
7.2 社会保障卡在业务系统中的应用	(93)
7.2.1 社会保险业务系统的卡应用	(93)
7.2.2 劳动业务系统的卡应用	(94)
7.2.3 民政业务系统的卡应用	(94)
7.2.4 相关业务系统的卡应用	(94)
7.2.5 自助服务终端系统的卡应用	(94)
7.3 社会保障卡在业务系统中的应用流程	(95)
7.3.1 在社会保险业务中的应用流程	(96)
7.3.2 在劳动业务中的应用流程	(102)
7.3.3 在民政业务中的应用流程	(104)
第八章 工程实施中的考虑	(107)
8.1 工程实施步骤安排	(107)
8.2 实施措施和保障条件	(109)
8.3 运营模式的考虑	(111)
参考文献	(114)

第一章

IC 卡简介

根据国家劳动和社会保障部有关《社会保障(个人)卡规范》和《社会保障(个人)卡安全要求》,社会保障卡将采用 CPU 接触式 IC 卡。为此,本章将先对 IC 卡进行介绍。

1.1 IC 卡定义

IC 卡是集成电路卡(Integrated Circuit Card)的简称,是镶嵌集成电路芯片的塑料卡片,其外形和尺寸都遵循国际标准(ISO)。芯片一般采用不易挥发的存储器(ROM、EEPROM)、保护逻辑电路、甚至带微处理器 CPU。带有 CPU 的 IC 卡才是真正的智能卡。

1.2 IC 卡的分类

按照嵌入集成电路芯片的形式和芯片类型的不同大致可将 IC 卡按图 1.1 所示分类。

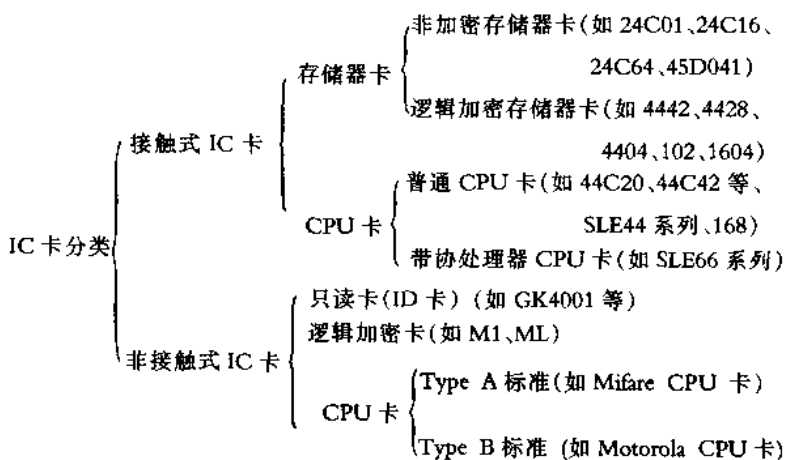


图 1.1 IC 卡的分类

以下对各种 IC 卡作一简单的描述:

1. 非接触式 IC 卡

非接触式 IC 卡是通过无线电波或电磁场感应的方式将卡的集成电路内的数据与外部接口设备通信的 IC 卡。

非接触式 IC 卡不是国家劳动和社会保障部社会保障卡标准规范中指定的 IC 卡。

2. 接触式 IC 卡

接触式 IC 卡是指在使用时,通过有形的电极触点将卡的集成电路与外部接口设备直接接触连接,进行数据交换的 IC 卡。

在接触式 IC 卡中有存储器卡和 CPU 卡两种。而存储器卡又可分为非加密存储器卡和逻辑加密存储器卡;CPU 卡则又可分为普通 CPU 卡和带协处理器 CPU 卡。

非加密存储器卡:卡内的集成电路芯片主要是 EEPROM,具

有数据存储功能,不具有数据处理功能和硬件加密功能。

逻辑加密存储器卡:在非加密存储器卡的基础上增加了加密逻辑电路,加密逻辑电路通过校验密码方式来保护卡内的数据对于外部访问是否开放,但只是低层次的安全保护,无法防范恶意的攻击。

普通 CPU 卡:也称智能 IC 卡,卡内的集成电路中带有微处理器(CPU)、存储单元(包括随机存储器 RAM、程序存储器 ROM(FLASH)、用户数据存储器 EEPROM)、输入/输出接口单元以及芯片操作系统(Chip Operation System 简记为 COS)。装有 COS 的 CPU 卡相当于一台微型计算机,不仅具有数据存储功能,同时具有命令处理和数据安全保护等功能。

带协处理器 CPU 卡:也称带协处理器的智能 IC 卡,它是在普通 CPU 卡的基础上增加了协处理器,以提高卡的运算和处理能力。

图 1.2 为存储器卡和 CPU 卡的内部结构示意图:

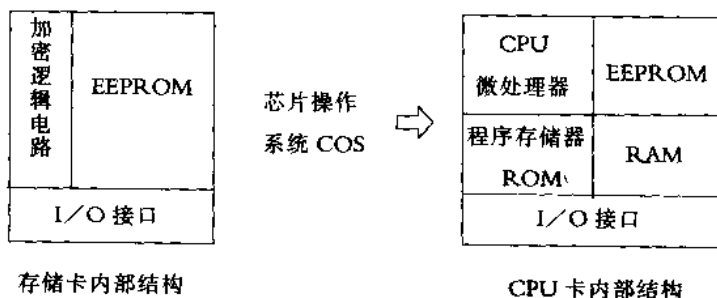


图 1.2 存储器卡和 CPU 卡的内部结构示意图

存储器卡属于一种被动型的,其数据输入/输出通信一般采用同步方式的 IC 卡。CPU 卡则属于主动型,它不仅能够管理各种输入/输出的数据,校验来自接口设备输入的个人密码(PIN);而且能够根据应用系统的要求主动识别与之连接的接口设备。因

此,在 CPU 卡中,能够建立多种应用系统的授权,存放多个应用系统的相关数据,并实现对数据信息存取的高可靠性、高安全性控制,可以进行复杂的信息处理和计算。

1.3 智能 IC 卡的特点

相对于存储器卡,智能 IC 卡具有如下特点:

- 1) 芯片和 COS 的安全技术为智能 IC 卡提供了双重的安全保证。
- 2) 自带操作系统的智能 IC 卡对计算机网络系统要求较低,可实现脱网操作;而存储器卡则必须在完善的网络环境下使用。
- 3) 可实现真正意义上的一卡多应用,每个应用之间相互独立,可受控于各自的密钥管理系统。
- 4) 存储容量大,可提供 1K~64K 字节的数据存储间。
- 5) 使用寿命长,数据存储时间可达 10 年以上。

1.4 智能 IC 卡的主要功能

智能 IC 卡主要有如下功能:

(1) 身份认证

对持卡人、卡终端和卡片三方的合法身份做认证。

(2) 支付和结算工具

小额的电子钱包和电子存折的支付手段,可避免携带现金和找零的不便,提高交易效率。

(3) 安全保密模块

使用相应的密钥实现加密、解密以及交易处理,从而完成与用户卡之间的安全认证。

(4)数据载体

智能 IC 卡可做为个人档案或重要数据的安全载体,数据可至少保存 10 年以上。

1.5 智能 IC 卡芯片操作系统

智能 IC 卡的核心是芯片操作系统(Chip Operation System),它是一个比较小而又非常完整严密的系统。这个系统管理着卡片的一举一动,外界对卡发布的所有命令都需要通过操作系统才能对智能 IC 卡起作用。COS 的主要功能是控制智能 IC 卡和外界的信息交换、管理智能 IC 卡内的存储器并在卡内部完成各种命令的处理。

值得注意的是,接触式智能 IC 卡在各应用系统中是否通用,主要是看其操作系统(COS)。社会保障卡虽然有国家劳动和社会保障部的标准规范,但若采用了不同的 COS,要使社会保障卡在全国范围内通用,甚至在本地区内通用是不可能的。为此,国家劳动和社会保障部专门对各厂家的芯片和 COS 进行检测。目前通过劳动和社会保障部检测并发了证书的厂家或公司有 24 家共 28 个 COS,例如中国华大集成电路设计中心、珠海惠泽信息系统有限公司、深圳市明华澳汉科技有限公司、珠海东信和平智能卡股份有限公司、清华同方股份有限公司、北京捷德智能卡系统有限公司等。由于不同的 COS,其初始化和发卡程序都不一样,所以,为了方便社会保障卡的制卡、发行和管理,建议各地在建设社会保障卡时,应当选用一家类似上述公司或厂家的通过国家劳动和社会保障部检测的 COS。另外,为了确保在全国范围内的通用,国

家劳动和社会保障部除了对 COS 进行检测外,还开展了通用性测试,即对各地完成了初始化和个人化(可以模拟)的实发样卡进行测试,只有通过通用性测试的社会保障卡,才能在该城市正式发行。

由于智能 IC 卡的上述特性,我国把智能 IC 卡作为金卡工程的主流,国家劳动和社会保障部也在《社会保障卡(个人)规范》中建议采用 8K 或以上字节的 CPU 接触式集成电路卡。

社会保障卡包括社会保障个人卡和社会保障单位卡,本书将以广州市社会保障卡的建设为例进行阐述。根据广州市社会保障信息系统的总体规划,社会保障单位卡将统一采用国家质量技术监督局发行的组织机构信息卡,其在广州市社会保障信息系统中的应用、相关制度、标准和应用规范将结合组织机构信息卡的相关规定制定和执行,因此本书只涉及面向社会保障对象的个人卡的发行及应用。

为了叙述方便,本书对各种社会保障(广义)的管理、服务对象统一简称为“参保人”。