社会保障（个人）卡规范
第 6 部分：应用数据结构

引言

本部分作为《社会保障（个人）卡规范》的第 6 部分，包括以下主要内容：

——社会保障卡应用的文件结构。其中包括对 DDF，ADF 和 EF 中的内部属性，访问控制等信息。

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

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）

3　定义

以下定义适用于本规范。

3.1　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。

3.2　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。

3.3　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。

3.4　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）。

3.5　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。

3.6　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。

3.7　密钥(Key)

控制加密转换操作的符号序列。

3.8　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。 广义的

社会保障应用可以包括有关生命与健康、社会救助与优待抚恤等方面的应用。

3.9 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。

3.10 就业与失业应用(Employment and Unemployment Application)

一种为持卡人在人力资源和社会保障部门（以下简称人力资源社会保障部门）办理求职、就业登记或失业登记等事务而设计的社会保障卡应用。

3.11 社会保险应用(Social Insurance Application)

在本规范中将除医疗保险应用以外的各项社会保险应用统称为“社会保险应用”，即为持卡人在人力资源社会保障部门办理养老保险、失业保险、工伤保险、生育保险等事务而设计的社会保障卡应用。

3.12 社会保险应用 1(Social Insurance Application 1)

在本规范中将社会保险中的与医疗保险事务有关的应用单独称为“社会保险应用 1”，即一种为持卡人享受医疗保险待遇，办理相关就医手续等事务而设计的社会保障卡应用。

3.13 帐户划入(Wipe In Account)

将持卡人基本医疗保险个人帐户上尚未写入卡内的资金额度写到卡内基本医疗保险个人帐户中。

3.14 医疗消费(Medical Treatment Consume)

指持卡人就医、取药等与医疗有关的消费，从资金来源上划分，包括帐户支付、现金支付、统筹基金支付。卡内记录帐户支付、个人自付和统筹基金支付三种形式。

3.15 帐户支付(Account Payment)

指持卡人从卡内基本医疗保险个人帐户中支付医疗费用。

3.16 个人自付(Individual Payment)

指持卡人在医疗消费中，属于基本医疗保险统筹基金支付范围内的个人自付部分，包括现金支付和利用基本医疗保险个人帐户支付的金额。

3.17 统筹基金支付(Social-pooling Fund Payment)

指持卡人在医疗消费中，基本医疗保险统筹基金支付的金额。

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)
CIA	卡内医疗保险个人帐户(Individual Account for Medical Treatment on Card)
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)

MAC	报文鉴别代码（Message Authentication Code）
MF	主控文件(Master File)
PIN	个人密码(Personal Identification Number)
RID	已注册的应用提供者标识(Registered Application Provider Identifier)
SSSE	社会保障系统环境(Social Security System Environment)
TAC	交易验证码(Transaction Authorization Cryptogram)
‘0’-‘9’ ‘A’-‘F’	十六进制数字
xx	任意值

5 社会保障应用

社会保障卡应用可以同时支持本规范规定的所有专业应用，也可以只支持其中的某几项。

本规范适用于就业与失业、社会保险应用。

本规范支持医疗保险采用联网处理和脱网处理两种方式。

本规范准许发卡方在上述应用的基础上扩充其他应用。

卡内应用的扩充规则，参见本文第 6.7 部分。

5.1 标识符和标签

表 1 社会保障系统环境 SSSE 的应用标识符如下表所示。

表 1 社会保障系统环境 SSSE 的应用标识符

DDF	应用标识符内容	应用标识符
SSSE	sx1.sh.社会保障	7378312E73682EC9E7BBE1B1A3D5CF

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（如本规范附录 A 中定义的应用）则采用规定的应用标签，并通过应用标签选择该应用。

表 2 规定了社会保障应用应用标识符和应用标签。

表 2 社会保障应用的应用标识符和应用标签

应用名称	应用标识符	应用标签
公共应用	D1 56 00 00 05 00	公共应用信息区
就业与失业应用	D1 56 00 00 05 01	就业与失业信息区
社会保险应用 1	D1 56 00 00 05 02	社会保险信息区 1
社会保险应用 2	D1 56 00 00 05 03	社会保险信息区 2

5.2 安全数据

表 3 描述了存储在社会保障卡上用于社会保障应用的密钥。

表 3　IC 卡中存储的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	发卡方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
	STK_{DF01}		公共应用
	STK_{DF02}		就业与失业应用
	STK_{DF03}		社会保险应用 1
	STK_{DF04}		社会保险应用 2
卡片或应用锁定控制密钥	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
	LK_{DF03}		社会保险应用 1
	LK_{DF04}		社会保险应用 2
应用数据更新密钥	UK_{MF}	发卡方或应用提供方控制应用数据更新操作的密钥	发卡方和持卡人基本信息
	$UK1_{DF01}$		户籍信息
	$UK2_{DF01}$		个人状况信息、就业单位信息
	$UK3_{DF01}$		婚姻状况信息
	$UK4_{DF01}$		通讯信息
	$UK5_{DF01}$		工资信息
	$UK1_{DF02}$		职业和专业技能信息
	$UK2_{DF02}$		就业与失业信息
	$UK3_{DF02}$		就业记录
	$UK1_{DF03}$		失业保险信息
	$UK2_{DF03}$		丧失劳动能力鉴定信息
	$UK3_{DF03}$		养老保险信息
	$UK4_{DF03}$		工伤保险信息
	$UK5_{DF03}$		生育保险信息
	$UK6_{DF03}$		新农保信息
	$UK1_{DF04}$		城镇职工医疗保险基本信息（联网、脱网）
	$UK2_{DF04}$		医疗保险帐户信息（联网）
	$UK3_{DF04}$		城镇居民医疗保险信息
医疗保险交易密钥（脱网）	DLK	用来产生帐户划入交易中使用的过程密钥(SESLK)，在帐户划入交易中计算 MAC	医疗保险帐户划入交易（脱网）
	DPK	用来产生医疗消费中使用的过程密钥(SESPK)，在医疗消费交易中计算 MAC	医疗保险医疗消费交易（脱网）
	DTK	用来产生帐户支付、个人自付和统筹基金支付交易中使用的 TAC	医疗保险交易（脱网）

续表

分类	密钥	用途	适用的应用范围
应用数据读取密钥	$RK1_{DF03}$	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
	$RK2_{DF03}$		失业保险信息
	$RK3_{DF03}$		工伤保险信息
	$RK4_{DF03}$		生育保险信息
	$RK5_{DF03}$		新农保信息
	$RK1_{DF04}$		医疗保险帐户信息（联网）

6 社会保障应用的文件结构

6.1 社会保障应用的文件结构

图 1 为社会保障卡文件结构。

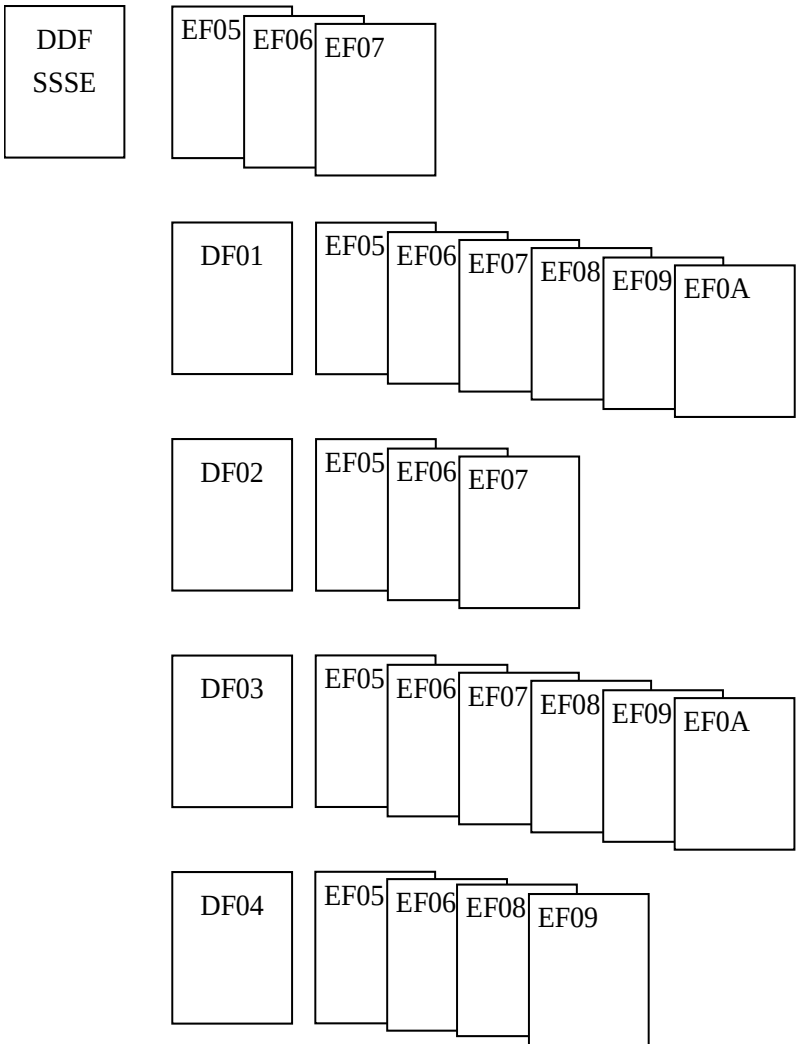

图 1 社会保障卡文件结构

6.2 基本应用数据区

基本应用数据是指那些在社会保障卡的整个生命周期中不会改变的信息，该区内包含发卡机构数据文件（‘EF05’）、持卡人的基本信息文件（‘EF06’）和指纹数据文件（‘EF07’）三个文件，它们被组织成基本文件存在于 SSSE 的 DDF 下。

表 4　基本应用数据区文件特性

文件定义	文件标识符	短文件标识符	读控制	写控制	文件结构	可选性
发卡机构数据文件	‘EF 05’	‘05’	无	UK_{MF}	变长记录	必选
持卡人的基本信息文件	‘EF 06’	‘06’	无	UK_{MF}	变长记录	必选
指纹数据文件	‘EF 07’	‘07’	无	UK_{MF}	透明	必选

6.3　公共应用数据区

公共应用数据是指社会保障卡中由不同的应用提供方分别维护，但各种专业应用都需要使用的信息，包括持卡人的户籍信息文件（‘EF 05’）、通讯信息文件（‘EF 06’）、个人状况信息文件（‘EF 07’）、婚姻状况信息文件（‘EF 08’）、就业单位信息文件（‘EF 09’）和工资信息文件（‘EF 0A’），它们被组织成基本文件存在于标识符为‘DF 01’的 DF 下。

表 5　公共应用数据区文件特性

文件定义	文件标识符	短文件标识符	读控制	写控制	文件结构	可选性
户籍信息文件	‘EF 05’	‘05’	PIN	$UK1_{DF01}$	变长记录	必选
通讯信息文件	‘EF 06’	‘06’	PIN	$UK4_{DF01}$	变长记录	可选
个人状况信息文件	‘EF 07’	‘07’	PIN 或 $UK2_{DF01}$	$UK2_{DF01}$	定长记录	必选
婚姻状况信息文件	‘EF 08’	‘08’	PIN	$UK3_{DF01}$	变长记录	必选
就业单位信息文件	‘EF 09’	‘09’	PIN 或 $UK2_{DF01}$	$UK2_{DF01}$	变长记录	必选
工资信息文件	‘EF 0A’	‘0A’	PIN	$UK5_{DF01}$	定长记录	必选

6.4　就业与失业数据区

就业与失业应用数据是指社会保障卡中由人力资源社会保障部门维护，记录持卡人就业、失业等情况的信息，包括持卡人的职业和专业技能信息文件（‘EF 05’）、就业与失业信息文件（‘EF 06’）、就业记录文件（‘EF 07’），它们被组织成基本文件存在于标识符为‘DF 02’的 DF 下。

表 6　就业与失业数据区文件特性

文件定义	文件标识符	短文件标识符	读控制	写控制	文件结构	可选性
职业和专业技能信息文件	‘EF 05’	‘05’	PIN 或 $UK1_{DF2}$	$UK1_{DF2}$	变长记录	可选
就业与失业信息文件	‘EF 06’	‘06’	PIN 或 $UK2_{DF2}$	$UK2_{DF2}$	变长记录	可选
就业记录文件	‘EF 07’	‘07’	PIN 或 $UK3_{DF2}$	$UK3_{DF2}$	循环	可选

6.5　社会保险数据区 1

本数据区中的应用数据是指社会保障卡中由人力资源社会保障部门维护，记录持卡人除医疗保险以外的各项社会保险的信息，包括失业保险信息文件（‘EF 05’）、丧失劳动能力鉴定信息文件（‘EF 06’） 、养老保险信息文件（‘EF 07’），工伤保险信息文件（‘EF 08’），生育保险信息文件（‘EF 09’），新农保信息文件（‘EF 0A’），它们被组织成基本文件存在于标识符为‘DF 03’的 DF 下。

表 7　社会保险数据区 1 文件特性

文件定义	文件标识符	短文件标识符	读控制	写控制	文件结构	可选性
失业保险信息文件	‘EF 05’	‘05’	PIN & $RK2_{DF03}$	$UK1_{DF03}$	变长记录	可选
丧失劳动能力鉴定信息文件	‘EF 06’	‘06’	PIN	$UK2_{DF03}$	变长记录	可选
养老保险信息文件	‘EF 07’	‘07’	PIN & $RK1_{DF03}$	$UK3_{DF03}$	变长记录	可选
工伤保险信息文件	EF 08	‘08’	（PIN & $RK3_{DF03}$）或 $UK4_{DF03}$	$UK4_{DF03}$	变长记录	可选
生育保险信息文件	EF 09	‘09’	（PIN & $RK4_{DF03}$）或 $UK5_{DF03}$	$UK5_{DF03}$	变长记录	可选
新农保信息文件	EF 0A	‘0A’	（PIN & $RK5_{DF03}$）或 $UK6_{DF03}$	$UK6_{DF03}$	变长记录	可选

6.6　社会保险数据区 2

本数据区中的应用数据是指社会保障卡中由医疗保险管理部门维护，记录持卡人医疗保险有关情况的信息。本规范定义的医疗保险应用包括两种模式：联网处理方式和脱网处理方式。医疗保险应用联网处理方式下存在三个文件：城镇职工医疗保险基本信息文件（‘EF 05’）、医疗保险帐户信息文件（‘EF 06’）和城镇居民医疗保险信息文件（‘EF 09’）。医疗保险应用脱网处理方式下存在四个文件：城镇职工医疗保险基本信息文件（‘EF 05’）、医疗保险金额文件（COS 内部操作文件）、医疗保险交易明细文件（‘EF 08’）和城镇居民医疗保险信息文件（‘EF 09’）。它们被组织成基本文件存在于标识符为‘DF 04’的 DF 下。

表 8　社会保险数据区 2 文件特性

文件定义	文件标识符	短文件标识符	读控制	写控制	文件结构	可选性
城镇职工医疗保险基本信息文件	‘EF 05’	‘05’	PIN	$UK1_{DF04}$	变长记录	可选
医疗保险帐户信息文件（联网处理方式下存在）	‘EF 06’	‘06’	PIN & $RK1_{DF04}$	$UK2_{DF04}$	定长记录	可选
医疗保险交易明细文件（脱网处理方式下存在）	‘EF 08’	‘08’	PIN	不允许改写	循环	可选
城镇居民医疗保险信息文件	‘EF 09’	‘09’	PIN	$UK3_{DF04}$	变长记录	可选

循环文件的结构应符合 ISO/IEC 7816-4。对循环文件中所有数据项的修改必须考虑数据完整性和安全要求。

6.7　卡内应用扩充规则

本部分给出了发卡地区在本规范的基础上扩充卡内应用时所需遵循的规则。

应用扩充包括文件的扩充和数据项的扩充。

6.7.1　基本原则

发卡地区在实际应用社会保障卡时，可以根据本地需求进行卡内应用的扩充或不扩充。

本规范中已经规定的 DF 文件标识符、EF 文件标识符、EF 文件内的数据项（包括规范规定的可选数据项）标志不允许更改、占用。发卡地区对于所选择的应用和数据项必须采用规范规定的标识符和标志。

6.7.2 DF 应用文件扩充规则

DF 文件可以扩充,扩充的 DF 文件标识符从‘DF0A’开始向后排列。

6.7.3 EF 基本文件扩充规则

SSSE 环境下和各 DF 文件下的 EF 文件可以扩充，扩充的 DF 文件标识符从‘EF0C’开始向后排列。