社会保障卡加载金融功能全业务功能终端规范

1 引言

本规范对具有金融功能的社会保障卡全业务功能终端的功能、部件、安全等提出要求和规定。

2 适用范围

本规范适用于人力资源和社会保障领域面向社会公众发行的具有金融功能的社会保障卡的全业务功能终端。其使用对象主要是与具有金融功能的社会保障卡应用相关的终端设计、制造和受理以及应用系统的研制、开发、集成和维护等组织机构。

3 参考标准

GB/T 16649．3—2006	识别卡　带触点的集成电路卡　第 3 部分：电信号和传输协议（ISO/IEC 7816-3：1997）
ISO/IEC 7816-3：2006	识别卡　带触点的集成电路卡　第 3 部分：电信号和传输协议
JR/T 0025-2010	中国金融集成电路（IC）卡规范
LB002-2000	社会保障（个人）卡规范

4 定义

以下定义适用于本规范。

4.1 社保应用（Human Resources and Social Security Application）

即人力资源社会保障应用，是在人力资源和社会保障各专业领域管理和服务工作中的社会保障卡应用总称。

4.2 接口设备（Interface Device）

终端上插入 IC 卡的部分，包括其中的机械、电气和逻辑控制部分。

4.3 终端（Terminal）

为进行业务处理而在服务网点安装的设备，用于同 IC 卡的连接。它包括接口设备，也可包括其他部件和接口。

4.4 命令（Command）

终端向 IC 卡发出的一条信息，该信息启动一个操作或请求一个应答。

4.5 响应（Response）

IC 卡处理完成收到的命令报文后，回送给终端的报文。

4.6 交易（Transaction）

持卡者和业务、管理部门之间根据 IC 卡所支持的应用接受、提供服务的行为。

4.7 功能（Function）

由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。

4.8 集成电路（Integrated Circuit，IC）

设计用于完成处理和/或存储功能的电子器件。

4.9 集成电路卡（IC 卡）（Integrated Circuit（s） Card）

内部封装一个或多个集成电路的 ID-1 型卡。

4.10 ICC 连接器（ICC Connector）

ICC 连接器是 IFD 与 ICC 电气连接的物理实现部分。在逻辑上，本规范规定用它来标识与它电气上稳定连接的 ICC。

4.11 报文（Message）

由终端向卡或卡向终端发出的，不含传输控制字符的字节串。

4.12 明文（Plain Text）

没有加密的信息。

4.13 密钥（Key）

控制加密转换操作的符号序列。

4.14 认证中心（Certification Authority）

证明公钥和其它相关信息同其拥有者相关联的可信的第三方机构。

4.15 公钥 （Public Key）

在一个实体使用的非对称密钥对中可以公开的密钥。在数字签名方案中，公钥用于验证。

5 缩略语和符号表示

AID	应用标识符（Application Identifier）
IC	集成电路（Integrated Circuit）
ICC	集成电路卡（Integrated Circuit Card）
PIN	个人密码（Personal Identification Number）
SAM	安全存取模块（Secure Access Module）

6 全业务功能终端的要求

可以受理未加载金融功能的社会保障卡、普通的金融 IC 卡、以及具有金融功能的社会保障卡中的社保应用和金融应用的全业务功能终端应同时符合《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）要求。

6.1 功能部件配置要求

全业务功能终端应满足表 1 给出的最低功能部件配置要求。其中的显示器、IC 卡接口设备、键盘、密码键盘、打印机、存储设备、磁条阅读器等部件既可以直接集成在终端上，也可以以独立设备的形式通过电缆与终端主体部分相连。

表 1　终端的最低功能部件配置要求

终端部件	配置要求
显示器	必备型（Mandatory）
IC 卡接口设备	必备型（Mandatory）
键盘	必备型（Mandatory）
密码键盘	必备型（Mandatory）
安全存取模块	必备型（Mandatory）
打印机	必备型（Mandatory）
网络通信接口	可选型（Optional）
存储设备	必备型（Mandatory）
实时时钟	必备型（Mandatory）
汉字扩展字符集	必备型（Mandatory）
电源	必备型（Mandatory）
磁条阅读器	必备型（Mandatory）

6.2　功能部件的特性

6.2.1　显示器

用于交易过程显示及错误指示。本规范要求显示器具有显示汉字、字母、数字和符号的能力。

6.2.2　IC 卡接口设备

终端应提供用来与 IC 卡进行命令数据传递通讯的 IC 卡读卡器，该读卡器应至少配置两个 ICC 连接器，其中一个用来连接用户 IC 卡，另一个用来连接安全存取模块。该读卡器模块包括机械、电气和逻辑协议等部分。

建议终端的用户卡 IC 卡读卡器插槽附近有一明显标记指示如何插入 IC 卡。如果终端有锁卡或吞卡功能，则应保证在掉电、设备异常或交易取消时能释放或退出卡。

6.2.3　键盘

终端应带有用于输入交易数据、选择命令和执行功能的键盘。支持应用所需的数字键、字母键、命令键和功能键。

6.2.4　密码键盘

终端应提供输入个人识别码（PIN）验证的密码键盘，允许持卡人输入 4－12 位的 PIN。可以是与终端键盘集成在一起的内置式密码键盘，也可以是与终端通过通讯线连接的外置式密码键盘。密码键盘的设计应当符合应用的要求。

6.2.5　安全存取模块

用于对终端操作社会保障卡的权限鉴别，包括权限控制密钥的存储、鉴别数据的计算等功能。

6.2.6　打印机

终端应配置有能打印银行卡交易单据的打印机，可以是针式或热敏打印机。对每笔批准的银行卡交易，不论是脱机或联机都能打印出交易单据。

打印单据格式由各关联收单银行自定，但应包含如下数据：卡号、应用标识符 AID、交易日期时间、签名栏。

终端还可根据社保应用的需要配置相应的打印机，本规范对其特性不作规定。

6.2.7 网络通信接口

终端应当配置有与后台通信的模块。用于联机交易或终端与后台之间的数据传输，及下载管理。具有联机交易功能的终端，其通信模块与后台的通信速度应能满足实时传送 IC 卡交易数据的要求。

6.2.8 存储设备

用于存储交易记录、黑名单、特殊的业务数据和（或）扩展中文字符集等信息。建议根据其用途为终端配备有足够存储容量的存储设备。

6.2.9 实时时钟

用于提供业务处理所需的终端时间和日期。

6.2.10 扩展中文字符集

用于持卡人姓名中 GBK 字符集之外的汉字字符处理。它可以以存储设备中的软件形式存在，也可以是专用的硬件部件。

6.2.11 电源

电池供电终端应保证可连续工作 4 小时，待机时间不小于 24 小时。

市电供电终端的工作电压为 220V，允差±10％。

6.2.12 磁条阅读器

磁条阅读器应能够准确阅读在磁性标准正常范围内的磁道信息，并可同时读取磁条卡二、三磁道数据。可选支持读取一、二或一、二、三磁道的卡片，并处理相应的磁卡交易。

6.3 下载管理

终端应能提供对应用程序、密钥和参数等数据的下载，更新和删除。下载的通讯端口可以是串行通讯口（RS232、RS485）、Modem 通讯口、USB 口、红外、GPRS、CDMA 和 TCP/IP 网络端口或其它类型的通讯端口等中的一种或几种。下载方式也可为本地下载或远程下载等方式。

终端应保证下载控制的安全。只有经过授权或认可的一方才能向终端下载数据，未经授权，不得更改终端中的内容。终端还应能够确认下载数据的安全，能验证终端下载程序的完整性和正确性，确保敏感关键的密钥数据在下载过程中不会泄漏。

6.4 终端安全

6.4.1 终端数据安全要求

本节规定了终端数据存储、处理的一般性安全要求，同时也对安全存取模块提出了具体的要求。如何实现这些安全要求则超出了本规范的范围。

6.4.1.1 一般要求

终端一般存在两种类型的数据：

——通用数据：包括时间、终端识别号、终端交易记录等。外界可以对这些数据进行访问，但不允许进行无授权修改。

——敏感数据：包括应用密钥、认证中心公钥、用于 PIN 加密的对称密钥及终端或应用程序内部的参数。在未授权的情况下，外界不允许对这类数据进行访问和修改。

6.4.1.1.1 通用数据的安全要求

通用数据一般存放在存储器中。在更新参数以及下载新的应用程序时，终端必须做到：

——验证更新方的身份，对于应用程序重新下载，只允许终端制造厂商、终端所有者或者经终端所有者或代理方批准的第三方执行；

——校验下载参数及应用程序的完整性。

对存储器要求必须做到：无论在什么情况下，终端的应用数据都不会随意改变或丢失，并保证数据有效。

所有与交易相关的数据均应以记录形式存储于终端存储器中。终端须保证这些数据的完整性。

6.4.1.1.2 敏感数据的安全要求

敏感数据一般应存放在终端安全存取模块中。

安全存取模块是一种能够提供必要的安全机制，以防止外界对终端所储存或处理的数据进行非法攻击的硬件加密模块。

此模块主要负责保存和处理所有的敏感数据，这些数据包括各种密钥及其他与数据安全有关的敏感信息。此外该模块还应提供必须的加密功能。用于社保应用的安全存取模块为PSAM 卡，用于金融应用的安全存取模块的具体物理形式在本规范中将不做具体要求。

在正常的操作环境下，安全存取模块必须要求：出入模块的、以及其内部存放的和正在处理的数据不会由于模块自身或其接口造成任何泄露和改变。

6.4.1.2 安全存取模块的物理安全要求

安全存取模块的硬件设计必须能保证在物理上限制对其内部存贮的敏感数据的存取与窃取，以及对安全存取模块的非授权使用和修改。一旦安全存取模块受到非法的篡改和攻击，其自身必须能够立即完成对内部敏感数据的删除。要实现这些目标，安全存取模块应具有防窃、查窃、窃取显示或窃取响应机制。

同时，安全存取模块也必须具有足够的防范特性，能够发现是否被篡改过。

安全存取模块的设计和构造必须满足以下要求：

——只有通过专门的技术及工具或严重破坏的方法，才能对模块的软硬件进行增加、替换或修改。

——任何对敏感数据的访问和修改，只能通过对安全存取模块的有效物理接触才能实现。

——安全存取模块的任何部分的损坏或失效都不能导致敏感数据的泄露。

——如果安全存取模块是由多个分离部件组合而成，而处理的数据又必须在这些部件之间传递，那么各部件须保持相同的安全级别。

6.4.1.3 安全存取模块的逻辑安全要求

一个安全存取模块的逻辑设计应保证，调用任何单一功能或组合功能，都不会导致敏感数据的泄露。对于某些敏感操作，必须有一定的权限限制。

安全存取模块中可存放多组不同版本的主密钥和多组认证中心公钥及其相关信息。所有的主密钥和认证中心公钥通常必须在终端投入使用之前，被导入到安全存取模块中。如果在终端使用过程中，主密钥和认证中心公钥需要修改，必须使用安全报文。实现该操作通常必须在特殊的授权情况下完成，对外部不能存在任何取得存放在安全存取模块中密钥的机会。

为避免伪操作，存放在安全存取模块中的任何类型的主密钥必须与某个特定的操作相结合，而不适用于其他操作。

对于需要报文鉴别码的交易，安全存取模块应能够生成并传递符合具有金融功能的社会

保障卡安全规范要求的报文鉴别码。

在每次交易结束或超时状态下，安全存取模块应自动清除内部缓存区中存放的数据。

安全存取模块必须能够实现具有金融功能的社会保障卡安全规范所规定的各种加解密算法和主密钥到子密钥的分散算法，以及用于从密码键盘到终端的用户 PIN 加密以及脱机数据认证。

6.4.2 终端设备安全要求

6.4.2.1 防入侵设备

防入侵设备必须保证在其正常运行环境中，设备及其接口不会泄露或改变任何输入到设备、从设备中输出、存储在设备中以及在设备中处理的敏感数据。

当防入侵设备在安全的受控环境中运行时，则对该设备的防入侵特性要求可以降低，因为受控环境和对设备的管理提供了对设备的保护。

6.4.2.1.1 物理安全性

防入侵设备必须被设计为限制对其内部存储的敏感数据的物理访问，阻止数据被窃取，防止未经授权的使用或者修改。这些目标总体上要求将对入侵的抵御、对入侵的检测、对入侵的指示或反应机制结合起来，如可视或有声的报警。

处于非运行状态的防入侵设备，不允许包含在之前任何交易中使用过的加密密钥或者其它的敏感数据（例如 PIN），但可以包含用于提高防入侵能力的认证信息。

如果能够在该设备和存储在其中的密钥重新投入使用前监测到入侵，那么即使被非法入侵也不会影响安全。

如果设备被设计为允许内部访问，那么在进入内部区域时，敏感数据应被立即擦除。

设备的防入侵能力取决于针对物理安全的攻击的监测，因此，这种设备必须被设计为具有足够的防入侵特性，使得任何入侵对于持卡人都应该是可见的或者能被商户或收单行监测到。

设备必须被设计和构造为：

——不允许轻易入侵设备，并对设备的软硬件进行增加、替换或修改；如果在没有特别的技巧和专门的装备，并且不对设备造成严重的、显而易见的破坏的前提下，不允许测定或修改任何敏感数据，以及重新安装设备；

——只有真正进入设备内部，才能做到对输入的，存储的或正在处理的敏感数据进行未经授权的访问或修改。

——不允许采用通用的包装材料，以防止使用一般都具备的材料生产“看上去一样”的假冒复制品。

——当设备的任何部件发生任何故障时，不会导致秘密或敏感的数据的泄露。

——如果设备的设计需要部分部件在物理上分离，并且处理的数据或持卡人的指令在这些分离的部件之间传递，那么对设备的所有部件的保护等级应该是相同的。

——对交换敏感数据如明文 PIN 来说，将不同的部件整合在单一的防入侵的外壳中是必要的条件。

6.4.2.1.2 逻辑安全性

防入侵设备必须被设计为没有单一的功能或功能组合能够导致敏感数据的泄露；除了在终端中实现的安全机制明确允许的以外，不会被额外指令或任何指令组合轻易攻破；即使在

使用合法功能的情况下，也必须有足够的逻辑保护使其不会危及敏感数据的安全，这个要求可以通过内部的统计监控或控制对敏感功能调用的最小时间间隔来实现。

如果终端可以被置于一种“敏感状态”，即进入到通常情况下不被允许的敏感功能（例如，人工安装密钥），这样的转换必须在两个或两个以上可信赖的人员的协助下进行。如果用密码或其它明文数据来控制转换到敏感状态，那么这些密码的输入也要用和其它敏感数据一样的方式来保护。

为了将由未经授权的对敏感功能的使用所导致的风险降至最低，对敏感服务必须有调用次数（适当的）的限制和时间限制。一旦达到这些限制，设备必须返回正常状态。

交易结束或者响应超时时，防入侵设备必须自动清除内部的缓存。

6.4.2.2 密码键盘安全性

密码键盘必须设计为防入侵设备。它必须支持输入 4-12 个数字的 PIN。如果密码键盘有显示屏，必须以不泄漏实际 PIN 值的方式显示每一个输入的数字，比如以*号代替数字显示。

如果终端支持脱机 PIN 校验，则 IC 卡读卡器和密码键盘要么被集成为单一的防入侵设备，要么是两个分离的防入侵设备。

——如果 IC 卡读卡器和密码键盘是集成的并且脱机 PIN 被以明文格式传递给卡片，那么在明文 PIN 被直接从密码键盘传到 IC 卡读卡器的情况下，密码键盘不对脱机 PIN 进行加密；

——如果 IC 卡读卡器和密码键盘是集成的并且脱机 PIN 被以明文格式传递给卡片，但脱机明文 PIN 不是被直接从集成的密码键盘传到 IC 卡读卡器，那么密码键盘必须依照 ISO 9564-1（或相当的被支付系统批准的其它方式）对脱机 PIN 进行加密，再将其传递给 IC 卡读卡器。IC 卡读卡器随后对脱机 PIN 解密，再以明文传递给卡；

——如果 IC 卡读卡器和密码键盘不是集成的并且脱机 PIN 以明文格式传递给卡片，那么密码键盘必须依照 ISO 9564-1（或相当的被支付系统批准的其它方式）对脱机 PIN 进行加密，再将其传递给 IC 卡读卡器。IC 卡读卡器随后对脱机 PIN 解密，再以明文传递给卡。

PIN 的加密过程必须发生在下面两种其一的情况：

如果终端支持联机 PIN 校验，当 PIN 被输入后，必须依照 ISO 9564-1 对 PIN 进行加密来保护 PIN，并且对 PIN 的传输必须符合支付系统的规则。

显示在密码键盘上提示输入 PIN 的信息必须由密码键盘生成。这并不意味着只有和 PIN 相关的信息才能在密码键盘上显示，但其它的信息在显示前必须被密码键盘批准。密码键盘必须拒绝任何未经批准的信息的显示。

对于有人值守的终端，金额输入过程必须和 PIN 输入过程分开，以避免意外地将 PIN 显示在终端的显示屏上。特别是如果在同一个键盘上输入金额和 PIN，那么金额输入和 PIN 输入必须是明显分开的两个操作，如果没有其他确认操作，持卡人输入的 PIN 应被用于金额确认。

密码键盘必须被设计为能提供隐私性和机密性，使得在正常的使用中，只有持卡人能够看到输入或显示的信息。密码键盘的安装和替换必须保证它的周边环境为持卡人输入 PIN 提供了足够的隐密性，从而将 PIN 暴露给他人的风险降到最低。

密码键盘必须在以下两种条件发生后自动清除内部缓存：

——交易完成；

——响应超时，比如输入一个 PIN 字符后，长时间等待。