附件

社会保障卡加载金融功能总体方案

为推动社会保障卡加载金融功能工作，规范具有金融功能的社会保障卡的发行和管理，促进具有金融功能的社会保卡的应用，编制本方案。

本方案确定了具有金融功能的社会保障卡的技术实现方式、应用领域和发行管理模式。各地人力资源社会保障部门（以下简称人社部门）联合商业银行等相关单位，按照人力资源社会保障部和人民银行的总体部署，在本方案确定的框架内，开展社会保障卡加载金融功能工作。

一、技术实现方式

具有金融功能的社会保障卡采用单一芯片接触式CPU卡，社保应用与金融应用共置于同一个芯片之中，应用分设，密钥管理体系相互独立，支持各自功能的实现。

（一）卡片技术实现

1.芯片。依据社保应用和金融应用需求，芯片存储介质采用高可靠性的EEPROM，具有接触式接口，支持《社会保障（个人）卡规范》和《中国金融集成电路（IC）卡规范》（JR/T 0025—2010）定义的加密算法。

2.卡片操作系统（COS）。采用单COS双应用的架构，采用硬掩膜技术，同时支持社保应用和金融应用。通过COS内部防火墙机制，确保社保应用和金融应用从安全、文件系统、命令等各方面进行独立管理，互不影响。

3.文件结构。卡片建立社保应用系统环境（SSSE）和金融支付系统环境（PSE）。社保、金融的数据文件和密钥文件分别建立在各自环境下。终端通过选择SSSE进入社保应用系统环境，选择PSE进入金融支付系统环境，此后依据《社会保障（个人）卡规范》和《中国金融集成电路（IC）卡规范》（JR/T 0025—2010）定义的交易流程对卡片进行操作。

4.卡片架构。本方案定义的卡片采用单一芯片，通过硬件驱动层支持卡片操作系统（COS）。卡片COS同时支持社保应用和金融应用，两种应用分别具有独立的命令管理模块、文件管理模块和安全管理模块，通过防火墙机制相互独立，互不影响。卡片架构图见附图1。

（二）读写终端技术实现

读写终端可采用POS、PC+Reader、ATM等方式，从功能上分为社保业务功能终端、金融业务功能终端和全业务功能终端三种模式。

1.社保业务功能终端。与现行社会保障卡受理终端采用相同的技术要求，即配有显示器、IC卡接口设备、键盘、密码键盘、安全存取模块、存储设备等硬件设备，具备读取社保应用环境、应用初始化、有效性检查、联机处理等功能。可受理未加载金融功能的社会保障卡，以及具有金融功能的社会保障卡中的社保应用。

2.金融业务功能终端。符合《银行卡销售点（POS）终端规范》（JR/T 0001—2009）、《银行卡自动柜员机（ATM）终端规范》（JR/T 0002—2009）等技术标准，与现行符合《中国金融集成电路（IC）卡规范》（JR/T 0025—2010）的金融IC卡受理终端采用相同的技术要求。可受理金融IC卡，以及具有金融功能的社会保障卡中的金融应用。

3.全业务功能终端。同时符合以上两种技术要求和功能要求。

（三）应用系统技术实现

人社部门应按照人力资源社会保障部相关要求，建立社会保障卡管理系统，形成个人基础信息库，实现对社会保障卡的制卡、密钥、应用、黑名单等的规范管理，并与相关业务系统相衔接，保证社会保障卡在人力资源和社会保障各业务领域的有效应用。

商业银行应建立基于借记卡的IC卡发卡、密钥管理、授权和清算等系统，或对相关系统做出适当改造，确保社会保障卡金融功能的有效应用。中国银联应做好金融IC卡相关系统和受理环境改造，确保社会保障卡金融功能跨行转接与清算顺利进行。

（四）安全体系技术实现

具有金融功能的社会保障卡设置卡片主控密钥。卡片主控密钥用于创建SSSE和PSE，并装载上述两个系统环境的环境主控密钥。在完成上述系统环境创建和主控密钥装载后，卡片主控密钥对各应用环境不再拥有控制权，而转由各自的环境主控密钥控制。其中，社保环境主控密钥用于创建SSSE目录下的文件，装载社保应用密钥。金融环境主控密钥用于创建PSE目录下的文件，装载金融应用密钥。环境主控密钥不受卡片主控密钥控制，可以自主更新。

具有金融功能的社会保障卡中，社保应用与金融应用在各自的应用环境中，分别遵循《社会保障（个人）卡规范》和《中国金融集成电路（IC）卡规范》（JR/T 0025—2010）定义的安全机制。

同时支持社保应用和金融应用的全业务功能终端中，用以存储密钥等敏感信息的安全存取模块（PSAM卡）只应用于社保应用，需满足《社会保障（个人）卡规范》要求。

二、应用领域

具有金融功能的社会保障卡不仅可以支持身份凭证、信息查询、医疗费用结算等不需要金融功能支持的社保应用（以下简称与金融功能无关的社保应用），也可以支持社会保险费缴纳、待遇领取等需要金融功能支持的社保应用（以下简称基于金融功能的社保应用），同时也支持金融应用（人民币借记应用）。

（一）与金融功能无关的社保应用

与金融功能无关的社保应用主要包括三个方面：

1.身份凭证。作为享受公共就业服务、就业扶持政策，和参保登记、缴费申报、社会保险关系转移接续、医疗费用报销、待遇领取资格认证等业务办理的身份凭证。

2.信息查询。以社会保障卡为入口，持卡人可以登录网站及在触摸屏上查询相关信息，还可以在网上办理有关人力资源社会保障事务。

3.医疗费用结算。凭卡实现在本统筹地区及跨统筹地区医疗费用即时结算。

（二）基于金融功能的社保应用

社会保障卡加载金融功能后，各地人社部门要积极推动其在社会保险费缴纳、待遇领取等业务环节的应用，逐步将涉及个人缴费、支付的各项业务，集成到社会保障卡加载的银行账户之中办理，实现集约化管理和服务。具体包括：

1.社会保险费缴纳。包括灵活就业人员、城镇参保居民、农村参保人员社会保险费的缴纳和银行代扣等。

2.待遇领取。包括养老金、失业保险金、工伤保险定期待遇、各项社会保险一次性待遇，医疗费用等的报销返还，以及面向个人的各类就业扶持政策补贴等的领取。

3.医疗费用即时结算后的费用支付（包括个人自付部分结算时个人账户不足额时的费用结算、个人自费部分结算）。

各地可在上述应用基础上，借助社会保障卡加载的金融功能，探索开展其他便民服务。

（三）金融应用

具有金融功能的社会保障卡作为具有特殊性质的银行卡，其金融功能做如下限制和定制：

1.只限境内使用。具有金融功能的社会保障卡具有政府服务功能，使用范围暂时限定在中华人民共和国境内。

2.暂支持借记应用。社会保障卡加载的金融功能暂限定为人民币借记应用。

3.支持专有的金融增值服务。合作银行可与商户协商推出基于具有金融功能的社会保障卡的增值服务功能，如持卡人在药店、医疗机构等和社保应用有关的商户消费时，持卡可享受特别优惠，或者具备商户积分功能。

4.优惠措施。由于具有金融功能的社会保障卡所具备的公益性和政府服务的职能，人社部门可与合作银行协商，给予持卡人一定的优惠。

（四）应用实现方式

与金融功能无关的社保应用依靠社会保障卡信息记录、信息查询、业务办理等基本功能实现；基于金融功能的社保应用以社会保障卡为基础，依靠加载的金融功能，通过商业银行提供金融服务来实现；金融应用依靠社会保障卡加载的金融功能，通过商业银行提供金融服务来实现。

人社部门应建立支持上述应用的信息系统，并通过网络互联、信息交换等方式，实现与银行业务系统的衔接。

具体实现方式见附图2。

三、应用管理

具有金融功能的社会保障卡具体应用过程中，人社部门与合作银行应建立管理沟通机制，促进服务体系的衔接，为持卡人提供便捷、高效、安全的联动服务。合作银行应制定具有金融功能的社会保障卡银行业务应用管理规定，加强关键环节管控。

为保证卡的唯一性，首次发放、补卡和换卡须由人社部门发起。

（一）首次（初次）发放：人社部门对参保人资料进行审核，审核通过后生成社保应用个人化数据，并将个人资料信息批量发送给合作银行，合作银行按照《中华人民共和国反洗钱法》（中华人民共和国主席令第56号）、《个人存款账户实名制规定》（中华人民共和国国务院令第285号）等法规制度要求对客户资料进行审核，审核通过后生成金融应用个人化数据。按照商定的方式完成卡片制作与个人化后，个人化机构将成品卡传递到人社部门，人社部门将卡发放给持卡人。合作银行应按照人民银行有关批量办卡的规定，要求持卡人持个人身份证原件到柜台办理金融功能的激活手续。

（二）挂失：挂失分为口头挂失和书面挂失。口头挂失可采用电话等多种渠道。口头挂失后持卡人需要办理正式书面挂失手续。书面挂失可采用两种方式，第一种是分别在人社部门服务网点和合作银行服务网点挂失；第二种是在人社部门服务网点和合作银行任意一方挂失，人社部门和合作银行应采取措施保证挂失信息同步。书面挂失应以第一种方式为主，待各项条件成熟后，各地可逐步研究第二种方式的应用。

（三）解挂：解除挂失有两种方式，一种是分别到人社部门服务网点和合作银行网点办理解除挂失手续；第二种是到人社部门或合作银行任意一方办理解除挂失手续，人社部门和合作银行应采取措施保证解除挂失信息同步。解除挂失应以第一种方式为主，待各项条件成熟后，各地可逐步研究第二种方式的应用。

（四）补卡：书面挂失后，持卡人应在规定的时间内到人社部门申请挂失补卡，流程与首次发放一致。在补卡的过程中，人社部门可向持卡人提供适当方式进行社保业务办理。

（五）换卡：应用到期或卡损坏后，持卡人可申请换卡，流程与首次发放一致。在换卡的过程中，人社部门可向持卡人提供适当方式进行社保业务办理。

（六）销卡：销卡分两步完成。持卡人先到人社部门完成社保应用的注销，凭人社部门开具的清户通知书再到合作银行完成金融应用的注销。合作银行将卡回收，完成整个销卡处理流程。人社部门和合作银行应采取措施保证销卡信息同步。

（七）销毁：销毁分为两种模式，一种为合作银行销毁，合作银行将注销的卡片粉碎销毁；另一种为人社部门销毁，合作银行将已回收卡片送往人社部门，由人社部门粉碎销毁。无论采用何种销毁方式，人社部门和合作银行均应采取措施保证销毁信息共享。

（八）密钥管理：人社部门按照人力资源社会保障部关于社会保障卡密钥管理的有关要求，管理卡中的社保应用密钥；合作银行按照人民银行关于金融IC卡密钥管理的有关要求，管理卡中的金融应用密钥。

四、产品选择

各地发行具有金融功能的社会保障卡，所采用的产品应符合《“中华人民共和国社会保障卡”管理办法》（人社部发〔2011〕47号）以及人民银行关于金融IC卡的有关规定。相关要求如下：

（一）芯片选择

具有金融功能的社会保障卡芯片应符合《“中华人民共和国社会保障卡”管理办法》（人社部发〔2011〕47号）的相关要求，同时获得人力资源社会保障部和人民银行的认可。

（二）卡片选择

具有金融功能的社会保障卡卡片和卡内操作系统（COS）需经过人力资源社会保障部与人民银行认可的检测机构检测。

（三）读写终端选择

受理具有金融功能的社会保障卡的社保业务功能终端应经过人力资源社会保障部认可的检测机构检测；金融业务功能终端应经过人民银行认可的检测机构检测；全业务功能终端应经过人力资源社会保障部与人民银行认可的检测机构检测。

（四）卡片供应商选择

具有金融功能的社会保障卡制作应选择满足人力资源社会保障部和人民银行相关要求，并获得人力资源社会保障部和人民银行认可的卡片供应商完成。

（五）第三方个人化机构选择

如采用集中个人化模式，承担具有金融功能的社会保障卡个人化的第三方机构须同时符合人力资源社会保障部和人民银行相关资质要求，获得人力资源社会保障部和人民银行的认可；如采用分步个人化模式，第三方机构须符合人力资源社会保障部关于社会保障卡个人化的相关要求，或人民银行关于金融IC卡个人化的相关要求。

五、卡片制作与个人化模式

具有金融功能的社会保障卡卡内文件结构划分、控制密钥加载、卡面印刷、个性化信息写入等卡片制作（以下简称个人化）工作，可采用社保应用与金融应用统一进行个人化的工作模式（即集中个人化模式），也可采用社保应用与金融应用分别进行个人化的工作模式（即分步个人化模式）。具体方式由发卡地区人社部门商合作银行共同确定，但应优先选择集中个人化模式。

（一）集中个人化模式

集中个人化模式由同一组织或机构一次性完成社保、金融两部分应用的个人化。集中个人化模式的个人化机构可以是地方人社部门、合作银行，也可以是双方认可的第三方个人化机构。该第三方机构需要具备本方案第四部分所提出的各类管理要求。

集中个人化模式具体过程如下：

1.数据写入。社保应用与金融应用分别准备各自的业务数据，按照各自的规则分别生成发卡数据文件，传到个人化机构的数据准备系统，经校验、比对、整合后，建立数据关联关系，经个人化系统一并写入卡中，并进行卡面个人化。

2.密钥写入。社保密钥与金融密钥分别由各方提供的密钥管理系统进行管理。在个人化时，两个应用的各类密钥（包括各自的主控密钥KMC）通过个人化机构密钥管理系统提供的密钥服务，经个人化系统一并写入卡中。

（二）分步个人化模式

分步个人化模式由不同组织或机构分步完成社保、金融两部分应用的个人化。其中，社保应用个人化机构可以是地方人社部门或地方人社部门认可的第三方个人化机构；金融应用个人化机构可以是合作银行或合作银行认可的第三方个人化机构。

分步个人化模式具体过程如下：

1.个人化过程。先由一方的个人化机构完成相关应用的个人化，再交由另一方的个人化机构完成另一应用的个人化。双方的个人化均按照各自个人化规则进行。各方在完成个人化后均需生成包括个人化反馈数据在内的个人化相关数据文件。后进行个人化的一方，生成的个人化相关数据文件中还应包括卡片邮寄数据、卡片包装数据等发卡数据，供卡的发放使用。

2.两次个人化的关联。两次个人化的关联关系可以通过两种方式建立。

方式一：通过卡片内存储的个人信息进行关联。第二次个人化时读取第一次个人化写入卡片的个人信息，查询个人化数据，建立关联关系，完成第二次个人化。

方式二：通过第一次个人化产生的反馈数据进行关联。第一次个人化后产生个人化反馈数据，第二次个人化通过反馈数据和个人化数据建立关联关系，完成第二次个人化。

（三）数据准备与数据匹配

采用上述两种个人化模式皆应针对社保应用和金融应用，分别做好数据准备工作，并对两项应用中的数据进行匹配。

1.数据准备。社保数据准备应依据人力资源社会保障部批准的卡内文件结构进行，具体数据文件的格式，由个人化机构与发卡地区人社部门事先约定。金融数据准备的要求，参照《中国金融集成电路（IC）卡规范》（JR/T0025-2010）执行。

2.数据匹配。已完成各自单独应用数据准备工作的社保应用、金融应用两部分个人化数据，应按照一定规则进行匹配。数据匹配必须采用双方数据文件中共有的数据项作为唯一的匹配标识，且该数据项本身具有唯一性（如社会保障号码）。完成匹配的数据文件格式，由个人化机构与发卡地区人社部门、合作银行共同确定。

防火墙

**社保应用**

命令管理模块

文件管理模块

安全管理模块

命令管理模块

文件管理模块

安全管理模块

**金融应用**

硬件驱动层（通讯、运算、存储器访问）

芯片

**附图1 具有金融功能的社会保障卡卡片架构**

**附图2 具有金融功能的社会保障卡应用实现架构**

基于金融功能的

社保应用：

养老金领取

社会保险费缴纳

医疗费用个人自

费部分结算等…

**人力资源社会保障应用系统**

与金融功能无关的

社保应用：

参保登记

待遇查询

医疗费用即时结

算等…

信息记录、信息查询、业务办理等社会保障卡基本功能

消费、转账、结算、存取现金等金融功能

**具有金融功能的社会保障卡**

金融应用：

现金存取

余额查询

转账汇款

持卡消费等…

**银行应用系统**