

社会保障“一卡通”应用技术规范

第 2 部分：卡内结构

Technical specifications for the application of social security cards
Part 2 : Card structure

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2023 – XX – XX 发布

2023 – XX – XX 实施

湖南省市场监督管理局 发 布

目 次

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 符号和缩略语 1

5 卡结构组成 2

 5.1 应用架构 2

 5.2 卡空间分配 2

 5.3 社会保障应用数据结构 2

 5.4 非对称认证应用 6

 5.5 一卡通公共服务应用数据结构 8

 5.6 金融环境数据结构 9

 5.7 交通环境数据结构 9

 5.8 校园卡应用数据结构 9

参考文献 10

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是DB43/T ***《社会保障一卡通应用技术规范》的第2部分。DB43/T ***已经发布以下部分：

- 第1部分：卡片；
- 第3部分：终端；
- 第4部分：应用系统接入规范。

本文件由湖南省社会保障卡服务中心提出。

本文件由湖南省人力资源和社会保障厅归口。

本文件起草单位：湖南省社会保障卡服务中心、湖南农业大学、长沙市人力资源和社会保障局、湘潭市人力资源和社会保障局、常德市人力资源和社会保障局、娄底市人力资源和社会保障局、华容县人力资源和社会保障局、衡南县人力资源和社会保障局、湖南正智标准咨询有限公司。

本文件主要起草人：吴意、刘辉、夏菁、卓辉、邓波、唐浩、罗毅辉、王云祥、陶星星、张弼、徐浩宇、李腾辉、刘春、刘伟、李胜、罗臣廷、李星星、许慧、雷雨亮、徐进、张伟、杨玲、吴敏、周怀洲。

社会保障“一卡通”应用技术规范

第 2 部分：卡内结构

1 范围

本部分规定了湖南省社会保障卡的卡内结构组成。
本部分适用于湖南省社会保障卡。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB/T 2260 中华人民共和国行政区划代码
- GB/T 2261.1 个人基本信息分类与代码 第1部分：人的性别代码
- GB/T 3304 中国各民族名称的罗马字母拼写法和代码
- GB/T 7408 数据元和交换格式 信息交换 日期和时间表示法 GB 11643 公民身份号
- GB/T 16649.4 识别卡 集成电路卡 第4部分：用于交换的结构、安全和命令
- GB/T 25056
- GM/T 0016 智能密码钥匙密码应用接口规范
- JR/T 0025 中国金融集成电路（IC）卡规范
- JT/T 978 城市公共交通IC卡技术规范
- LD/T 32 社会保障卡规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。[来源：GB/T 25056—2018，3.10]

3.2

公钥 public key

非对称密码算法中可公开的密钥。
[来源：GB/T 25056—2018，3.12]

4 符号和缩略语

下列符号和缩略语适用于本文件。

- ACSE 非对称认证系统环境 (asymmetric certification system environment)
- ADF 应用数据文件 (application data file)
- AID 应用标识符 (application identifier)
- EC 电子现金 (electronic purse)
- EF 基本文件 (elementary file)
- EP 电子钱包 (electronic cash)
- RID 已注册的应用提供者标识符 (registered application provider identifier)
- SSC 社会保障卡 (social security card)
- SSS 社会保障管理环境 (social security system)
- SSSE 社会保障系统环境 (social security system environment)
- PIN 个人密码 (personal identification number)
- PSE 支付系统环境 (Payment System Environment)
- PPSE 近距离支付系统环境 (Proximity Payment Systems Environment)
- PBOC 金融应用 (people (s) bank of china financial application)

5 卡结构组成

5.1 应用架构

湖南省社会保障卡卡结构由社会保障、金融、交通、校园等应用组成。卡片应用架构应符合图1的要求。

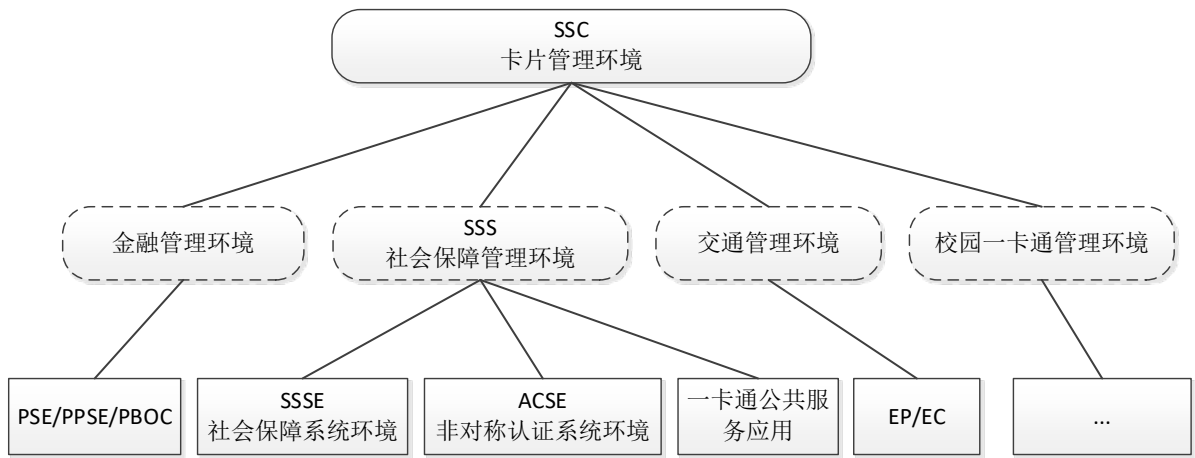


图1 卡片应用架构

5.2 卡空间分配

各应用的应用标识符 (AID)、空间分配、功能描述，应符合表1的要求。

5.3 社会保障应用数据结构

5.3.1 标识符和标签

社会保障系统环境的应用标识符应符合表2的要求。
社会保障应用的应用标识符和应用标签应符合表3的要求。

表1 卡片应用说明

应用名称	应用标识符（AID）	空间	功能说明
社会保障应用	7378312E73682EC9E7BBE1B1A3D5CF	24K	结合湖南本地需求的社保数据结构
非对称认证应用	504B492EC9E7BBE1B1A3D5CF	8K	标准的非对称认证应用
金融应用	315041592E5359532E4444463031（PSE）	16K	包含标准PBOC2018相关数据内容（根据银行要求支持UICS相关内容）
	325041592E5359532E4444463031（PPSE）		
	A000000333010101（PBOC）		
交通应用	325041592E5359532E4444463031（PPSE）	22K	交通部交通应用
	A000000632010105（EP）		
	A000000632010106（EC）		
校园应用	后续根据应用自定义	8K	校园一卡通
一卡通公共服务应用	D2BBBFA8CDA8B9ABB9B2B7FECEF1	32K	预留其他的各项公共服务应用

表2 社会保障系统环境的应用标识符

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

表3 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	公共应用数据区
就业与失业	D1 56 00 00 05 01	就业与失业数据区
社会保险1	D1 56 00 00 05 02	社会保险1数据区
社会保险2	D1 56 00 00 05 03	社会保险2数据区
人事与人才	D1 56 00 00 05 04	人事与人才数据区
生命与健康	D1 56 00 00 05 05	生命与健康数据区
社会救助与优待抚恤	D1 56 00 00 05 06	社会救助与优待抚恤数据区

5.3.2 基本应用数据区

基本应用数据区数据结构应符合LD/T 32的规定。

5.3.3 公共应用数据区

公共应用数据区数据结构应符合LD/T 32的规定。

5.3.4 就业与失业数据区

就业与失业数据区数据结构应符合LD/T 32的规定。

5.3.5 社会保险 1 数据区

社会保险1数据区数据结构应符合LD/T 32的规定。

5.3.6 社会保险 2 数据区

社会保险2数据区数据结构应符合LD/T 32的规定。

5.3.7 人事与人才数据区

人事与人才数据区数据结构应符合LD/T 32的规定。

5.3.8 生命与健康数据区

生命与健康应用数据区应符合表4、表5的要求。

表4 生命与健康文件特性

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	类别
生命与健康数据文件	‘EF05’	‘05’	自由	UK1 _{DF05}	变长记录	预设

表5 生命与健康文件数据格式

标志	数据项	类型	长度
‘A0’	健康状况	an	‘01’
‘A1’	残疾类别	an	‘01’
‘B9’	残疾等级	an	‘01’
‘A2’	ABO 血型代码	an	‘04’
‘A9’	RH 血型代码	cn	‘01’
‘A3’	禁忌药信息 1（见标志‘A5’—‘A6’）	B-TLV	‘18’
‘A3’	禁忌药信息 2（见标志‘A5’—‘A6’）	B-TLV	‘18’
‘A3’	禁忌药信息 3（见标志‘A5’—‘A6’）	B-TLV	‘18’
‘A3’	禁忌药信息 4（见标志‘A5’—‘A6’）	B-TLV	‘18’
‘A3’	禁忌药信息 5（见标志‘A5’—‘A6’）	B-TLV	‘18’
‘A5’	禁忌药	an	‘10’
‘A6’	禁忌药代码	an	‘04’
‘A4’	重大疾病信息 1（见标志‘A7’-‘A8’）	B-TLV	‘17’
‘A4’	重大疾病信息 2（见标志‘A7’-‘A8’）	B-TLV	‘17’
‘A4’	重大疾病信息 3（见标志‘A7’-‘A8’）	B-TLV	‘17’
‘A4’	重大疾病信息 4（见标志‘A7’-‘A8’）	B-TLV	‘17’
‘A4’	重大疾病信息 5（见标志‘A7’-‘A8’）	B-TLV	‘17’
‘A7’	重大疾病	an	‘10’
‘A8’	重大疾病代码	an	‘03’
‘BA’	过敏物质名称	an	‘14’
‘BB’	过敏反应	an	‘64’
‘AA’	免疫接种名称	an	‘14’
‘AB’	免疫接种时间	cn	‘04’
‘AC’	哮喘标志	an	‘01’
‘AD’	心脏病标志	an	‘01’

表 5（续）

标志	数据项	类型	长度
‘AE’	心脑血管标志	an	‘01’
‘AF’	癫痫病标志	an	‘01’
‘B0’	凝血紊乱标志	an	‘01’
‘B1’	糖尿病标志	an	‘01’
‘B2’	青光眼标志	an	‘01’
‘B3’	透析标志	an	‘01’
‘B4’	器官移植标志	an	‘01’
‘B5’	器官缺失标志	an	‘01’
‘B6’	可装卸的义肢标志	an	‘01’
‘B7’	心脏起搏器标志	an	‘01’
‘BC’	精神病标志	an	01
‘B8’	其他医学警示名称	an	‘28’

5.3.9 社会救助与优待抚恤数据区

社会救助与优待抚恤应用数据区应符合表6、表7的要求。

表6 社会救助与优待抚恤文件特性

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	类别
荣誉信息文件	‘EF05’	‘05’	RK1 _{DF07}	UK1 _{DF07}	变长记录	预设
专家信息文件	‘EF06’	‘06’	RK2 _{DF07}	UK2 _{DF07}	变长记录	预设
军队转业干部信息文件	‘EF07’	‘07’	RK3 _{DF07}	UK3 _{DF07}	变长记录	预设

表7 社会救助与优待抚恤文件数据格式

标志	数据项	类型	长度	所属文件
‘C0’	救助金发放机构名称	an	‘46’	‘DF06’ ‘EF05’
‘C2’	救助金发放机构代码	an	‘09’	
‘C3’	社会救助信息 1（见标志‘E3’-‘E7’）	B-TLV	‘1A’	
‘C4’	社会救助信息 2（见标志‘E3’-‘E7’）	B-TLV	‘1A’	
‘C5’	社会救助信息 3（见标志‘E3’-‘E7’）	B-TLV	‘1A’	
‘E3’	社会救助代码	cn	‘01’	
‘E4’	社会救助批准日期	cn	‘04’	
‘E5’	社会救助复核日期	cn	‘04’	
‘E6’	最近一次获得社会救助的金额	cn	‘04’	
‘E7’	社会救助已发放月度	cn	‘03’	

表 7（续）

标志	数据项	类型	长度	所属文件
‘C6’	优待抚恤金发放机构	an	‘46’	‘DF06’ ‘EF06’
‘C8’	优待抚恤金发放机构代码	an	‘09’	
‘C9’	优待抚恤代码 1	cn	‘01’	
‘CA’	优待抚恤批准日期 1	cn	‘04’	
‘CB’	优待抚恤截止日期 1	cn	‘04’	
‘CC’	当年义务兵优待金发放标准	cn	‘04’	
‘CD’	优待抚恤已发放年度 1	cn	‘02’	
‘CE’	优待抚恤代码 2	cn	‘01’	
‘CF’	优待抚恤批准日期 2	cn	‘04’	
‘D0’	优待抚恤截止日期 2	cn	‘04’	
‘D1’	当年定期抚恤金发放标准	cn	‘04’	
‘D2’	优待抚恤已发放月度 2	cn	‘03’	
‘D3’	优待抚恤代码 3	cn	‘01’	
‘D4’	优待抚恤批准日期 3	cn	‘04’	
‘D5’	优待抚恤截止日期 3	cn	‘04’	
‘D6’	当年定期补助发放标准	cn	‘04’	
‘D7’	优待抚恤已发放月度 3	cn	‘03’	
‘D8’	优待抚恤代码 4	cn	‘01’	
‘D9’	优待抚恤批准日期 4	cn	‘04’	
‘DA’	优待抚恤截止日期 4	cn	‘04’	
‘DB’	当年抚恤金标准（中央）	cn	‘04’	
‘DC’	当年抚恤金补助标准（地方）	cn	‘04’	
‘DD’	当年保健金标准（中央）	cn	‘04’	
‘DE’	当年保健金补助标准（地方）	cn	‘04’	
‘DF’	伤残抚恤金已发放月度	cn	‘03’	
‘E0’	伤残抚恤补助金已发放月度	cn	‘03’	
‘E1’	伤残保健金已发放年度	cn	‘02’	
‘E2’	伤残保健补助金已发放年度	cn	‘02’	

5.4 非对称认证应用

5.4.1 标识和标签

5.4.1.1 非对称认证系统环境的应用标识符，应符合表 8 的要求。

表8 非对称认证系统环境的应用标识符

应用名称	应用标识符内容	应用标识符
ACSE	PKI.社会保障	504B492EC9E7BBE1B1A3D5CF

5.4.1.2 非对称认证系统环境的文件结构以 GM/T 0016 中定义的应用逻辑结构为基础,示意图见图 2,可根据实际情况进行扩展,如增加应用、容器或临时加解密公私钥等。

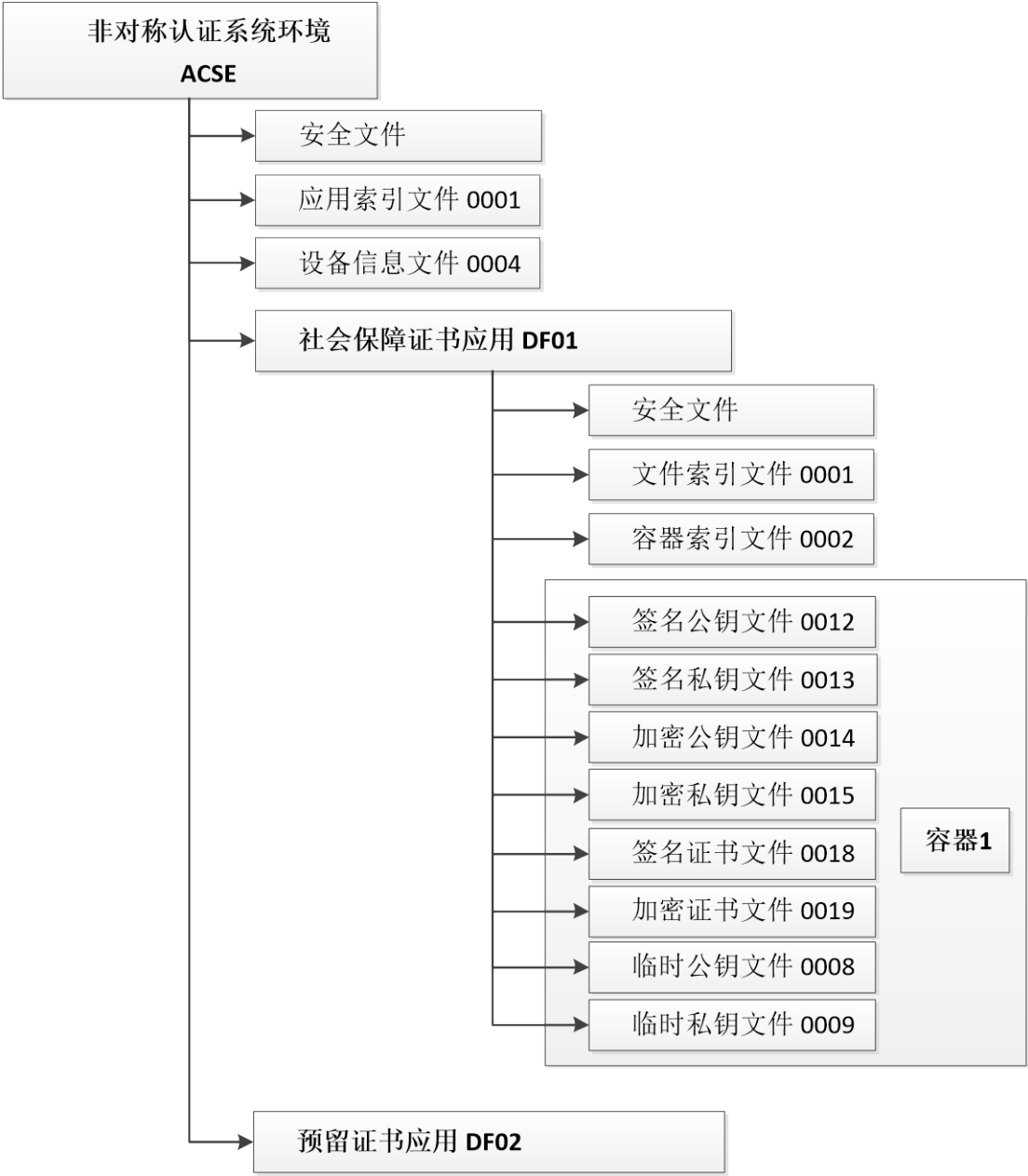


图2 非对称认证系统环境文件结构示意图

5.4.1.3 非对称认证应用的文件特性应符合表 9 的要求,表中 PIN 为当前目录下的用户 PIN, PIN 标识符为 01, ‘0018’ 和 ‘0019’ 文件大小分别为 1K。

表9 非对称认证应用的文件特性

数据区	文件标识	文件内容	文件结构	读控制	写控制	使用
非对称认证系统环境ACSE	'0001'	应用索引文件	定长记录	无	MKACSE	/
	'0004'	设备信息文件	透明	无	MKACSE	/
社会保障证书应用DF01	'0001'	文件索引文件	定长记录	无	MKDF01	/
	'0002'	容器索引文件	定长记录	无	MKDF01	/
容器1	'0012'	签名公钥文件	内部	无	PIN	无
	'0013'	签名私钥文件	内部	不允许读	PIN	PIN
	'0014'	加密公钥文件	内部	无	PIN	无
	'0015'	加密私钥文件	内部	不允许读	PIN	PIN
	'0018'	签名证书文件	透明	无	PIN	/
	'0019'	加密证书文件	透明	无	PIN	/
	'0008'	临时公钥文件	内部	无	PIN	无
	'0009'	临时私钥文件	内部	不允许读	PIN	PIN

5.4.2 非对称认证系统环境（ACSE）

5.4.2.1 应用索引文件

应用索引文件数据格式应符合表10的要求。

“应用名称1”为社会保障证书应用名称“SS.CERT.ADF1”，“应用名称2”为预留证书应用名称，命名规则按照“RFU.CERT.ADF2”。

表10 应用索引文件数据格式

标志	数据项	类型	长度
01	应用名称 1	/	'10'
01	应用名称 2	/	'10'

5.4.2.2 设备信息文件

设备信息文件数据格式应符合表11的要求，分组密码算法标识为 0x00000413，非对称密码算法标识为 0x00020500，密码杂凑算法标识为 0x00000001，设备认证使用的分组密码算法标识为 0x00000401。

5.4.2.3 文件索引文件

文件索引文件数据格式应符合表12的要求。共有8条记录。

5.4.2.4 容器索引文件

容器索引文件数据格式应符合表13的要求，容器名称为“SS.CERT.CONTAINER”，容器类型为“0x02”，标识SM2算法。

5.5 一卡通公共服务应用数据结构

一卡通公共服务应用环境的应用标识符，应符合表14要求。

表11 设备信息文件数据格式

起始位置	数据项	类型	长度
‘0000’	设备标签	an	‘20’
‘0020’	序列号	an	‘20’
‘0040’	分组密码算法标识	b	‘4’
‘0044’	非对称密码算法标识	b	‘4’
‘0048’	密码杂凑算法标识	b	‘4’
‘004C’	设备认证使用的分组密码算法标识	b	‘4’
‘0050’	预留数据	b	‘40’

表12 文件索引文件数据格式

标志	数据项	类型	长度
02	文件1信息	—	‘2E’
‘A1’	文件FID	b	‘02’
‘A2’	文件名称	an	‘10’
‘A3’	空间大小	b	‘02’
‘A4’	读权限	b	‘01’
‘A5’	写权限	b	‘01’
‘A6’	使用权限	b	‘01’
‘A7’	预留	b	‘09’

表13 容器索引文件数据格式

标志	数据项	类型	长度
03	容器信息	—	‘45’
‘A8’	容器名称	an	‘40’
‘A9’	容器类型	b	‘01’

表14 一卡通公共服务应用环境的应用标识符

应用标识符内容	应用标识符
一卡通公共服务应用	D2BBBFA8CDA8B9ABB9B2B7FECEF1

5.6 金融环境数据结构

金融应用应符合JR/T 0025的要求。根据各发卡机构的数据结构要求，支持借贷记、小额支付和小额支付扩展应用等金融支付功能。

5.7 交通环境数据结构

交通应用应符合JT/T 978的要求。

5.8 校园卡应用数据结构

校园卡应用，按照各学校自身要求，制定满足要求的校园卡应用数据结构，支持相关功能。

参 考 文 献

- [1] 《关于印发社会保障卡文件结构和数据项（V2.0）的通知》（人社信息函[2012]37号）
 - [2] 《中国人民银行办公厅 人力资源社会保障部办公厅关于印发具有金融功能的第三代社会保障卡技术规范的通知》（银办发〔2017〕170号）
 - [3] 《关于印发第三代社会保障卡相关技术规范的通知》（人社网信函〔2018〕1 号）
-