社会保障卡加载金融功能通用规范

1 引言

本规范对具有金融功能的社会保障卡的卡片整体结构、系统环境选择、安全控制、个人化过程等提出要求和规定。

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。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。

3 参考标准

ISO/IEC 7816-4:2005	识别卡 带触点的集成电路卡 第 4 部分：行业间交换用命令
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 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。

4.3 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。

4.4 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。

4.5 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。

4.6 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。

4.7 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。

4.8 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。

4.9 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。

4.10 报文鉴别代码（Message Authentication Code）

对交易数据及其相关参数进行运算后产生的代码，主要用于验证报文的完整性。

4.11 密钥（Key）

控制加密转换操作的符号序列。

4.12 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。

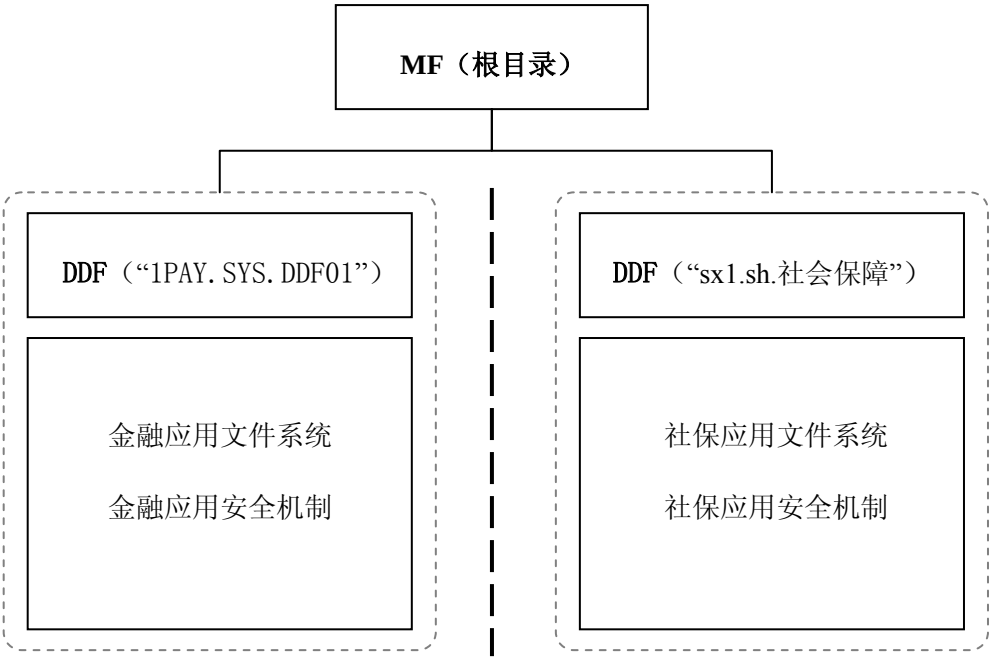
5 缩略语和符号表示

AID	应用标识符（Application Identifier）
ADF	应用数据文件（Application Definition File）
DDF	目录定义文件（Directory Definition File）
DF	专用文件（Dedicated File）
FCI	文件控制信息（File Control Information）
IC	集成电路（Integrated Circuit）
ICC	集成电路卡（Integrated Circuit Card）
PSE	金融支付系统环境（Payment System Environment）
MAC	报文鉴别代码（Message Authentication Code）
MF	主控文件（Master File）
SSSE	社保应用系统环境（Social Security System Environment）

6 卡片整体结构

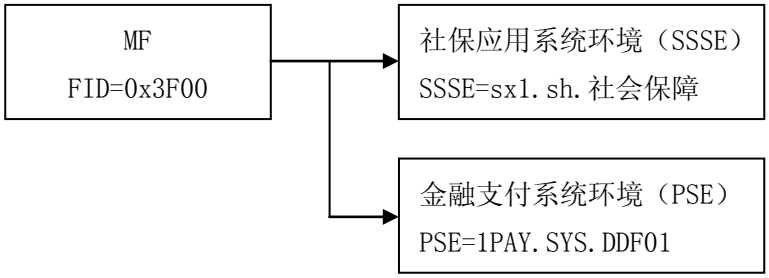
6.1 整体安全架构

具有金融功能的社会保障卡的整体安全架构见下图：



6.2 卡片应用结构

具有金融功能的社会保障卡的卡片总体结构见下图：



MF 是具有金融功能的社会保障卡的根，其下有社保应用系统环境（SSSE）和金融支付系统环境（PSE）。进入到各系统环境后，相关命令、交易流程、安全机制遵循《社会保障（个人）卡规范》或《中国金融集成电路（IC）卡规范》（JR/T 0025-2010）。

7 系统环境选择

7.1 选择流程

卡片完成复位应答后，卡片应位于 MF 下，通过选择不同的系统环境进入不同的应用。

7.2 选择社保应用系统环境

终端通过发送 SELECT 命令（“sx1.sh.社会保障”）给 IC 卡进入社保应用系统环境。

进入社保应用系统环境后，终端应通过应用选择的方式确定一个应用进行交易。

7.3 选择金融支付系统环境

终端通过发送 SELECT 命令（“1PAY.SYS.DDF01”）给 IC 卡进入金融支付系统环境。

进入金融支付系统环境后，终端应通过应用选择的方式确定一个应用进行交易。

8 SELECT 命令

SELECT 命令通过文件名或 AID 来选择 IC 卡中的 SSSE、PSE 或 ADF。

成功执行该命令后，SSSE、PSE 或 ADF 的路径被设定。

从 IC 卡返回的应答报文包含回送 FCI。

本命令定义适用于 MF，SSSE 下的 SELECT 命令由《社会保障（个人）卡规范》规定，PSE 下的 SELECT 命令由《中国金融集成电路（IC）卡规范》（JR/T 0025-2010）规定。

9 安全控制

9.1 MF 安全控制

MF 是整个 IC 卡文件系统的根，拥有卡片主控密钥。卡片主控密钥用于控制更新卡片主控密钥、创建系统环境和装载系统环境主控密钥；成功创建系统环境和装载系统环境主控密钥后，卡片主控密钥对该系统环境不再拥有控制权。

9.2 社保应用系统环境下的安全控制

社保应用系统环境拥有社保环境主控密钥，社保环境主控密钥用于控制更新社保环境主控密钥、创建社保应用系统环境目录下的文件、装载社保应用密钥等。社保应用系统环境下的安全机制必须符合《社会保障（个人）卡规范》的安全要求。

9.3 金融支付系统环境下的安全控制

金融支付系统环境拥有金融环境主控密钥，金融环境主控密钥用于控制更新金融环境主控密钥、创建金融支付系统环境目录下的文件、装载金融应用密钥等。金融支付系统环境下的安全机制必须符合《中国金融集成电路（IC）卡规范》（JR/T 0025-2010）的安全要求。

9.4 应用防火墙机制

社保应用系统环境和金融支付系统环境在 IC 卡中通过应用防火墙相互隔离，互不影响。

10 个人化要求

10.1 个人化过程

个人化过程具体指卡片从完成封装之后到生产为成品卡实施发放之前的全过程，包括卡片激活、预个人化处理、数据准备和个人化处理四个子过程。

10.2 卡片激活

由卡片生产工厂按照本规范的规定对卡片完成卡片激活子过程，包括设置卡片的默认传输密钥和设置卡片复位信息。

10.3 预个人化处理

社保应用的预个人化，应符合《社会保障（个人）卡规范》的要求。

金融应用的预个人化，应符合《中国金融集成电路（IC）卡规范》（JR/T 0025.10-2010）的要求。

预个人化处理子过程，通常在卡片生产工厂完成，也可以部分或全部在个人化机构完成。如果有部分或全部在个人化机构完成，社保应用和金融应用的预个人化处理子过程，可以集

中完成，也可以分别和相应的个人化处理子过程一起分步完成。

10.3.1 数据准备

社保应用和金融应用的数据准备子过程，通常是独立的，分别创建用于个人化社保应用和金融应用的所有数据，包括应用数据、应用密钥和证书等。数据准备子过程中创建的保密数据必须加密，并且应该为传送到个人化设备的数据产生一个 MAC，以保证数据的完整性。

社保数据准备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力资源社会保障部门事先约定。

金融数据准备要求，参照《中国金融集成电路（IC）卡规范》（JR/T 0025.10-2010）规范执行。

10.3.2 个人化处理

社保应用和金融应用的个人化，可以在一个个人化机构集中个人化，也可以在多个个人化机构分步个人化。社保应用和金融应用的个人化，分别需要先认证各自的系统环境主控密钥。

10.4 个人化模式

具有金融功能的社会保障卡的个人化可采用集中个人化和分步个人化两种模式。发卡地区应优先采用集中个人化模式。

10.4.1 集中个人化模式

集中个人化模式是指由同一组织或机构一次性完成卡片社保、金融两部分应用个人化的模式。集中个人化模式的个人化机构可以是：地方人力资源社会保障部门、商业银行、双方认可的第三方个人化机构。

集中个人化模式如图 1 所示：

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。

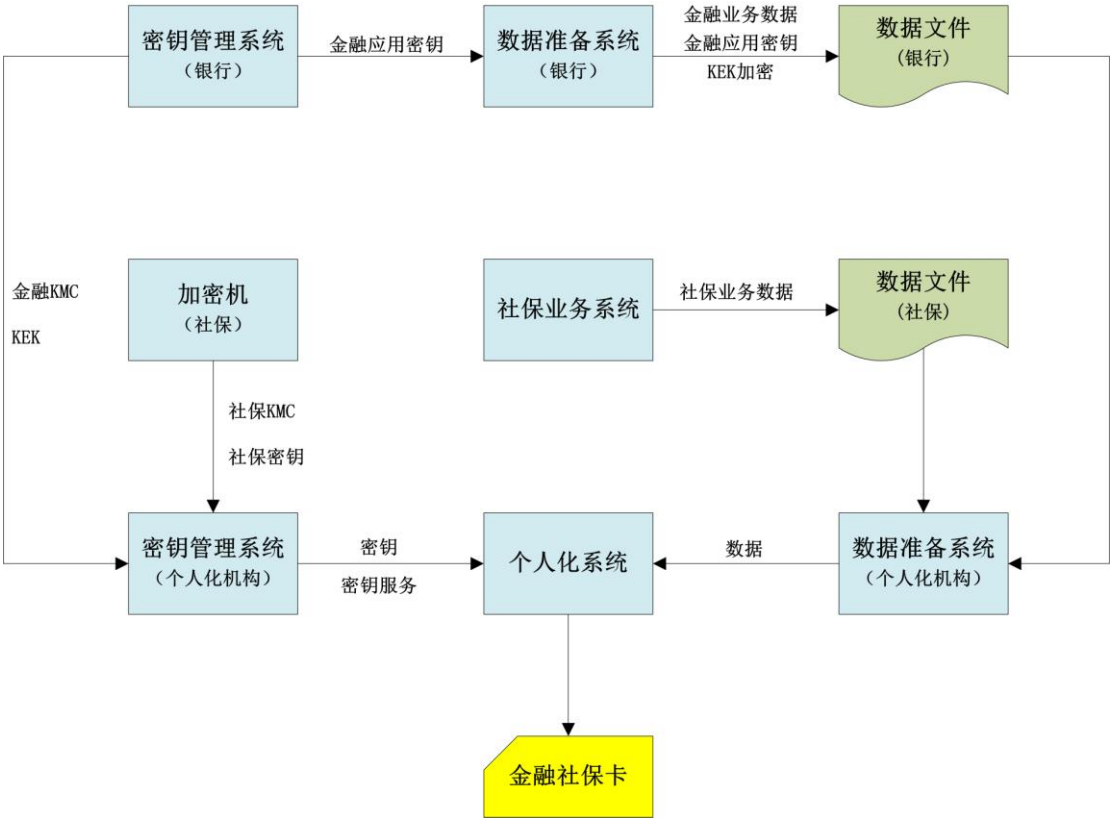


图1　集中个人化模式

10.4.2　分步个人化模式

分步个人化模式是指由不同组织或机构分步完成对卡片社保、金融两部分应用个人化的模式。其中，社保应用个人化机构可以是地方人力资源社会保障部门或地方人力资源社会保障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商业银行或商业银行认可的第三方个人化机构。

分步个人化模式如图 2 所示：

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的个人化相关的数据文件。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，供卡片发放使用。

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。

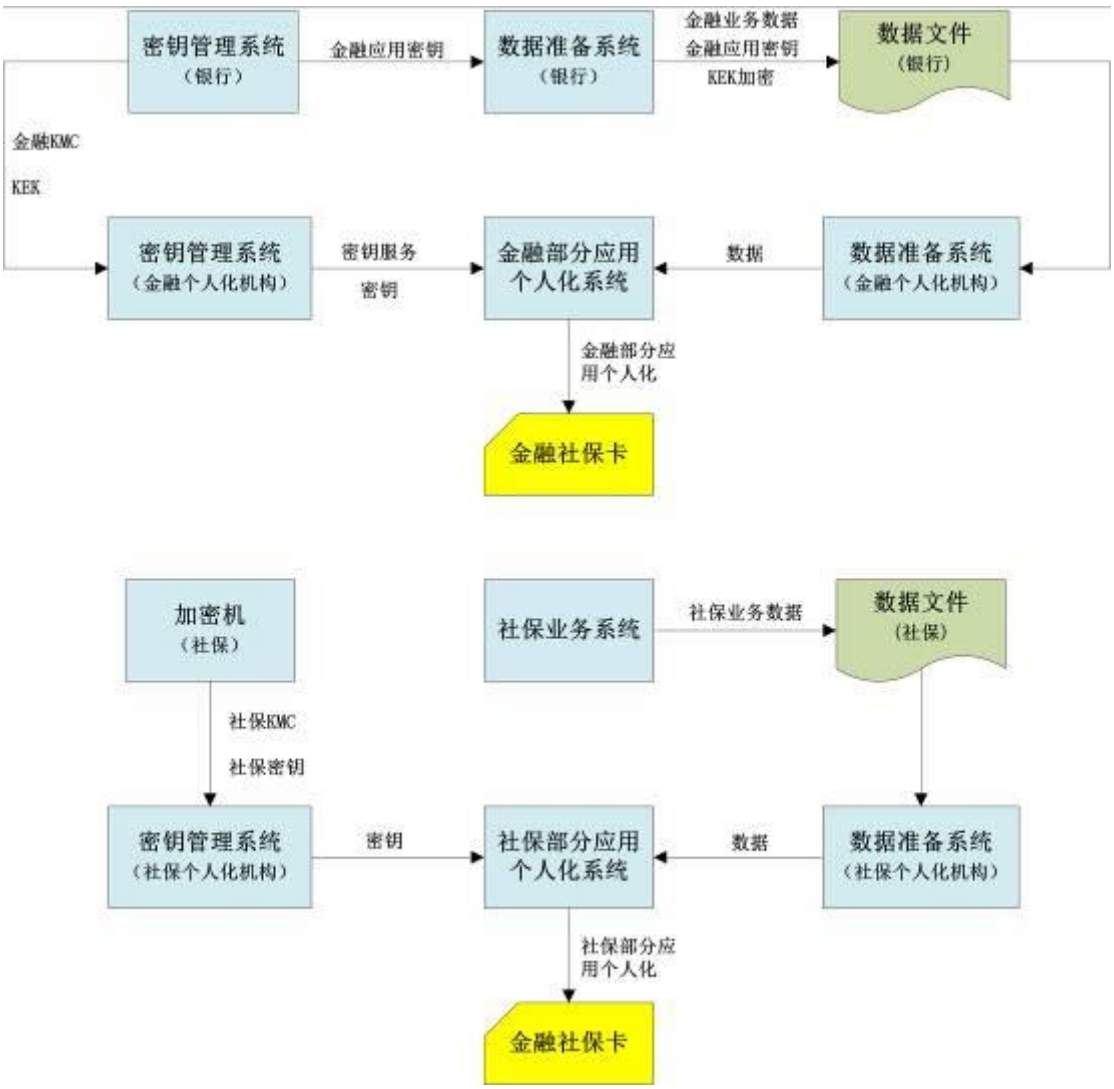


图2　分步个人化模式

10.5　个人化安全要求

在具有金融功能的社会保障卡个人化过程中，每一个步骤的安全要求应符合《社会保障（个人）卡规范》和《中国金融集成电路（IC）卡规范》（JR/T 0025.10-2010）的规定。