社会保障（个人）卡规范
第 10 部分：个人化指南

引言

本部分作为《社会保障（个人）卡规范》的第 10 部分，包括以下主要内容：

——社会保障卡在 COS 激活、卡片预个人化、持卡人数据准备、卡片个人化等各个阶段有关数据定义及安全、管理等方面的规定。

1 适用范围

本规范适用于人力资源和社会保障领域面向各类参保人员发行的社会保障卡。其使用对象主要是与社会保障卡应用相关的卡片设计、制造、管理、发行和受理以及应用系统的研制、开发、集成和维护等组织机构。

2 参考文件

3 定义

以下定义适用于本规范。

3.1 集成电路（Integrated circuit ,IC）

具有处理和/或存储功能的电子器件。

3.2 集成电路卡（IC 卡）(integrated circuit(s) card)

内部封装一个或多个集成电路用于执行处理和存储功能的卡片。

3.3 明文（Plain Text）

没有加密的信息。

3.4 密文（Cipher Text）

通过密码系统产生的不可理解的文字或信号。

3.5 密钥（Key）

控制加密转换操作的符号序列。

3.6 加密算法（Cryptographic Algorithm）

为了隐藏或揭露信息内容而变换数据的算法。

3.7 对称加密技术（Symmetric Cryptogram Technique）

发送方和接收方使用相同保密密钥进行数据变换的加密技术。在不掌握保密密钥的情况下，不可能推导出发送方或接收方的数据变换。

3.8 非对称加密技术（Asymmetric Cryptogram Technique）

采用两种相关变换进行加密的技术，一种是公开变换（由公共密钥定义），另一种是私有变换（由私有密钥定义）。这两种变换具有以下属性，即私有变换不能通过给定的公开变换导出。

3.9 私有密钥（Private Key）

一个实体的非对称密钥对中仅供实体自身使用的密钥。在数字签名模式中，私有密钥用于签名功能。

3.10 公共密钥（Public Key）

一个实体的非对称密钥对中可以公开的密钥。在数字签名模式中，公共密钥用于签名验证功能。

3.11 保密密钥（Secret Key）

对称加密技术中仅供指定实体所用的密钥。

3.12 数据完整性（Data Integrity）

数据不受未经许可的方法变更或破坏的属性。

3.13 读写器（Reader）

本部分中“读写器”一词是指与卡片交互的受理设备。

4 缩略语和符号表示

以下缩略语和符号表示适用于本规范。

AID	应用标识符（Application Identifier）
APDU	应用协议数据单元（Application Protocol Data Unit）
ATR	复位应答（Answer to Reset）
DEA	数据加密算法（Data Encryption Algorithm）
DF	专用文件（Dedicated File）
DIR	目录（Directory）
EF	基本文件（Elementary File）
IC	集成电路（Integrated Circuit）
ICC	集成电路卡（Integrated Circuit Card）
K_M	主控密钥（Master Key）
K_S	过程密钥（Session Key）
MAC	报文鉴别码（Message Authentication Code）
MF	主控文件（Master File）
PIN	个人密码（Personal Identification Number）
RST	复位（Reset）
SAM	安全存取模块（Secure Access Module）
SSA	社会保障应用（Social Security Application）
SSSE	社会保障系统环境（Social Security System Environment）

5 个人化过程

5.1 COS 激活

芯片在卡片制造商处要进行 COS 激活才能进一步操作使用，这个过程包括两个方面的操作，设置卡片默认传输密钥、设置卡片复位信息。

5.1.1 设置卡片默认传输密钥

在 COS 激活过程中设置默认传输密钥，这个默认的传输密钥在卡片后期处理中会被卡

片加载的主控密钥替换或隐藏。当卡片后期进行结构删除后，卡片主控密钥一并被删除，此时初始化设置的传输密钥自动被启用或重新生效。设置此默认的卡片传输密钥的目的是处于对卡片的安全性管理的需要，在对卡片进行文件创建时需要先认证此传输密钥，获得创建权限，才能进行文件结构的创建操作。

5.1.2 历史字节设置

在 COS 激活过程中要设置其上电复位后返回的历史字节，设置历史字节的方式通过向芯片发送 apdu 指令来实现。

卡上电后，COS 向接口设备发送复位应答序列，结构如下：

3B	6x（‘1’ ~ ‘F’）	00	00	历史字节（0~15 字节）

历史字节：由制卡商根据用户的要求写入卡内。包含的历史字节信息举例如下：

符号	数值	说明
TS	3Bh	正向约定
T0	6xh	TB1 和 TC1 存在，保存 x 个历史字节
TB1	00h	不使用 Vpp
TC1	00h	额外所需的保护时间的数量
T1-	两	芯片提供机构注册标识号
T3-	两	送检年月
T5	一	COS 版本号
T6-	两	卡片制造机构注册标识号
T8-	六	卡序列号（可以由年月日 nnmmdd+初始化流水号 yyyyyy 组

5.2 预个人化

卡片在完成 COS 激活后需要进行预个人化操作，此过程包括认证卡片默认的传输密钥、加载卡片主控密钥替换卡片的传输密钥、创建社保应用的环境目录文件，加载社保环境的主控密钥，创建社保环境下相应的应用目录文件和数据文件结构、以及加载应用相关的密钥信息。这个与个人化可以由卡片制造商来完成，也可以由具备相应资质的机构来完成，例如一个市的社保应用项目可以有该省的社保初始化中心来完成此与个人化操作。

5.2.1 认证卡片默认的传输密钥

一般情况下，COS 设置都要求先认证卡片在初始化阶段设置的默认传输密钥，认证成功后才具备进一步操作卡片，建立社保应用相关文件。这是此安全载体的安全性要求，否则卡片就有可能受到外界的一些恶意攻击。卡片的默认传输密钥值一般由初始化机构知会承接卡片预个人化的单位，这时候所有卡片的传输密钥都是一个统一的定值。

5.2.2 创建社保环境 DDF

在预个人化阶段，当认证卡片默认传输密钥成功后，即可以创建社保环境的目录文件，此文件的名称一般采用“sx1.sh.社会保障”，社保应用目录的相关属性，比如应用空间大小、应用锁定密钥标识、应用主控密钥尝试次数、相关的目录文件短标识、等等属性的设置，需要根据相应社保项目的具体结构规划来确定。

5.2.3 加载社保环境主控密钥

在创建完社保环境的目录文件后，一般要紧接着加载卡片主控密钥，此时的卡片主控密钥是可以是一个 COS 默认值，也可以是一个临时主控密钥值，它的作用在于可以以此固定的密钥值保护加载社保应用的相关其他密钥，实现安全而又快速的加载密钥。同时又可以整个预个人化过程中，当出现异常导致失败时，可以使用此密钥值删除应用并重新进行预个人化操作。

5.2.4 创建社保环境下相应应用文件和数据结构

创建社保环境下的相关文件，必须包括但不限于社保规范规定的应用目录文件和数据记录文件。

社会保障应用各个具体应用的标识符（AID）必须采用由国家 IC 卡注册中心颁发的 RID，并通过 RID 选择该应用；对尚未获得 RID 的应用则采用社保规范附录规定的应用标签，并通过应用标签选择该应用。

5.2.5 加载应用相关密钥

当建立完卡片内社保应用目录文件和数据记录文件后，就接着加载社保应用的所有应用功能密钥，且这些密钥都是存放在安全介质中，例如硬件加密机，加密母卡等等。每条加载的密钥都是用卡片内的唯一标识例如卡片复位信息或者卡片识别码的一部分对加密介质中的根密钥进行分散，将分散后的密钥加载到卡内。这样一卡一密的方式，保证了社保应用使用过程中的安全性。

5.2.6 替换卡片主控密钥

在预个人化阶段的最后，一般是进行卡片主控密钥的替换，替换卡片主控密钥的方式一般是采用更新密钥的指令方式，在临时主控密钥的保护下，采用线路保护加效验码的方式进行。在此环节才进行卡片主控密钥的替换有利于卡片在发卡过程中失败时，可在认证卡片默认传输密钥或者临时主控密钥成功后，进行反复制卡。此过程完成后卡片的主控密钥是一卡一密，保证了卡片在管理过程中的安全性。

5.3 数据准备

社保卡在完成预个人化操作之前，需要完成社保应用制卡数据的数据准备，或者在预个人化的时候同步完成，否则会影响制卡流程的进度。

5.3.1 流程产生的背景

由于社保卡发行单位传输到制卡结构的原始数据格式存在不统一，为了提高接下来的个人化制卡阶段的程序开发效率和操作的准确性，需要将不同项目上社保卡发行单位传输来的原始数据按照制卡结构内部约定的个人化数据格式进行转换处理。

5.3.2 流程的实现方式

制卡机构内部一般会成立数据开发小组，专门负责制卡数据的处理工作，其中就包含转

换处理发行单位传送来的制卡原始数据。原始数据的的格式一般有 Excel 格式、txt 文本格式、XML 格式等等，这些格式都会因数据采集方式方法不同或原始数据生成方式而有所差别。对于某一个制卡机构，其内部最终转换出来的数据文件类型和格式一般会形成统一，以便个人化制卡程序的快速开发。

5.3.3 流程的可操作性和安全性

数据准备之初，需要可发行单位约定数据的传输接收方式，社保项目的数据一般要求按照加密方式传输，由于社保项目的数据量非常大，通常用到的传输方式是 FTP 站点传送的方式，采用的数据加密通常是靠软件工具加密，例如 PGP 软件加密，是一种常用加密方式，是靠产生 RSA 密钥对，用公私钥实现解密加密的。

5.4 个人化

5.4.1 解析社保卡制卡数据项

卡片个人化程序需要首先解析出相应的卡片个人化制卡数据，由于许多数据项的实际长度随持卡人的具体情况存在差异，当某一数据项的实际长度不足规范所定义的长度时，一般的填充规则是：

对格式为 cn 的数据项左靠齐并且右补十六进制‘F’，

对格式为 an 的数据项左靠齐并且右补十六进制‘0’，

在解析各数据项时，将解析出来的数据项的长度按照以上填充规则填充，使其达到社保规范所定义的长度。为下一步写入到卡内做好准备。

5.4.2 开发社保应用个人化数据项更新程序

开发社保应用个人化数据项更新程序，需要按照具体应用的结构文档，遵照文档中个数据项的相应格式，长度、类型来进行数据项的提取和整理。

5.4.3 认证密钥获得个人化权限，写入个人化数据项

个人化数据的添加或更新，一般都需要受到相关更新密钥的保护，需要认证相应的更新密钥成功后，才能获得更新权限。如果某条个人化数据更新失败，不影响之前已更新成功的数据内容，同时此条个人化数据项可以重新进行更新操作而不会影响卡片的其他性能。

5.4.4 社保卡卡面数据项的个人化

社保卡卡面的数据项一般会包含姓名、性别、社会保障号码、卡号、发行日期/失效日期等等，这些数据一般都是靠个人化程序从制卡数据中解析出来，其个人化工艺因发行单位的要求而会有所不同，其个人化的字体大小、位置等需求在卡片版面确认时，发行单位就已经确定。

一般包括但不限于以下工艺：光刻工艺；热转印印刷工艺；数码印刷工艺。

6 安全规范

6.1 预个人化安全

6.1.1 社保卡密钥定义

社会保障卡规范中列出了社保卡密钥的用途及应用范围。

6.1.2 社保卡密钥生成机制。

社保卡密钥包括卡片、应用主控密钥及从人力资源和社会保障部申领回来的应用密钥。

生成机制如下：

1. 卡片、应用主控密钥主要是用来保护卡片及应用不被擅自删除、添加，由发卡方来定义。

2. 从人力资源和社会保障部申领回来的应用密钥主要是用来维护公共、就业与失业、社会保险、医疗保险等应用，其他发卡方扩充的应用，由发卡方进行密钥管理。

3. 发卡方将所需的密钥存储到加密存储介质，如加密机，进而从加密存储介质中由传输密钥保护以密文带安全报文（MAC）的形式传递给卡片。

6.2 数据准备安全

6.2.1 传输密钥定义、生成和传输

1. 传输密钥定义：

个人化数据在数据传输保护过程中用以加密所需的密钥。对于数据的机密性通过对数据的加密进行解决，使用加密算法（使用加密密钥）将明文转换为密文，并使用相应的解密算法将密文转换回明文。

数据的加解密可使用对称密钥或非对称密钥加密技术。

对称密钥加密技术，是对在传输过程中对敏感数据采用相同的密钥进行加密和解密。目前，国内外应用最广的对称密钥加密技术采用的是 DES 算法。本指南要求对称密钥算法密钥长度为 128 位。

非对称密钥加密技术，与对称密钥加密技术相反，使用的是不相同的密钥进行加密和解密。目前，国内外使用最广的非对称密钥技术采用的是 RAS 算法。本指南要求非对称密钥算法密钥长度大于 1024 位。

2. 传输密钥的生成和传输

传输密钥可通过软件或硬件的方式生成。软件的方式指的是发卡方可提供解密程序给到个人化厂商，或者个人化厂商提供加密程序给到发卡方来进行数据的加解密。硬件的方式与软件的方式类同，区别在于它可以把密钥存储在硬件里，进行数据加解密时使用硬件里的密钥便可实现数据的安全传输。

3. 传输密钥的生命周期

传输密钥的生命周期为 5 年。

4. 传输密钥的交换方式

对于对称密钥，交换方式极其重要，必须保证密钥能够安全提供给对方。可在加解密硬件和软件的基础上再增加一个密码的认证，在网络传输方面采用点对点的传输，以减少对称密钥交换带来的风险。

对于非对称密钥，从很大程度上避免了对称加密密钥传送问题的麻烦。先由个人化卡厂生成一对非对称密钥，将生成的公钥提供给发卡方，再由发卡方用公钥对数据进行加密，最后传送到卡厂对数据进行解密。基于非对称密钥技术的特点，公钥是不能对数据进行解密，也只有拥有私钥的拥有者能够对数据进行解密。

6.3 个人化安全

6.3.1 数据接收及存储安全

个人化生产厂商的数据员的权利必须严格审核，拥有权利的数据员按照事先约定好的加

解密规则对相应的密文数据进行解密，并将解密的数据与发卡方进行比对校验，确保数据传输过程的完整性。

从个人化设备接收到个人化应用数据后应正确存储以保证数据的安全性，以供日后使用。

存储数据的环境必须高度安全，必须安装安防监控报警，实行 24 小时监控；下班无人时，必须启动安防报警装置设防；不允许使用摄影、录像、录音等与工作无关的记录设备；网络安全方面管理须严，必须做到防病毒、设置防火墙、网络隔离、入侵检测、网络监控等。

6.3.2 数据销毁

发卡结束出货检验合格后，数据管理员在产品保安人员监督下立即删除打卡机的相应数据，如果发卡方需要监督执行，则在发卡方指定人员的监督下执行删除相应的数据文件，并做好记录。

整批数据使用完成，卡片出货检验完成后，数据管理员在产品保安人员的监督下删除数据处理中心电脑中的数据，如果发卡方需要监督执行，则在发卡方指定人员监督下执行删除数据，并做好记录。

6.3.3 密钥安全

密钥安全管理是在 IC 卡之外执行的一切加密和解密操作必须在硬件安全模块上进行，并且要求硬件密钥存储器与生产设备分属不同场区，由专人负责管理，并且实施全程录相监控以保证安全，同时要求安全保障部门与管理部门分属不同业务范畴。

密钥存储以防止密钥泄露、被修改和被代替为原则。主要安全要求如下：

1. 普通文本私钥和秘密的密钥必须只存在于硬件加密设备内。

2. 私人和秘密的密钥及其组成部分必须用双重控制和分别持有的原则存储。这些原则的有效执行需要程序性控制的屏障存在，以防止任何管理人（或任何个体组成部分的非管理人）有机会访问足够构成实际密钥的组成部分。

3. 私人的和秘密的密钥组成部分可存储在介质上（例如：软盘、PC 卡、智能卡等）。这些介质必须安全存储，以防止未授权的个体得到密钥组成部分。

4. 如果私人的和秘密的密钥组成部分可存储在介质上，并且一个个人识别码介质，那么只有介质的拥有者必须同时拥有介质和它相应的 PIN。

5. 存储在密钥转移设备里的私人的或秘密的密钥组成部分必须通过像口令这样的充分的访问控制来保护。

6. 任何时候私人的密钥或密钥加密秘密的密钥及其组成部分从存储或加载到一个安全系统设备时，记录必须被保留。记录至少应该包括日期和进出的时间、访问的目的、访问此组成部分的管理人的签名等信息；这些记录应该被明确地保留，直到当密钥被终止或销毁时。

6.4 管理要求

6.4.1 密钥管理概述

社会保障卡的密钥管理采用部分集中管理方式，即

——对于由人力资源社会保障部信息中心负责维护其 AID 的应用，由人力资源社会保障部信息中心将密钥分发给发卡方。

——对于其他应用（包括发卡方扩充的应用），由发卡方进行密钥管理。

对于使用多版本密钥控制的交易，密钥版本号包含在相关的命令报文中。IC 卡收到这样的命令后，使用命令中所给的密钥版本号找到卡中的相应密钥进行运算。

在交易过程中，涉及密钥控制的所有阶段都必须使用过程密钥（Session Keys）,并且采用《社会保障（个人）卡规范》第一部分 IC 卡规范中描述的方式产生所有的过程密钥。

6.4.2 密钥管理

IC 卡上的密钥必须安全存储。

下表描述了存储在社会保障卡上用于社会保障应用的密钥。

分类	密钥	用途	适用的应用范围
	IRK	鉴别发卡方的密钥	应用提供者
	PUK	个人密码解锁密钥	发卡方
应用维护密钥	STK	发卡人或应用提供方用于产生应用锁定、卡片锁定和更新二进制或记录命令的 MAC	发卡方
	STKdf01		公共应用
	STKdf02		就业与失业应用
	STKdf03		社会保险应用
	STKdf04		医疗保险应用（联网、脱网）
卡片活应用锁定控制密钥	BK	发卡方或应用提供方控制锁定卡片或应用操作的密钥	发卡方
	LKdf03		社会保险应用
	LKdf04		医疗保险应用（联网、脱网）
	UKmf	发卡方或提供方控制应用数据更新操作的	发卡方和持卡方基本信息
	UK1df01		户籍信息
	UK2df01		个人状况信息、就业单位信息
	UK3df01		婚姻状况信息
	UK4df01		通讯信息
	UK5df01		工资信息
	UK1df02		职业和专业信息
	UK2df02		就业与失业信息
	UK3df02		就业信息

应用数据更新密钥	UK4df02	密钥	农村流动劳动力就业登记卡信息
	UK5df02		农村流动劳动力就业证信息
	UK1df03		失业保险信息
	UK2df03		丧失劳动能力鉴定信息
	UK3df03		养老保险信息
	UK4df03		医疗保险基本信息（联网、脱网）
	UK5df03		医疗保险帐户信息（联网）
医疗保险交易密钥（脱网）		用来产生帐户划入	医疗保险帐户划入交易
	DPK	用来产生医疗消费	医疗保险医疗消费交易
	DTK	用来产生帐户支付、	医疗保险交易（脱网）
应用数据读取密钥	RK1df03	发卡方或应用提供方控制部分应用数据读取操作的密钥	养老保险信息
	RK2df03		失业保险信息
	RK1df04		医疗保险帐户信息（联网）

6.4.2.1 密钥操作管理

密钥操作主要通过规范的方式使用，完全由软件程序控制，系统与外部网络物理隔离。

当 DES 密钥正被传输或存储时，以下措施将限制数据泄漏的潜在危险。

1. DES 密钥可以被安全地转移到一块安全设备或智能卡的保护之下，以进行传输和存储。

2. DES 密钥传输必须以双重控制和分别持有为原则。

6.4.2.2 密钥存储管理

密钥存储以防止密钥泄漏、被修改和被代替为原则。主要安全要求如下。

1. 普通文本私钥和秘密的密钥必须只存在于硬件加密设备（HSM）内。

2. 私人和秘密的密钥及其组成部分必须用双重控制和分别持有的原则存储。这些原则的有效执行需要程序性控制的屏障存在，以防止任何管理人（或任何个体组成部分的非管理人）有机会访问足够构成实际密钥的组成部分。

3. 私人的和秘密的密钥组成部分可存储在介质上（例如：软盘、PC 卡、智能卡等）。这些介质必须安全存储，以防止未授权的个体得到密钥组成部分。

4. 如果私人的和秘密的密钥组成部分可存储在介质上，并且一个个人识别码（PIN）介质，那么只有介质的拥有者必须同时拥有介质和它相应的 PIN。

5. 存储在密钥转移设备里的私人的或秘密的密钥组成部分必须通过像口令这样的充分的访问控制来保护。

6. 任何时候私人的密钥或密钥加密秘密的密钥及其组成部分从存储或加载到一个安全系统设备时，记录必须被保留。记录到少应该包括日期和进出的时间、访问的目的、访问此组成部分的管理人的签名等信息;这些记录应该被明确地保留,直到当密钥被终止或销毁时。

6.4.2.3 密钥备份方案

加密机的密钥备份由人力资源社会保障部密钥管理软件完成备份,在生产场所不允许非授权的备份。

6.4.2.4 密钥安全控制管理

在正式发卡过程中,卡商都会从加密机里导密钥到正式卡片,这过程卡商一般都会有发卡的日志,所以发卡日志要定时销毁,避免卡片密钥外泄。

6.4.2.5 密钥异常处理

当加密机的在使用过程中发生密钥丢失等情况,必须通知某项目当地的人力资源社会保障局信息中心负责管理,由某项目当地人力资源社会保障局派相关人员完成密钥重新安装等操作；所有操作必须建立记录。

6.5 安全模块

6.5.1 个人化安全

IC 卡个人化设备向 IC 卡发送个人化命令和指令时，必须对发送的密钥数据和常规数据进行加密和 MAC 校验，其加密过程必须与硬件安全模块（HSM）相连。

必须位于单位的高安全区并满足所有安全要求及程序。

个人化生产设备与硬件安全模块 HSM 分属不同的生产场区，以保证数据的安全性。

6.5.2 设备安全控制

设备必须是独立的，且与应用无关；

在数据注入过程中，个人化设备必须与一个硬件安全模块（HSM）相连，以保证发送指令时进行数据的加解密和 MAC 校验；

必须位于工厂的高安全区并满足所有安全要求及程序，达到《社会保障卡生产企业安全管理指南》中的要求。

6.5.3 PSAM 卡安全控制

1. PSAM 卡管理

用于生产的 PSAM 卡发卡方应派专人专项进行存储保管，存储采用专柜方式，并作存储及使用备案记录，并委派保安部门定期检查并作检查登记备案。

2. PSAM 卡操作

首先登记申请使用 PSAM 卡用于某个项目个人化生产；进行登记使用备案记录，并领用相应 PSAM 卡进行生产，相关人员进行记录安全控制登记，且保安部门定期检测记录要案。；审计和控制日志必须保留所有的使用活动记录；任何有能力加密一个密钥的安全加密系统设备和那个密钥产生的密文必须被对知道密钥或知道密钥组成部分的未授权的使用加密保护.这种保护采取以下一种或两种形式：要双重访问控制以使密钥加密功能成为可能、双重控制下的设备的物理保护（例如：对其访问加锁）。

3. PSAM 卡返还

当一台设备出现使用故障或被永久废弃和销毁时，要求如下：

PSAM 卡记录登记相应 PSAM 卡返还业主记录以备案，包括相应 PSAM 卡唯一标识号以及时间及经办人员；

相应 PSAM 卡返还给业主，并业主方留案登记。

6.6 风险审计

在每个 IC 卡应用的个人化过程的最后，必须创建这个应用的个人化过程的记录。在整个个人化过程的最后，必须创建包含所有的 IC 卡应用的个人化过程纪录的审计文档。这些记录可保证对个人化过程的可审计性和可跟踪性。

6.6.1 个人化环境风险防范的手段及控制

社会保障 IC 卡个人化环境，包括个人化中心人员进出、个人化中心人员流程操作管理、个人化设备使用维护与管理、个人化数据操作管理、个人化存储设备管理。主要采取的风险防范手段：保安进出管理、电视全程监控、设备操作规范及权限设置及控制、流程操作规范、数据操作规范、设备(服务器及加密机)管理制度、生产网络访问权限设置及控制、环境管理的安全监督机制。

6.6.2 个人化人员管理风险防范的手段及控制

社会保障个人化人员日常就与敏感数据打交道，其中，生产网络管理人员、数据操作人员在这方面尤其突出。所采用的主要控制手段有：保密协议制度、上岗审查制度、保安进出管理、电视全程监控、人员管理的安全监督机制。