社会保障（个人）卡规范
第 3 部分：文件系统和应用选择

引言

本部分作为《社会保障（个人）卡规范》的第 3 部分，包括以下主要内容：

——文件系统。定义了社会保障卡的专用数据元、应用数据文件结构等内容。

——应用选择。定义了卡和终端完成应用选择的处理过程。

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 参考标准

GB/T 7408—2005	数据元和交换格式　信息交换　日期和时间表示法
GB/T 16263．1—2006	信息技术 ASN.1 编码规则 第 1 部分:基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)规范（ISO/IEC 8825：1990）
ISO/IEC 7816-4：1995	识别卡　带触点的集成电路卡　第 4 部分：行业间交换用命令
GB/T 16649．5—2002	识别卡　带触点的集成电路卡　第 5 部分：应用标识符的编号系统和注册程序（ISO/IEC 7816-5：1994）
GB/T 16649．6—2001	识别卡　带触点的集成电路卡　第 6 部分：行业间数据元（ISO/IEC 7816-6：1996）

3 定义

以下定义适用于本规范。

3.1 终端（Terminal）

为处理社会保障卡业务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，例如与主机通信的接口。

3.2 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。

3.3 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。

3.4 交易（Transaction）

持卡者和业务、管理部门之间根据社会保障卡所支持的应用接受、提供服务的行为。

3.5 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。

3.6 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。

3.7 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（如 ISO/IEC 7810、ISO/IEC 7811 第 1 至第 5 部分、ISO/IEC 7812 和 ISO/IEC 7813 中描述的）。

3.8 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。

3.9 密钥（Key）

控制加密转换操作的符号序列。

3.10 社会保障应用（Social Security Application）

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。

3.11 专业应用（Speciality Application）

由人力资源和社会保障各业务管理部门提供并维护的社会保障卡应用，例如就业与失业应用。

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）
AEF	应用基本文件 Application （Elementary File）
an	字母数字型（Alphanumeric）
b	二进制（Binary）
B-TLV	BER-TLV 符合基本编码规则的标签、长度、值（Basic Encoding Rules of Tag Length, Value）
DDF	目录定义文件（Directory Definition File）
DF	专用文件（Dedicated File）
EF	基本文件（Elementary File）
FCI	文件控制信息（File Control Information）
ISO	国际标准化组织（International Organization for Standardization）
MF	主控文件（Master File）
PIX	专用应用标识符扩展码（Proprietary Application Identifier Extension）
RID	已注册的应用提供者标识（Registered Application Provider Identifier）
SFI	短文件标识符（Short File Identifier）
SSA	社会保障应用（Social Security Application）
SSSE	社会保障系统环境（Social Security System Environment）
SW1	状态码 1（Status Word One）
SW2	状态码 2（Status Word Two）
TLV	标签、长度、值（Tag Length Value）
‘0’-‘9’ ‘A’-‘F’	十六进制数字
xx	任意值

5 文件系统

IC 卡中的每个应用都包括一系列信息项，在终端成功地完成应用选择后可以对这些信息进行访问。

一个信息项称为一个数据元，数据元是信息的最小单位，它用名称、逻辑内容说明、格式及代码来标识。

数据文件中数据元以记录方式或二进制方式存储，文件结构及引用方式由文件的用途决定，并将在下面加以描述。除目录文件外，数据文件的内容和布局在《社会保障（个人）卡规范》第 6 部分：应用数据结构中说明，也可由发卡方补充定义。

5.1 文件结构

本规范的文件结构符合 ISO/IEC 7816-4。

本节描述了符合本规范的应用文件结构，这些应用被定义为社会保障应用（SSA）。符合 ISO/IEC 7816-4，但不符合本规范的其他应用也可以出现在 IC 卡上，并可以使用本规范中定义的命令进行操作。

IC 卡中 SSA 的路径可以通过明确选择社会保障系统环境（SSSE）来激活，SSSE 可以位于 MF，也可以位于 MF 下的 DDF。正如《社会保障（个人）卡规范》第 6 部分：应用数据结构中所描述的，一个成功的 SSSE 选择能够对目录结构进行访问。应用选择过程在本规范第 6 章应用选择中描述。

从终端角度来看，SSA 相关的 SSSE 文件呈一种可通过目录结构访问的树形结构。

树的根和每一分支都是一个应用数据文件（ADF）。一个 ADF 是一个或多个应用基本文件（AEF）的入口点。一个 ADF 及其相关数据文件处于树的同一分支上。

5.1.1 应用数据文件（ADF）

ADF 的树形结构：

——能够将数据文件与应用联系起来；

——确保应用之间的独立性；

——可以通过应用选择实现对其逻辑结构的访问。

从终端角度看，ADF 是一个只包含其文件控制信息（FCI）中纯数据对象的文件，参见表 1。

表 1 ADF 文件控制信息

标志	值	存在方式
‘6F’	FCI 模板	M
‘84’	DF 名	M

5.1.2 应用基本文件（AEF）

一个 AEF 包含有一个或多个原始 BER-TLV 数据对象（记录结构的 AEF），或一个非结构化的纯数据元（透明结构的 AEF）。在选择了某一应用后，AEF 既能通过其文件标识符进行查询，也可以通过其短文件标识符（SFI）进行查询。

记录结构的 AEF 具有如下属性：记录的长度是固定的或是可变的；记录的组织结构是线形结构或循环结构。

5.1.3 ISO/IEC 7816-4 文件结构中文件的映像

ISO/IEC 7816-4 中使用下列映像表：

——包含一个 FCI 的专用文件（DF）（ISO/IEC 7816-4 中定义）被映像为 ADF，可以通过它来访问 EF 和 DF。在卡中处于最高层的 DF 称为主控文件（MF）。

——包含一组应用数据元的基本文件（EF）（ISO/IEC 7816-4 中定义）被映像为 AEF，EF 不能作为进入另一个不同双亲的 DF 文件的入口点。

在此规范中，DF 中相关联的 EF 的访问是透明的。

5.1.4 目录结构

社会保障应用的各个具体应用项对应的专用文件（DF）与基本数据文件分别构成一个树状结构的各个分支。每个专用文件是其下属的基本数据文件的入口点。

为便于发卡方和服务提供方根据实际情况确定本规范中所定义的应用是否在社会保障卡中存在，应用具体采用何种密码算法，以及满足允许在社会保障卡中存在非本规范所定义的其他应用的需要，IC 卡可以选择支持用于社会保障系统环境（SSSE）应用列表的目录结构，SSSE 由发卡方通过目录选择。

目录结构包括一个社会保障系统目录文件（DIR 文件）和一些由目录定义文件（DDF）引用的附加目录。

目录结构采用以其应用标识符（AID）的方式进入一个应用，或以 AID 的前 N 个字节作为 DDF 名的方式进入一组应用。

在 SSSE 选择的响应报文中对 DIR 文件进行编码（见《社会保障（个人）卡规范》第 5 部分：命令）。

DIR 文件是一个记录结构的 AEF，它包含 ISO/IEC 7816-5 中定义的数据对象，即本规范第 6 章应用选择中描述的一个或多个应用模板（标签为‘61’）。

在 IC 卡中社会保障系统外的其他目录是可选的，且不限制它们存在的数量。其中每个目录的位置由包括在每个 DDF 中的 FCI 的目录 SFI 数据对象指定。

如果不存在目录文件，则认为社会保障卡中包含了《社会保障（个人）卡规范》所定义的所有应用。

5.1.5 卡片结构示例

图 1 给出了一个卡片内部结构示例，该卡片支持公共应用（户籍信息、婚姻状况信息）和就业与失业、社会保险等应用。图 1 仅仅是一个例子。

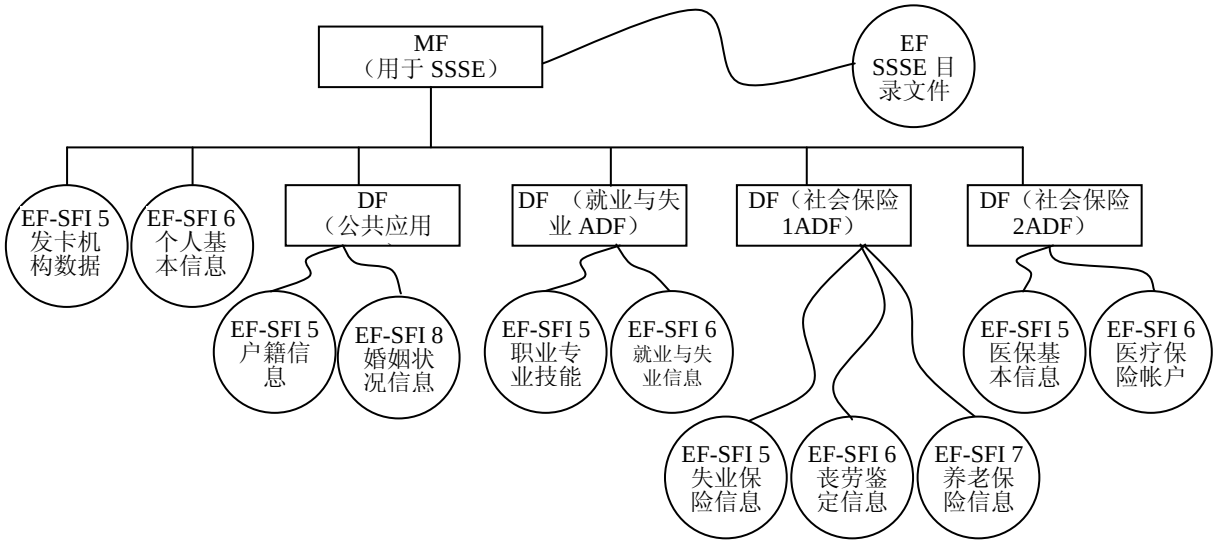

图 1　卡片内部结构示例

5.2　文件查询

依照其类型，文件可以通过文件名、文件标识符或 SFI 进行查询。

5.2.1　通过文件名查询

卡中的任何 ADF 或 DDF 可通过其 DF 名查询，ADF 的 DF 名对应其 AID，每个 DF 名在给定的卡中应是唯一的。

5.2.2　通过文件标识符查询

卡中的任何 ADF、DDF 或 AEF 可通过其文件标识符查询，每个 DF 的文件标识符在给定的卡中应是唯一的，AEF 的文件标识符在一个给定的应用中必须是唯一的。

5.2.3　通过 SFI 查询

SFI 用于选择 AEF。对给定应用中的任何 AEF，可以通过 SFI（5 位代码，取值范围从 1~30）查询。SFI 的编码在每个用到它的命令中描述。

在一个给定的应用中 SFI 应是唯一的。专用 SFI 的使用由应用决定。

5.3　记录引用

在每个记录结构的 EF 内，每个记录可以通过记录标识符和/或记录号来引用。记录标识符和记录号都是值在从‘01’至‘FE’范围内无符号 8 比特整数。值‘00’被保留用于特定目的。值‘FF’为 RFU。

通过记录标识符引用将导致对记录指针的管理。卡的复位、选择文件和带有有效短 EF 标识符的任何命令都能影响记录指针。通过记录号引用应不影响记录指针。

5.3.1　通过记录标识符引用

每个记录标识符由应用来提供。如果记录是报文的数据字段中的简单 TLV 数据对象，则记录标识符是数据对象的第 1 个字节。在记录结构的 EF 内，记录可以具有相同记录标识符，在此情况下，在记录中所包含的数据可以用来辨别这些记录。

每次使用记录标识符进行引用，一个指针应指定目标记录的逻辑位置：第 1 个或最后一个出现，下一个或先前一个出现都与记录指针有关。

——在每个线性结构的 EF 内，当写入或添加时，逻辑位置应有序地被分配，即按建立的次序。因此，第 1 个建立的记录是在第 1 个逻辑位置上。

——在每个循环结构的 EF 内，逻辑位置应按相反的次序来分配，即，最近建立的记录是在第 1 个逻辑位置上。

对于线性结构和循环结构，定义下列附加规则。

——第 1 个出现的应是带有规定标识符并在第 1 个逻辑位置上的记录；最后一个出现的应是带有规定标识符并且在最后一个逻辑位置上的记录。

——当不存在当前记录时，下一个出现应等价于第 1 个出现；先前一个出现应等价于最后一个出现。

——当存在当前记录时，下一个出现的应是同规定标识符的最接近记录，但是在比当前记录更大的逻辑位置上；先前一个出现的应是带有规定标识符的但是在比当前记录更小的逻辑位置上的最近记录。

——值‘00’应按编号顺序表示第 1 个、下一个或先前一个记录，但与记录标识符无关。

5.3.2 通过记录号引用

在每个记录结构的 EF 内，记录号是唯一的和顺序的。

——在每个线性结构的 EF 内，当写入或添加时，记录号应有序地被分配，即按建立的次序。因此，第 1 个记录（记录号 1，#1）是第一个创建的记录。

——在每个循环结构的 EF 内，记录号应按相反的次序来分配，即第 1 个记录（记录号 1，#1）是最近建立的记录。

对于线性结构和循环结构，定义了下列附加规则。

——值‘00’应表示当前记录，即通过记录指针所固定的那个记录。

6 应用选择

本章从卡片和终端两个角度描述了应用选择的过程。一方面描述了该过程所需的卡片数据和文件的逻辑结构，另一方面描述了适应这种卡片逻辑结构的终端逻辑。

终端按本章所描述的应用选择过程，根据这里所定义的协议使用 IC 卡上的数据来决定选择哪种社会保障应用进行交易，其过程分两个步骤：

——建立卡与终端两者共同支持的应用列表；

——在上述应用列表中选择一个将要运行的应用。

本章描述了为完成正确的应用选择所需要卡上的必要的信息以及两个终端选择算法。其他能够实现同样结果的终端选择算法可用来代替本章描述的算法。

应用选择通常是最先执行的应用功能。

一种社会保障系统应用包括以下内容：

——IC 卡上一组已由发卡方进行过客户化处理的数据文件；

——一组由业务部门提供的终端中的数据；

——一套卡和终端共同遵守的应用协议。

所有应用都唯一的由一个应用标识符（AID）标识。应用标识符的格式符合 ISO/IEC 7816-5（见 6.1）的有关规定。

鉴于目前社会保障卡内设置的一些应用尚未获得 RID，本规范为这些应用还定义了一个用文字描述的应用标签。在本规范中，除非特别说明，这些应用标签与 AID 具有等同的意义。对于所有接受符合本规范的社会保障卡的终端来说，应该维护这些应用标签与 RID 之间的对应关系表。

这里描述的社会保障系统所采用的技术在设计上应能满足下列主要目标：

——能够支持多功能 IC 卡；

——能够支持多功能终端，且这些终端能够支持符合本规范的 IC 卡；

——符合 ISO 标准；

——卡片支持多应用，但不要求所有的应用都是本规范第 6 部分应用数据结构所定义的社会保障应用；

——最小的存储开销和处理开销；

——具有允许发卡方优化选择过程的能力。

终端使用“SELECT”命令选择一个应用数据文件（ADF），ADF 中定义了 IC 卡中所支持某种应用的一组数据。

6.1 应用标识符的编码

应用标识符（AID）的结构符合 ISO/IEC 7816-5，它包含两个部分：

1．一个经过注册的应用提供者标识符（长度为 5 字节），它唯一地标识应用提供者。

2．一个可选的“专用应用标识符扩展码（PIX）”域，由应用提供者定义，最长 11 字节。

本规范规定的社会保障卡中使用的 AID 的具体编码方式见本规范第 6 部分：应用数据结构。

6.2 社会保障系统环境结构

社会保障系统环境应起始于一个名为“sx1.sh.社会保障”的目录定义文件（DDF）。这个 DDF 被映射到卡中的某个 DF，这个 DF 可以是 MF，也可以不是。

初始 DDF 所附属的目录包含了 ADF 的入口地址，这些入口地址是符合本规范格式的。而这些 ADF 定义的应用既可以符合也可以不符合本规范。该目录也可以包含其他 DDF 的入口地址，但这些入口地址的格式必须符合本规范。

不要求该目录包含卡片上所有的 DDF 和 ADF 的入口地址，也不要求沿着 DDF 的链接一定能够找到卡片支持的全部应用。当然，只有从初始目录开始，沿着 DDF 的链接能够找到的应用，才具备全国的互通性。

6.3 社会保障系统环境目录编码

社会保障系统目录文件（下文简称目录文件）是一个线性文件，用 5 到 15 的短文件标识符（SFI）标识。该目录文件附属于 DDF，目录文件的 SFI 包含在 DDF 文件控制信息中。目录文件可以使用本规范所定义的“READ RECORD”命令进行读取。目录文件中一个记录可以包含几个入口地址，但一个入口地址不能跨越多个记录存储。

社会保障系统目录文件的每一个入口地址都是一个应用模板（标记‘61’），它应包含表 2、表 3 所示信息。

表 2　DDF 目录入口地址格式

标志	长度	值	存在状态
‘4F’	5-16	DDF 名称	M

表 3　ADF 目录入口地址格式

标志	长度	值	存在状态
‘4F’	5-16	ADF 名称（AID）	M
‘50’	1-16	应用标签	M

6.4　社会保障系统环境选择

终端首先在社会保障系统环境下用 “SELECT”命令对文件“sx1.sh.社会保障”直接选择，由此进入社会保障系统环境。

终端将 IC 卡返回的密码算法标识与终端支持的密码算法标识列表进行比较，如果 IC 卡支持的的密码算法标识不在终端所支持的密码算法标识列表中，则终端与 IC 卡不匹配。

6.5　终端的应用选择

终端中应存放终端所支持的应用及其对应的应用标识符（AID） 和密码算法标识列表。本节描述两种应用选择过程：一个适用于支持较少数量应用的终端；另一个适用于支持较多数量应用的终端。

6.5.1　直接选择应用

如果一个终端支持的应用较少，该终端可以简单地使用“SELECT”命令轮流选择每个应用。如果“SELECT”命令执行成功（回送 SW1 SW2=‘9000’），则该终端将它所支持的 AID 与被选择文件的 FCI 中的文件名进行比较，通过比较的结果来查证 IC 卡是否支持此应用。如果二者相匹配，IC 卡支持该应用；如果返回的文件名比 AID 长而 AID 与返回文件名的起始部分相符，终端则重新发送“SELECT”命令并再次对选择进行验证；如果 IC 卡回送 SW1 SW2 不等于‘9000’，或者即使 IC 卡回送 SW1 SW2 等于‘9000’，而 AID 与文件名不相符且与文件名起始部分也不相符，则证明卡不支持此应用。

一旦终端支持的应用都被选择出来，则 IC 卡和终端都支持的应用列表就可以确定。然后终端可以选择指定的应用来运行。这一选择过程见 6.5.3。

6.5.2　社会保障系统环境目录的使用

如果终端支持较多的应用，可以通过使用社会保障系统环境目录来确定卡片所支持的应用。必须保证社会保障系统环境目录的结构设计正确，以便终端可以按照本规范描述的过程正确地选择应用。终端正确使用社会保障系统环境目录文件的步骤如下：

1．终端进入社会保障系统环境后，如果目录文件不存在，转至步骤 5；如果目录文件存在，则进入目录文件。

2．终端从第一条记录开始，连续读目录中的所有记录，直到卡回送 SW1 SW2=‘6A83’，表示所需记录序号已不存在。在执行“READ RECORD”命令查找第一个记录时，如果卡回送 SW1 SW2=‘6A83’，则表示目录为空，转至下面步骤 5。

3．如果目录中某个 ADF 名与终端支持的一个应用名相符，则将该应用列入最终应用选择的“候选名单”中。

4．如果目录中出现一个指向 DDF 的入口地址，且该 DDF 的名称至少与一个终端所支持的 AID 的前几位匹配（例如：一个名为 D156123456 的 DDF 可与一个名为 D15612345678 的 AID 匹配），则终端选择该 DDF。使用所选 DDF 的文件控制信息（FCI）中的目录短文件标识符（SFI）读出目录并按步骤 3 处理，之后终端继续回到上一个目录处理。

5．当终端处理完社会保障系统环境目录的列表后，所有能够按此方式找到的 ADF 就确定了，查找完毕。

6．终端也可以采用其他方式寻找卡内其他的专用应用（例如用 AID 找出本地特有的或非社会保障应用的专用选择方式），但不在本规范范围之内。

6.5.3　选择应用并执行操作

当终端确定了卡与终端相互支持的应用列表之后，下一步即要选取某个应用进行操作。可通过如下方法实现：

1．如果没有互相支持的应用，交易终止。

2．如果只有一个相互支持的应用，终端应向持卡人提出确认请求，如持卡人同意，则终端选择该应用；否则终端终止该交易。

3．建议显示应用列表请持卡人选择。显示应以终端的应用优先顺序为准；如果终端没有指定优先顺序，则按照应用在卡中出现的顺序为准。

一旦终端或持卡人确定了待执行的应用，则该应用被选中，终端发出一个“SELECT”命令进行应用的选择。如果命令回送的 SW1 SW2 ≠‘9000’，则此应用将从候选列表中删除，之后再将删除后的列表显示给持卡人，重新进行应用选择。