第 3 章　IC 卡信息编码(数据元、数据对象和文件)

IC 卡的流通范围很广,如银行卡,可以在国内或国际范围内流通;交通卡可以在一个城市或跨区域范围内使用。为了便于识别、阅读和检索 IC 卡中存放的各种信息(数据),从而制定了编码规则。按各种数据的内容、性质或用途的不同,对其进行分析、划分归类,给出不同的标记,并纳入国际标准中,以促进 IC 卡的流通使用。

在 IC 卡中存储的信息可归纳为数据元、数据对象和文件 3 种。

在 IC 卡和读写器之间的接口处所见到的最小信息项(诸如一个名称、逻辑描述符、格式编码等)称为数据元(Data Element,DE),而在接口处所见到的由标记 T(Tag)、长度 L(Length)和数值 V(Value)字段组成的信息称为数据对象(Data Object,DO)。在 IC 卡中,数据对象一般按照国际标准 ISO/IEC 8825-1 中定义的基本编码规则(Basic Encoding Rules,BER)进行编码,该标准是"抽象语法记法 1(ASN.1)"编码规则的第 1 部分。

文件是基于一项或多项应用而设置的,存放控制信息和应用数据。

3.1　ASN.1 的基本编码规则

3.1.1　编码结构(BER-TLV)

数据对象 DO 的编码由标记 T、长度 L 和数值 V 三部分组成,其中标记和长度是为了解释数值部分而引入的。每部分由一个或若干个字节组成,每个字节包含 8 位二进制数 $b_8 \sim b_1$,b_8 为最高位,b_1 为最低位。

标记 T	长度 L	数值 V

1. 标记 T

由一个或多个字节组成,首个 8 位字节安排如下(图 3.1)。

(1) b_8、b_7 表示标记类别,$b_8b_7=00$ 为通用类,$b_8b_7=01$ 为应用类,$b_8b_7=10$ 为上下文相关类,$b_8b_7=11$ 为专用类。

(2) b_6 表示编码类别,$b_6=0$ 为原始编码 P,$b_6=1$ 为结构化编码 C。

(3) $b_5 \sim b_1$ 为标记编号,如果编号范围在 0～30(二进制 0000～11110)以内,则表示标记 T 为 1 个字节(图 3.1);如果 $b_5 \sim b_1=11111$,则表示标记 T 为多个字节,其编号不小于 31。当后继字节的 b_8 为 1 时,表示后面还有后继字节;b_8 为 0 时,表示该字节是 T 的最后一个字节(图 3.2)。标记的编号由后继字节的 $b_7 \sim b_1$ 链接而成。

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1
标记类		P/C	标记编号				

图 3.1　标记 T(编号 0～30)

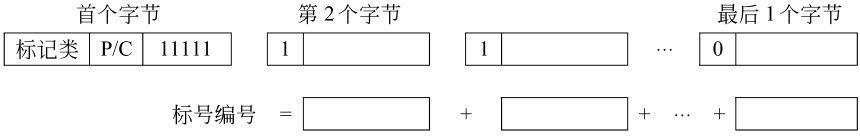


图 3.2　标记 T(编号由多个字节组成)

由此得出数据对象的 4 种标记类别的编码范围如表 3.1 所示。

表 3.1　数据对象的 4 种标记类别的编码范围(T 由 1 个字节组成)

b_8 b_7 类别	b_8～b_1 编码范围(十六进制表示,×为任意值)	
00 通用类	'0×'～'1×'(原始编码)	'2×'～'3×'(结构化编码)
01 应用类	'4×'～'5×'(原始编码)	'6×'～'7×'(结构化编码)
10 上下文相关类	'8×'～'9×'(原始编码)	'A×'～'B×'(结构化编码)
11 专用类	'C×'～'D×'(原始编码)	'E×'～'F×'(结构化编码)

在本章中还用数据下标表示进位制。

2. 长度 L

由 1 个或多个字节组成。如果 L 的首个字节的 $b_8=0$,则 L 的长度为 1 个字节,b_7～b_1 表示数值 V 的字节数(≤127);如果 $b_8=1$,则 L 的长度为多个字节,b_7～b_1 表示后继长度的字节数,后继长度字节的内容为数值 V 的字节数。

L 的首个字节不使用 FF,FF 供将来扩展使用。

例如:

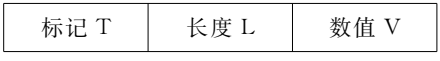
(1) $L=33_{10}$(十进制数 33),b_8～b_1 编码为 00100001_2,$b_8=0$,L 的长度为 1 个字节。

(2) $L=201_{10}$,编码为 10000001_2 11001001_2,首个字节的 $b_8=1$,表示长度由多个字节组成;b_7～$b_1=0000001$,表示 L 后继字节的长度为 1。第 2 个字节为数值 V 的字节数 201_{10}($2^7+2^6+2^3+2^0=128+64+8+1=201_{10}$)。

3. 数值 V

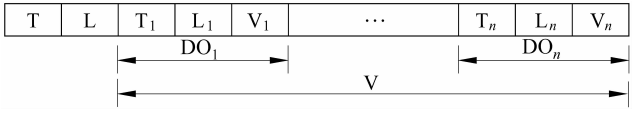
由 0 个、1 个或多个字节组成,有两种编码方式:DO 的原始编码和结构化编码。这两种编码的主要差别是 V 字段的表示方法不同。

(1) 原始编码格式:



前面介绍的编码格式即是原始编码格式。

(2) 结构化编码格式:



其中,T 为标记,L 为 V 字段的长度,而 V 字段则是由一个或多个数据对象组成,被称为 T 的模板(template)。在模板中:

T_1、…或 T_n＝DO_1、…或 DO_n 的标记。

L_1、…或 L_n＝DO_1、…或 DO_n 的长度。

V_1、…或 V_n＝DO_1、…或 DO_n 的数值。

用 TLV 来描述数据对象，可以完整地表示出数值的含义、值的大小以及数据对象长度。而且 TLV 的总字数可从其本身算出来。

在 IC 卡领域内，广泛采用 TLV 表达形式，当采用结构化编码格式，有多个数据对象链接时，数据对象之间可以不用分隔符(或称为定界符)。

3.1.2 通用类编码

通用类的编码在 ASN.1 编码规则中定义，应用类、上下文相关类和专用类与应用的场合有关，在其他相应的标准中定义。

下面将介绍一部分通用类编码，其中已确定编号的标记 T 具有唯一性，不能再进行其他定义。

1. 布尔值

原始编码：$T=01_{16}$。如果布尔值为假(false)，数值应为 0；如果布尔值为真(true)，数值应为任意非 0 值，如下所示(在本例中，用 FF 表示非 0 值)。

标记 T(布尔)	长度	数值
01_{16}	01_{16}	FF_{16}

十六进制数据 1 位相当于二进制数据 4 位，在 IC 卡中一般定义为 1 个数据单元，1 个字节包含 2 个数据单元。

在上例中，$T=01_{16}=\begin{matrix}b_8&b_7&b_6&b_5&b_4&b_3&b_2&b_1\\0&0&0&0&0&0&0&1_2\end{matrix}$，其中 $b_8b_7=00$，属于通用类，$b_6=0$ 为原始编码，$b_5\cdots b_1=00001_2$，其值在 0～30 之内，因此 T 为 1 个字节。长度 L 和数值各为 1 个字节。所以该数据对象的总字数为 3 个字节。

2. 位串值

原始编码：$T=03_{16}$；结构化编码：$T=23_{16}$。

若有位串值 $0A3B5F291CD_{16}$，可采用原始编码或结构化编码，如图 3.3 所示。

在图 3.3 中，数值部分的第一个字节表示最后一个字节未被使用的二进制位数，其范围为0～7 位。在图 3.3(a)中，第一字节为 04，表示最后一个 0 无用。在图 3.3(b)中位串值为 2 个 DO 链接，第一个 DO 的第一字节为 00，表示没有无用位；第二个 DO 的第一字节为 04，表示最后一个 0 无用。

如果位串为空，则数值部分仅有一个字节 00，没有后继字节。

3. 空值

原始编码：$T=05_{16}$，$L=00_{16}$，没有数值字段。

4. 序列值

结构化编码：$T=30_{16}$。

T（位串）	长度L	数值V
03_{16}	07_{16}	$040A3B5F291CD0_{16}$

(a) 原始编码

T（位串）	长度L	数值V		
		位串	长度	数值
23_{16}	$0C_{16}$	03_{16}	03_{16}	$000A3B_{16}$
		03_{16}	05_{16}	$045F291CD0_{16}$

(b) 结构化编码

图 3.3　位串值的编码

例如，要求顺序列出两个数据对象：名字 Smith 和布尔值为真，可编码如图 3.4 所示。

T（序列）	长度	数值		
30_{16}	$0A_{16}$	T（名字）	长度	数值
		16_{16}	05_{16}	Smith
		T（布尔）	长度	数值
		01_{16}	01_{16}	FF_{16}

图 3.4　序列值的编码

注：一个字节可表示二位十六进制数据(0～9，A～F)或一个英文字母(A～Z)。

5. 对象标识符

原始编码：$T=06_{16}$。

数值部分是链接的多个子标识符的编码。每个子标识符由一个或多个字节组成，每个字节的最高位指示它是否为该子标识符的最后一个字节，若是，$b_8=0$；若不是，$b_8=1$。子标识符由上述这些字节的 b_7～b_1 链接起来而形成的一个无符号的二进制数，其最高位是第一个字节的 b_7，最低位是最后一个字节的 b_1。

例如，ISO 9992-2 的 DO 是 06 04 28 CE 08 02。其中，06 是标记 T，04 是长度 L，28(十进制 40)为子标识符 ISO 的编码，CE 08 是子标识符 9992 的编码，02 是子标识符 2，28CE0802 构成 DO 的数值部分。

下面讨论如何从 9992_{10} 转换成 $CE08_{16}$。

根据计算，$9992_{10}=2708_{16}$，二进制值为 0010 0111 0000 1000，按 7 位分段，得 1001110 0001000，所以该子标识符由两个字节构成，第一个字节的最高位补充 1，第二个字节的最高位补充 0，最后得 11001110 00001000，等于 $CE08_{16}$。

3.2　IC 卡使用的数据对象

在 IC 卡和读写器之间的界面上所见到的数据对象在国际标准中又称为行业间数据对象(Interindustry Data Object，IDO)。在本章中仍简称为 DO。

3.2.1　数据对象的格式

IC 卡中的 DO，一般是用 Simple-TLV 和 BER-TLV 描述的两种 DO。

1）Simple-TLV 数据对象

- T 字段：由 1 个字节组成。编码范围为 1～254，'00'和'FF'为无效编码。
- L 字段：如果由 1 个字节组成，编码范围为 1～254，以 N 表示。如果第 1 个字节是'FF'，则 L 字段由 3 个字节组成，后继的 2 个字节表示数值字段长度，范围为 0～65 535，也以 N 表示。
- V 字段：如果 L 字段的 $N=0$，不存在数值字段，这是一个空值 DO；如果 $N>0$，数值字段由 N 个字节组成。

在 IC 卡的文件组织中，可以用 Simple-TLV 数据对象来描述一个记录。

2）BER-TLV 数据对象

上节中描述的 BER-TLV 同样适用于此。有两种 DO 编码：原始编码和结构化编码。

在国际标准 ISO/IEC 7816 中，数据元一般出现在数据对象 DO 的数值字段中或不用标记也能表达其含义的场合。

3.2.2 数据对象的标记分配

在 ISO/IEC 7816 中汇总了某些在 IC 卡中使用的 ASN.1—BER 应用类标记 DO（原始编码 4×、5×和结构化编码 6×、7×）。随着时间的推移和使用范围的扩大，肯定会有新的编码补充进来。

在 ISO/IEC 7816-4 中还定义了上下文相关类标记（8×、9×、A×、B×），这主要在本书的第 6 章中讨论。专用类标记尚未涉及。

表 3.2 给出了按标记数字次序排列的数据对象 DO（资料来源：ISO/IEC 7816-6）。标记与模板均为十六进制。在表中仅有一个通用类 DO，标记为 06。其他均为 IC 卡应用类数据对象（不适用于其他行业）。

表 3.2 按数字次序排列的 DO

标记	数据元名称	引 用 标 准	长度	可引用的模板
06	对象标识符	ISO 8825-1	可变	—
41	国家机构	ISO/IEC 7816-6	可变	—
42	卡发行者机构	ISO/IEC 7816-4	可变	—
43	卡服务数据	ISO/IEC 7816-4	1 个字节	—
44	初始访问数据	ISO/IEC 7816-4	可变	66
45	卡发行者数据	ISO/IEC 7816-4	可变	66
46	预先发行的数据	专有	可变	66
47	卡能力	ISO/IEC 7816-4	可变	66
48	状态信息	ISO/IEC 7816-4	1、2、3 个字节	—
4F	应用标识符	ISO/IEC 7816-5	可变	61/6E

续表

标记	数据元名称	引 用 标 准	长度	可引用的模板
50	应用标号	ISO/IEC 7816-5	可变	61/6E
51	路径	ISO/IEC 7816-4	可变	61
52	执行的命令	ISO/IEC 7816-4	可变	61
53	自由选择的数据	ISO/IEC 7816-4/5	可变	*
56	磁道 1(应用)	ISO/IEC 7813,ISO 8583	*ans*…76	6E
57	磁道 2(应用)	ISO/IEC 7813,ISO 8583	*n*…37	6E
58	磁道 3(应用)	ISO 4909,ISO 8583	*n*…104	6E
59	卡终止日期	—	*n*4	66
5A	主账号(PAN)	ISO/IEC 7813,ISO 8583	*n*…19	6E
5B	姓名	ISO/IEC 7501-1	可变	65
5C	标记列表	ISO/IEC 7816-4	可变	—
5D	首标列表	ISO/IEC 7816-4	可变	—
5E	登录数据(专有的)	专有	可变	6E
5F20	持卡者姓名	ISO/IEC 7813	*n*2…*n*6	65
5F21	磁道 1(卡)	ISO/IEC 7813,ISO 8583	*ans*…76	66
5F22	磁道 2(卡)	ISO/IEC 7813,ISO 8583	*n*…37	66
5F23	磁道 3(卡)	ISO/IEC 7813,ISO 8583	*n*…104	66
5F24	应用终止日期	—	*n*6	6E
5F25	应用生效日期	—	*n*6	6E
5F26	卡生效日期	—	*n*6	66
5F27	交换控制	ISO 4909	*n*1	66
5F28	国家代码	ISO 3166	*n*3	66
5F29	交换轮廓	—	待定义	67
5F2A	货币代码	ISO 4217	*a*3 或 *n*3	6E
5F2B	出生日期	—	*n*8	65
5F2C	持卡者国籍	ISO 3166	*n*3	65
5F2D	语言优先权	ISO 639	*a*2…*a*8	65
5F2E	持卡者生物统计数据	—	可变	65
5F2F	PIN 使用政策	ISO/IEC 7816-6	2 个字节	6E
5F30	服务代码	ISO/IEC 7813,ISO 8583	*n*3	6E
5F32	交易计数器	—	可变	6E
5F33	交易日期	—	*n*4 或 *n*10	6E
5F34	卡顺序号	—	*n*2	66
5F35	性别	ISO 5218	1 个字节	65

续表

标记	数据元名称	引 用 标 准	长度	可引用的模板
5F36	货币基本单位	ISO 4217	*n*1	6E
5F37	静态内部鉴别(一个步骤)	—	待定义	67
5F38	静态内部鉴别-第 1 个相关联的数据	—	待定义	67
5F39	静态内部鉴别-第 2 个相关联的数据	—	待定义	67
5F3A	动态内部鉴别	—	待定义	67
5F3B	动态外部鉴别	—	待定义	67
5F3C	动态相互鉴别	—	待定义	67
5F40	持卡者相片	—	*n*1	6C
5F41	元素列表	—	可变	—
5F42	地址	—	可变	65
5F43	持卡者手写体签名图像	ISO/IEC 11544	可变	6C
5F44	应用图像	ISO/IEC 10918-1	可变	6D
5F45	显示报文	—	可变	66
5F46	定时器	—	2 个字节	66
5F47	报文引用	—	可变	66
5F48	持卡者秘密密钥	—	可变	65
5F49	持卡者公开密钥	—	可变	65
5F4A	认证机构的公开密钥	—	可变	65
62	FCP 模板	ISO/IEC 7816-4	可变	—
63	封套	ISO/IEC 7816-4	可变	—
64	FMD 模板	ISO/IEC 7816-4	可变	—
68	特定用户要求	—	可变	65
6A	登录模板	—	可变	6E
6B	受限定的姓名	—	可变	65
6C	持卡者图像模板	—	可变	65
6D	应用图像模板	ISO/IEC 10918-1	可变	6E
6F	FCI 模板	ISO/IEC 7816-4	可变	—
73	自由选择的数据	ISO/IEC 7816-4	可变	*
78	兼容标记分配机构	—	可变	—
79	共存标记分配机构	—	可变	—
7D	安全报文模板	—	可变	—
7F20	显示控制	—	可变	66
7F21	持卡者证明书	—	可变	65

* ：本表中定义的所有模板。

表中的符号所表示的意义如下。

- a：字母字符。
- n：数字，BCD 编码（二进制编码的十进制数）。
- s：专用字符。
- …：在两个数之间表示值的范围。

例如：

$a3$ 表示 3 个字母字符。

n…3 表示最多 3 个 BCD 码。

$n2$…4 表示 2，3 或 4 个 BCD 码。

表 3.2 中的标记由 1 个或 2 个字节组成，如果第 1 个字节的 $b_5 \sim b_1$ 为 11111（表中的 5F），则表示标记为 2 个字节。

表 3.2 中提及的模板标记有 61、65、66、67、6C、6D、6E。

其对应的数据如下。

标记 61——应用模板。

标记 65——与持卡者相关的数据。

标记 66——卡数据。

标记 67——鉴别数据。

标记 6E——与应用相关数据。

另外，6C 和 6D 可分别编于标记为 65 与 6E 的模板中。例如，在标记为 61 的结构化 DO 模板中，可包含表 3.3 列出的内容，该表是根据表 3.2 列出的。同样，可列出标记为 65、66…的模板。

表 3.3　应用模板——标记 61

标记	长度	数　据　元	标记	长度	数　据　元
4F	可变	应用标识符	53	可变	自由选择的数据
50	可变	应用标号	73	可变	自由选择的 DO
52	可变	执行的命令	51	可变	路径

上下文相关类数据对象将在 3.3 节中讨论。

3.2.3　编码举例

（1）表示卡终止日期为 1995 年 2 月的 DO：

$$\frac{59}{\text{T}}\quad\frac{02}{\text{L}}\quad\frac{95\ 02}{\text{V}}$$

（2）表示应用终止日期为 1997 年 3 月 31 日的 DO：

$$\frac{5\text{F}\ 24}{\text{T}}\quad\frac{03}{\text{L}}\quad\frac{97\ 03\ 31}{\text{V}}$$

（3）表示个人出生日期的 DO：

$$\frac{5\text{F}\ 2\text{B}}{\text{T}}\quad\frac{04}{\text{L}}\quad\frac{\text{YYYYMMDD}}{\text{V}}$$

（Y：年；M：月；D：日）

注意：上述 3 例数值字段 V 的编码方法与 3.1.2 小节介绍的通用类编码方法不同，

因此在使用到在本书中尚未讨论过的标记时，要查阅有关资料。

(4) 结构化的 DO 的举例。

61	0D	4F	05	D××××××××××	53	04	×× ×× ×× ××
T	L	T_1	L_1	V_1	T_2	L_2	V_2

标记 61 为应用模板，结构化 DO 中有两个原始编码；DO 分别是国家注册的应用标识符 AID4F(5 字节)和自由选择数据标识符 53(4 字节)。

(5) 其他编码形式。

在 IC 卡中，某些数据元并不按 TLV 形式编码，如第 4 章中所讨论的复位应答、第 6 章中的命令编码等。由于它们出现在特定时间或场合，并由相关的国际标准予以详细的定义，不会产生二义性。

3.3 IC 卡的文件系统

3.3.1 文件的种类

文件用于管理应用和存储数据。

IC 支持两种文件：专用文件(Dedicated File，DF)和基本文件(Elementary File，EF)。

(1) 专用文件。用于主持应用和有层次结构的文件。一个“应用 DF”(application DF)对应一种应用。“应用 DF”可以作为其他文件的父文件(是上层的文件)，而其下层的文件被称为该 DF 的直属文件(可以是 DF 和 EF)。

(2) 基本文件。用于存放数据。EF 文件不能作为其他文件的父文件。EF 分为如下两类。

① 内部 EF：用于存储由卡所解释的数据，即为了管理和控制目的由卡内操作系统所分析和使用的数据。

② 工作的 EF：主要存储外界可使用的数据以及卡与读写器之间可相互传输的数据。

ISO/IEC 7816 提供如下两种逻辑组织方式。

(1) 图 3.5 所示为包含对应安全架构的 DF 层次结构。在这种卡的组织结构中，处于根部的 DF 称为主文件(Master File，MF)。所有 DF 可以是应用 DF，也可以有其下层的 DF 和 EF。

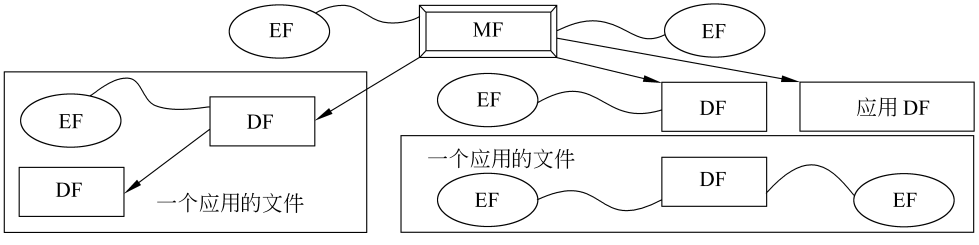


图 3.5　DF 层次结构示例

(2) 图 3.6 所示为平行结构的应用 DF，且没有 MF。该组织结构支持多个卡内的独立应用，在这些独立应用中的“应用 DF”可以包含其 DF 层次和对应安全结构，也可以有其下层的 DF 和 EF。

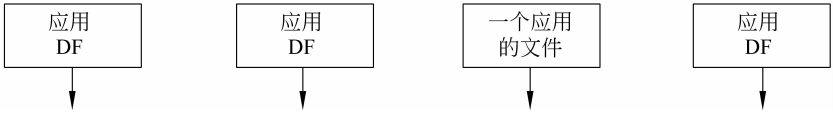


图 3.6　独立应用 DF 示例

3.3.2　结构选择方法、数据引用方法和文件控制信息

1. 结构选择方法

选择了一个结构，则可以访问其数据，如果是 DF 结构，则可以访问其子结构(下层)。结构选择可以是隐式实现，如 IC 卡加电复位后自动进行协议和参数的选择。如果一个结构不能被隐式选择，则应进行显式选择，可利用以下 4 种方式之一来选择文件。

(1) 通过 DF 名称选择。任何 DF 都可以通过按 1～16 个字节编码的 DF 名来选择。任何应用标识符(Application IDentifier，AID)均可作为“应用 DF”名。为了通过 DF 名进行无二义性的选择，“应用 DF”名在给定的卡内是唯一的。

(2) 通过文件标识符选择。任何文件都可以通过按 2 字节编码的文件标识符来引用。如果 MF 通过文件标识符来引用，应使用'3F00'(保留值)。值'FFFF'、'3FFF'和'0000'被保留。为了通过文件标识符来无二义性地选择任何文件，在给定 DF 下的所有直接 EF 和 DF 都应具有不同的文件标识符。

(3) 通过路径选择。任何文件都可以通过路径来引用(一串文件标识符的链接)。该路径以 MF 或当前 DF 的标识符开始，并且以文件自身的标识符结束。在这两个标识符之间，路径由连续父 DF(如果有)的标识符组成。文件标识符的次序总是在父级至子级的方向上。如果当前 DF 的标识符未知，值'3FFF'(保留值)可以用于路径的开始处。值'3F002F00'和'3F002F01'被保留，'2F00'为 EF. DIR，'2F01'为 EF. ATR。

(4) 通过短 EF 标识符选择。EF 可以通过值在 1～30 范围内的 5 位(二进制)编码的短文件标识符(Short File Identifier，SFI)来引用。用作短 EF 标识符的值 0(即二进制的 00000)引用当前已选择的 EF。短 EF 标识符不能用在路径中或不能作为文件标识符(如在第 6 章的 SELECT 命令中)。

EF. DIR 和 EF. ATR 是直接处于 MF 之下的两个基本文件(如果有的话)。EF. DIR 为目录文件，指示卡支持的一系列应用，由一组应用模板和/或应用标识符数据对象组成；EF. ATR 指示卡的操作特性，可理解为与复位应答 ATR(Answer To Reset)相关，复位应答是指 IC 卡加电后首先向读写器发出的一组数据，用来指出卡的基本特性和情况，详见第 4 章。

在 ISO/IEC 7816 中，对上述两个文件的内容到目前为止还没有更详细的描述。

在 TLV 结构的数据对象中，如果标记 T 为'51'，其数值 V 即为文件或路径，可以是任意长度。

2. 数据引用方法

在 DF 中，数据可能引用为数据对象。

在 EF 中，数据可能引用为数据单元、记录或数据对象，并可被相关命令存取。数据引用方式依赖于 EF。定义了以下 3 种 EF 结构。

(1) 透明结构。在 EF 中的数据可被看作一序列串联的数据单元，该序列通过“处理数据单元操作”的命令访问。数据单元大小一般为 4 位二进制数或 1 字节。

(2) 记录结构。在 EF 中的数据可被看作一可独立标识的记录序列，该序列通过“处理记录”的命令来访问。记录编号方法与 EF 相关。为按记录构成的 EF 定义了下列两种属性。

- 记录的长度：固定的或可变的。
- 记录的组织结构：按顺序(线性结构)或者按环形(循环结构)。

(3) TLV 结构。在 EF 中的数据可看作一个数据对象集合，该集合通过用于处理数据对象的命令来访问。这些在 EF 中的数据对象是 SIMPLE-TLV 或 BER-TLV。

为引用 EF 数据，卡必须至少支持图 3.7 中 5 种结构中的一种。

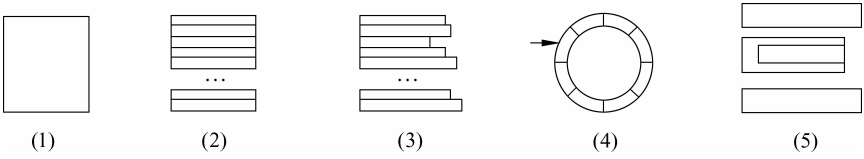


图 3.7　EF 结构

(1) 透明结构。

(2) 线性定长记录结构。

(3) 线性变长记录结构。

(4) 循环定长记录结构(箭头引用最近写入的记录)。

(5) TLV 结构(原始编码和结构化编码，在图中，上部和下部为原始编码 DO，中间是结构化编码 DO)。

3. 文件控制信息

文件控制信息(File Control Information，FCI)可包含在任意 DF 或 EF 中，执行 SELECT 命令后可从文件中读出。该命令在第 6 章中说明。

表 3.4 示出了 3 种模板来嵌套文件控制信息 BER-TLV 数据对象。

表 3.4　与 FCI 相关的模板

标　记	值
'62'	文件控制参数(FCP 模板)
'64'	文件管理数据(FMD 模板)
'6F'	文件控制参数和文件管理数据(FCI 模板)

(1) FCP 模板。它是文件控制参数(File Control Parameter, FCP)的集合,即在表 3.5 中列出的和定义的逻辑属性、结构属性和安全属性。在 FCP 模板中,数据对象定义为特定上下文类(标记为'80'至'BF')。标记'85'和'A5'引用自由选择数据。

(2) FMD 模板。它是文件管理数据(File Management Data, FMD)的集合,即在 ISO/IEC 7816 中规定的 BER-TLV 数据对象(如应用标识符、应用标号和应用有效日期)。在 FMD 模板中,标记'53'和'73'引用自由选择数据。数据对象定义为应用类,具体内容在用到时再介绍。

(3) FCI 模板。它是文件控制参数和文件管理数据的集合。

表 3.5 文件控制参数(模板标记'62')

标记 T	长度 L	值 V	适用于
'80'	变量	在文件中的数据字节数,不包括结构信息	任何 EF,1 次
'81'	2	在文件中的数据字节数,如果有,包括结构信息	任何文件,1 次
'82'	1	文件描述符字节(见表 3.6)	任何文件
	2	文件描述符字节后面紧跟着数据编码字节	
	3 或 4	文件描述符字节后面紧跟着数据编码字节和 1 个或 2 个字节的最大记录长度	任何支持记录结构的 EF
	5 或 6	文件描述符字节后面紧跟着数据编码字节和 2 个字节的最大记录长度以及 1 个或 2 个字节的记录个数	
'83'	2	文件标识符	任何文件
'84'	1～16	DF 名称	任何 DF
'85'	变量	非 BER-TLV 编码的专有信息	任何文件
'86'	变量	专有格式的安全属性	任何文件
'87'	2	包含扩充 FCI 的 EF 标识符	任何 DF,1 次
'88'	0 或 1	短 EF 标识符	任何 EF,1 次
'8A'	1	生命周期状态字节(LCS 字节)	任何文件,1 次
'8B'	变量	扩展格式安全属性	任何文件,1 次
'8C'	变量	压缩格式安全属性	任何文件,1 次
'8D'	2	包含安全环境模板的 EF 标识符	任何 DF
'8E'	1	通道安全属性	任何文件,1 次
'A0'	变量	数据对象模板安全属性	任何文件,1 次
'A1'	变量	专有格式模板安全属性	任何文件
'A2'	变量	模板包含一对或多对数据对象:短 EF 标识符(标记'88')-文件参考(标记'51',L>2)	任何 DF
'A5'	变量	BER-TLV 编码的专有信息	任何文件
'AB'	变量	扩展格式模板安全属性	任何文件,1 次
'AC'	变量	密码机制标识模板	任何 DF

表 3.5 列出了有特定上下文类中的文件控制参数，表中还指出了它仅发生一次（明确表示）或可重复（无表示）。“发生一次”表示该参数给出后不能再改变。

下面举例说明上下文类数据对象的意义。

DF 的部分控制信息可以存储在某个应用控制下的 EF 文件中，在文件控制参数中出现（通过标记'87'引用 EF 标识符），如果存在此类 EF，则文件控制信息必须以 FCP 标记'62'或 FCI 标记'6F'引入。此例说明该上下文类数据对象（标记'87'）必须在模板（标记'62'或'6F'）中应用，这就可认为是“上文”的意思，以后（“下文”）就使用此 EF 标识符。

下面再举一例，标记为'80'的数据对象，在模板'62'的引用下，其数值 V 字段指出在文件中的数据字节数，而在第 6 章安全报文 SM 模板（标记'7D'）的引用下，说明其数值 V 字段的内容是未编码为 BER-TLV 的明文。这说明上下文类数据对象在不同的上文指引下，在下文中其意义是不同的。

表 3.5 中列出的文件控制参数是很重要的，大部分参数的含义将在后面各章节（尤其是第 6 章）用到时再说明，但读者要了解“上下文类”的意义也很重要，因为在“上下文类”的数据不具有唯一性的特点。

表 3.6　文件描述符字节

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	含　义
0	×	—	—	—	—	—	—	文件可访问性
0	0	—	—	—	—	—	—	• 不可共享的文件
0	1	—	—	—	—	—	—	• 可共享的文件
0	—	1	1	1	0	0	0	DF
0	—	不全置 1			—	—	—	EF 类型
0	—	0	0	0	—	—	—	• 工作的 EF
0	—	0	0	1	—	—	—	• 内部的 EF
0	—	其他所有值			—	—	—	• EF 专用类型使用
0	—							EF 结构
0	—	不全置 1			0	0	0	• 没有信息给出
0	—	不全置 1			0	0	1	• 透明结构
0	—	不全置 1			0	1	0	• 线性结构，固定长度，没有进一步的信息
0	—	不全置 1			0	1	1	• 线性结构，固定长度，TLV 结构
0	—	不全置 1			1	0	0	• 线性结构，可变长度，没有进一步的信息
0	—	不全置 1			1	0	1	• 线性结构，可变长度，TLV 结构
0	—	不全置 1			1	1	0	• 循环结构，固定长度，没有进一步的信息
0	—	不全置 1			1	1	1	• 循环结构，固定长度，TLV 结构
0	—	1	1	1	0	0	1	• TLV 结构，用于 BER-TLV 数据对象
0	—	1	1	1	0	1	0	• TLV 结构，用于 SIMPLE-TLV 数据对象

习题

1. 试述数据元和数据对象的定义及两者之间的关系。
2. 原始编码和结构化编码数据对象的定义是什么？

3. 在结构化的 DO 中是否允许再套用结构化 DO?

4. 如果有两个 DO 链接如下：

   T_1-L_1-V_1- T_2-L_2-V_2

   假如其中不含有任何分隔符(或定界符)，而且都用数字编码来表示，请问这两个 DO 的分界处是否可能混淆?

5. 如何得出表 3.1 中通用类 DO 的原始编码范围为'0×'～'1×'，结构化编码范围为'2×'～'3×'?

6. 请写出 ISO 7816-4 的结构化 DO。

7. 在表 3.2 中，双字节标记 5F××是怎样产生的? 如果有 5E××标记是否合理?

8. 上下文类数据对象有何特点? 其标记是否具有唯一性? 具有唯一性标记是哪类数据对象?

9. 在表 3.5 的文件控制参数中，哪些标记可归在上下文类数据对象中?

10. 在 IC 卡中定义了哪几种文件? 对每一种 IC 卡来讲是否都必须有的?

11. EF 文件中存放在数据有哪几种格式?

12. 文件标识符一般由几个字节组成? 是否都可以用短文件标识符?

第 4 章　接触式 IC 卡的物理特性、触点、电信号和传输协议、ISO/IEC 7816-3110

4.1　接触式集成电路卡的物理特性

ISO/IEC 7816-1 制定的物理特性适合于 ID-1 型的识别卡，其尺寸为 85.6mm×53.98mm×0.76mm(参见第 2 章)。

ISO 7810 中为各种识别卡定义的物理特性适用于 IC 卡，ISO 7813 中对金融交易卡定义的某些特性也适用于 IC 卡。此外，还提出了以下附加特性。

(1) 防护紫外线的能力。

(2) X 光照射的剂量。

(3) 触点的表面轮廓。

(4) 卡和触点的机械强度。

(5) 触点电阻。

(6) 磁条与集成电路之间的电磁干扰。

(7) 强度磁场的影响。

(8) 静电影响。

(9) 热耗等。

标准规定了上述各项测试的具体指标，并要求经测试后的集成电路不应损坏或丧失功能。

使用时卡的表面温度不应超过 50℃。

4.2　接触式集成电路卡的触点尺寸和位置

ISO 7816-2 规定了 ID-1 型集成电路卡各触点的尺寸、位置和功能。规定每个触点都应有一个不小于 2.0mm×1.7mm 的矩形表面区域，各触点间应互相隔离，但未规定触点的形状和最大尺寸。

IC 卡有 8 个触点，从 C1 到 C8，触点可安排在卡的正面或反面。触点的位置如图 4.1 所示(以卡的接触面的左边和上边为基准线)。每个触点的功能如表 4.1 所示。

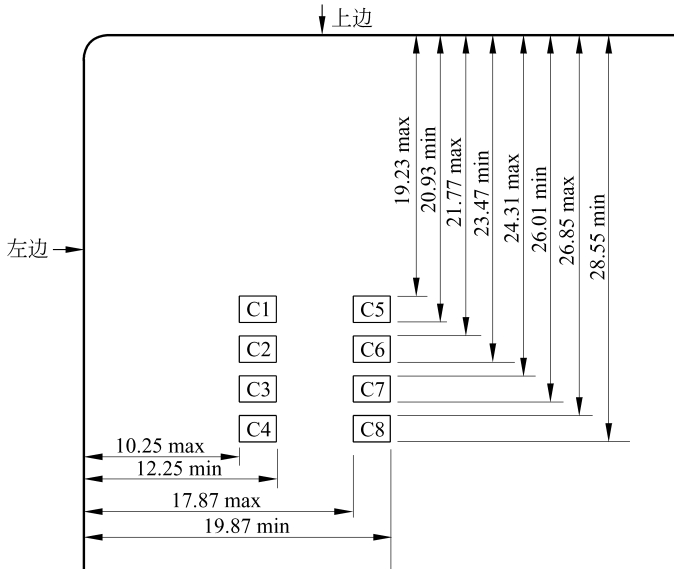


图 4.1　触点的位置

表 4.1　触点功能

触点编号	功　　能	触点编号	功　　能
C1	VCC(电源电压)	C5	GND(地)
C2	RST(复位信号)	C6	VPP(编程电压)
C3	CLK(时钟)	C7	I/O(数据)
C4	ISO/IEC JTC1/SC17 保留于将来使用	C8	ISO/IEC JTC1/SC17 保留于将来使用

4.3　接触式集成电路卡的电信号和传输协议

ISO/IEC 7816-3/10 中规定了电源及信号的结构，以及 IC 卡和读写器之间的信息交换，包括信号频率、电压电平、电流值、奇偶校验协定、操作过程、传送机制以及读写器与 IC 卡之间的通信协定等。在这里不包括信息和命令的内容。

IC 卡支持两种传输协议：同步传输协议和异步传输协议。前者在 ISO/IEC 7816-10 中定义，适用于逻辑加密卡；后者在 ISO/IEC 7816-3 中定义，适用于内含微处理器的智能卡。

4.3.1　触点的功能

在 ISO 7816-2 中对 IC 卡的 8 个触点作出了如下规定。

- I/O：IC 卡的串行数据的输入端和输出端。
- VCC：电源电压输入端。电压容错范围为±10%。目前有 3 种使用不同电压的

IC 卡(5V、3V 和 1.8V),当 IC 卡不慎插入提供高电压的读写器时,不应损坏,内容也不允许被修改。

- GND:地(参考电压)。
- VPP:E^2PROM 的编程电压输入端。一般 IC 卡内部有升压电路,将 V_{CC} 电压升到 E^2PROM 编程电压,VPP 触点已无用。
- CLK:时钟或定时信号输入端(由卡选用)。
- RST:复位信号(总清信号),可由读写器提供复位信号给 RST 触点;或由 IC 卡内部的复位控制电路在加电时产生内部复位信号。如果实现内部复位,必须提供电压到 VCC 端。

剩下两个触点的用途将在相应的应用标准中规定。某些接触式 IC 卡仅有 6 个触点。

I/O 触点有如下两种可能的状态。

(1) 高状态(Z 状态)。当卡和读写器均处在接收方式时,I/O 处于 Z 状态,也可被发送方规定为 Z 状态。

(2) 低状态(A 状态)。可被发送方规定为 A 状态。

如卡与读写器均处于接收方式时,I/O 端处于 Z 状态。当卡与读写器处于不匹配的传输方式时,I/O 端的逻辑状态可能是不确定的。在操作期间,卡与读写器不能同时处于发送方式。

4.3.2 接触式 IC 卡的操作过程和卡的复位

1. 读写器和卡之间对话的操作顺序

(1) 读写器连接卡(插卡),并"激活(active)"IC 卡。

(2) 卡的冷复位(reset)。

(3) 卡对复位的应答(Answer To Reset,ATR)。

(4) 在卡与读写器之间连续进行信息交换(读写器发命令,IC 卡返回响应)。

(5) 读写器"停活"IC 卡(终止操作)。

2. 读写器"激活"IC 卡的操作顺序(图 4.2)

(1) RST 处于 L 状态。

(2) VCC 加电。

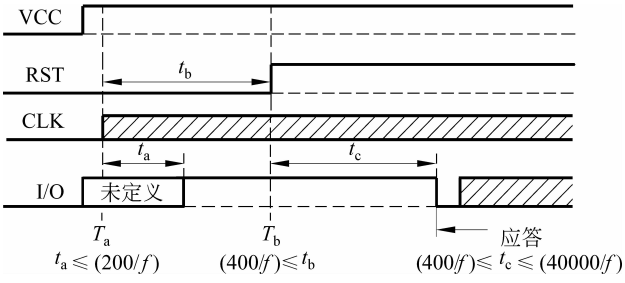


图 4.2 激活和冷复位

(3) 读写器的 I/O 端处于接收方式。

(4) 提供稳定的 CLK。

3. IC 卡的复位

复位有冷复位和热复位两种。

(1) 冷复位：当 IC 卡的电源电压和其他信号从静止状态按一定顺序加上时，称为冷复位，IC 卡发回应答信号 ATR。

(2) 热复位：在电源电压 V_{CC} 和时钟 CLK 处于激活状态下，读写器发出的复位称为热复位，IC 卡发回应答信号 ATR。

卡与读写器的交互，总是起始于冷复位，之后，读写器可启动热复位但非必须有热复位。

1) 冷复位

如图 4.2 所示，在 T_a 时间读写器在 CLK 端加时钟信号。I/O 端应在时钟信号加于 CLK 的 200 个时钟周期(t_a)内被卡置于状态 Z(t_a 时间在 T_a 之后)。时钟加于 CLK 后，保持 RST 为状态 L(低电平)至少 400 周期(t_b)(t_b 在 T_a 之后)。

在时间 T_b，读写器将 RST 置于状态 H(高电平)。I/O 上的应答由 IC 卡发出，应在 RST 信号的上升沿之后的 400～40 000 个时钟周期(t_c)内开始(t_c 在 T_b 之后)。

在 RST 处于状态 H 的情况下，如果应答信号在 40 000 个时钟周期内仍未开始，RST 上的信号将返回到状态 L，各触点的状态按照图 4.5 被读写器释放(停活)，IC 卡终止操作。

2) 热复位

按照图 4.3 所示，当 V_{CC} 和 CLK 保持稳定时，读写器置 RST 为状态 L 至少 400 时钟周期(时间 t_e)后，读写器启动热复位。

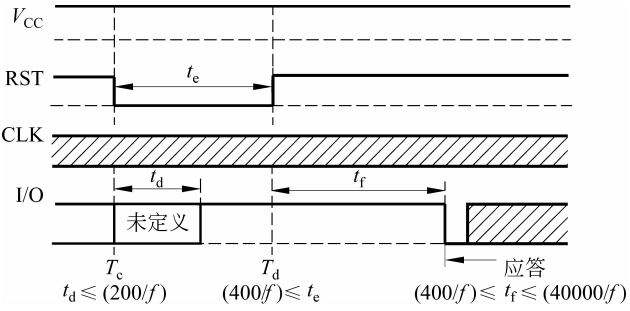


图 4.3　热复位

在时间 T_d，RST 置于状态 H。I/O 的应答在 RST 信号上升沿之后的 400～40 000 个时钟周期(t_f)开始(时间 t_f 在 T_d 之后)。

在 RST 处于状态 H 时，如果 IC 卡的应答信号未在 40 000 个周期之内开始，RST 上的信号将返回状态 L，且电路按图 4.5 所示被读写器停活。

3) 时钟停止(暂停)

对于支持时钟停止的卡，当读写器不希望从卡得到信息时，并且 I/O 保持在状态

Z 至少 1860 个时钟周期(t_g),按照图 4.4 所示,读写器可停止 CLK 上的时钟(在时间 T_e)。

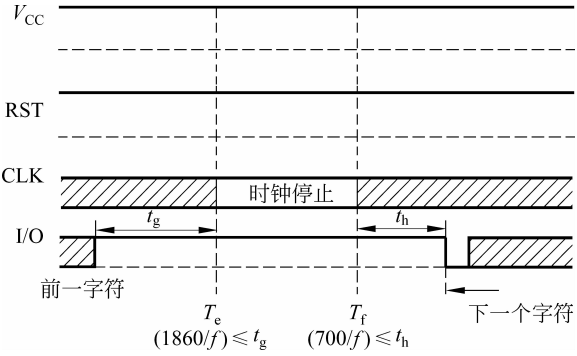


图 4.4 时钟停止

当时钟被停止(从 T_e 到 T_f),CLK 应保持在状态 H 或状态 L。这个状态由复位应答 ATR 的参数 X 指明(见 4.3.3 节)。

在时间 T_f,读写器重启时钟并且 I/O 上的信息交换可在至少 700 个时钟周期后继续(时间 t_h 在 T_f 之后)。

4. 停活

当信息交换结束或失败时(如无卡响应或发现卡被移出),读写器应按以下顺序停活 IC 卡,如图 4.5 所示。

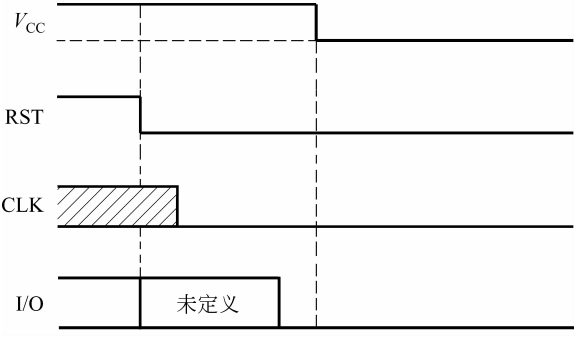


图 4.5 停活

(1) RST 应为状态 L。

(2) CLK 应为状态 L(除非时钟已在状态 L 上停止)。

(3) I/O 应被置为状态 A。

(4) V_{CC} 应被停活降至 0V。

ATR 和命令-响应是理解、设计 IC 卡和 RFID 标签的重点,并与应用密切相关,也为本书的重点。

4.3.3 异步传输的复位应答 ATR

复位应答信号以字符为单位(称为字符帧)进行传送。下面先介绍字符帧,然后描述复位应答信号。

1. 字符帧

字符帧如图 4.6 所示。

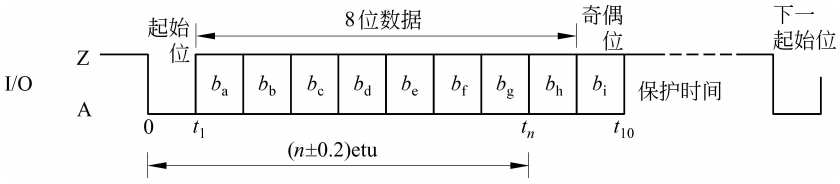


图 4.6 字符帧

在传送字符前,I/O 处于状态 Z。

每个字符由 10 位组成:起始位(1 位)为状态 A,8 位数据 b_a～b_h,第 10 位 b_i 为偶校验位(从 b_a 到 b_i,1 的个数为偶数是正确的)。每一位在 I/O 触点上的持续时间定义为基本时间单元 etu。在复位应答期间,1etu=372 个时钟周期,即 1etu=372/f,f 为时钟频率。

一个数据字节由 b_1～b_8 组成,b_1 为最低位,b_8 是最高位。

接收方在每一位的中间(0.5±0.2)etu 采样,采样时间应少于 0.2etu。

两个连续字符之间的延时(两起始位下降沿之间)至少为 12 个基本时间单元,包括字符宽度 10 个 etu 和一段保护时间,在保护时间内,读写器和卡都处于接收状态,因此 I/O 触点处于状态 Z。

在复位应答期间,卡发出的两个连续字符的起始位下降沿之间的延时不得超过 9600etu,这个最大值称为初始等待时间。

当奇偶校验不正确时,从起始位下降沿之后的 10.5etu 开始,收方发送状态 A 作为出错信号,该信号宽度为一个 etu 或两个 etu。发方检验 I/O 是在起始位下降沿之后的 11etu 处,如 I/O 处于状态 Z,则认为接收是正确的;如 I/O 处于状态 A,则认为有错,收方期望发方重发有错的字符(对使用T=0异步传输协议的卡必须重发,其他的卡则是可选择的)。

2. 复位应答信息的内容

其主要包括 IC 卡的发行者和应用标识符以及信息传输的基本参数等。假如读写器发现问题,可立即停止操作或为后面的操作提供指示。

卡产生的复位应答信息按以下顺序传送:初始字符 TS、格式字符 T0、接口字符 TA_i TB_i TC_i TD_i(i=1,2,…),历史字符 T1 T2…TK(最多 15 个字符)以及校验字符 TCK。其中,TS 和 T0 是一定要有的,接口字符和校验字符是可选择的。图 4.7 所示是复位应答的一般构成。在 TS 之后发送的字符数不超过 32 个。

(1) 初始字符 TS。I/O 开始处于状态 Z,然后是起始位 A,接着有两种表示方法,如