ICS 03.220.20;35.240.60
R 10
备案号:

JT

中华人民共和国交通运输行业标准

JT/T 825.2—2012

IC卡道路运输证件
第2部分:IC卡技术要求

IC card license for road transportation—
Part 2:Specification for IC card

2012-02-20 发布　　2012-05-01 实施

中华人民共和国交通运输部　发布

目　　次

前　言

JT/T 825《IC 卡道路运输证件》分为 13 个部分：

——第 1 部分：总体技术要求；

——第 2 部分：IC 卡技术要求；

——第 3 部分：IC 卡道路运输证数据格式；

——第 4 部分：IC 卡道路运输证规格与样式；

——第 5 部分：IC 卡从业资格证数据格式；

——第 6 部分：IC 卡从业资格证规格与样式；

——第 7 部分：IC 卡物理防伪膜技术要求；

——第 8 部分：密钥安全体系框架；

——第 9 部分：密钥管理系统技术要求；

——第 10 部分：IC 卡初始化设备技术要求；

——第 11 部分：IC 卡证卡打印机技术要求；

——第 12 部分：IC 卡读写器技术要求；

——第 13 部分：IC 卡及关键设备检测规范。

本部分为 JT/T 825 的第 2 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分由交通运输部信息通信及导航标准化技术委员会提出并归口。

本部分主要起草单位：交通运输部科学研究院、广东省交通运输厅。

本部分参加起草单位：交通运输部公路科学研究院、山西省交通运输管理局、甘肃省公路运输管理局。

本部分主要起草人：张永军、陈宓、郑晓峰、吴金中、陶圣、杨富峰、靳瑾、林海、张路彬、张晓征、李春里。

IC卡道路运输证件
第2部分:IC卡技术要求

1 范围

JT/T 825的本部分规定了IC卡道路运输证件的基本技术要求、物理特性、信号接口、传输协议、文件结构、命令集、安全机制以及应用选择。

本部分适用于IC卡道路运输证件的卡片选择、系统设计及应用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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 14916 识别卡 物理特性

GB/T 16649.1 识别卡 带触点的集成电路卡 第1部分:物理特性

GB/T 16649.2 识别卡 带触点的集成电路卡 第2部分:触点的尺寸和位置

GB/T 16649.3 识别卡 带触点的集成电路卡 第3部分:电信号和传输协议

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

JR/T 0025 中国金融集成电路(IC)卡规范(2.0版)

ISO/IEC 7816-4 信息技术 识别卡 有触点的集成电路卡 第4部分:用于交换的行业间信令[Identification cards-Integrated circuit(s) cards with contacts Part 4: Interindustry commands for interchange]

ISO/IEC 7816-5 识别卡 集成电路卡 第5部分:应用提供者的登记(Identification cards-Integrated circuit cards Part 5:Registration of application providers)

ISO/IEC 14443-1 识别卡 无触点集成电路卡 第1部分:物理特性[Identification cards-Contactless integrated circuit(s) cards-Proximity cards Part 1: Physical characteristics]

ISO/IEC 14443-2 识别卡 无触点集成电路卡 第2部分:耦合区域的尺寸和位置[Identification cards-Contactless integrated circuit(s) cards-Proximity cards Part 2: Radio frequency power and signal interface]

ISO/IEC 14443-3 识别卡 无触点集成电路卡 第3部分:电信号和复位规程[Identification cards-Contactless integrated circuit(s) cards-Proximity cards Part 3: Initialization & anticollision]

ISO/IEC DIS 14443-4 识别卡 无触点集成电路卡 第4部分:传输协议[Identification cards-Contactless integrated circuit(s) cards-Proximity cards Part 4: Transmission protocols]

3 术语和定义

下列术语和定义适用于本文件。

3.1

TSAM卡　transportation secure access module card

应用于IC卡道路运输证件系统中的安全控制模块。

3.2

终端　terminal

为完成道路运输行业管理业务而在业务点安装的设备，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。

3.3

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。

3.4

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。

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

对业务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

在将明文转换为密文或将密文转换为明文的算法中输入的数据。

3.8

加密算法　cryptographic algorithm

为了隐藏或揭露信息内容而变换数据的算法。

3.9

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。

3.10

物理卡号　physical card number

IC卡初始化和防碰撞过程中返回的标识卡片唯一性的四个字节ID号。

3.11

厂商标识　manufacturer ID

由交通运输主管部门统一向各IC卡厂商分配的唯一标识，长度为一个字节。

4　缩略语

下列缩略语适用于本文件。

ADF——应用数据文件(application data file)

AEF——应用基本文件(application elementary file)

AID——应用标识符(application identifier)

APDU——应用协议数据单元(application protocol data unit)

CLA——命令报文的类别字节(class byte of the command message)

COS——卡片操作系统(chip operating system)
DDF——目录数据文件(directory data file)
DEA——数据加密算法(data encryption algorithm)
DES——一种数据加密标准(data encryption standard)
DF——专用文件(dedicated file)
DIR——目录(directory)
EF——基本文件(elementary file)
FCI——文件控制信息(file control information)
INS——命令报文的指令字节(instruction byte of command message)
Lc——终端发出的命令数据的实际长度(exact length of data sent by the tal in a case 3 or 4 command)
Le——响应数据的最大期望长度(maximum length of data expected by the tal in response to a case 2 or 4 command)
MAC——报文认证码(message authentication code)
MF——主控文件(master file)
PICC——接近式卡(proximity card)
RTSA——道路运输系统应用(road transportation system application)
RTSE——道路运输系统环境(road transportation system environment)
SFI——短文件标识符(short file identifier)

5 基本技术要求

5.1 IC 卡道路运输证件的基本技术要求

IC 卡道路运输证件应满足以下要求:
——非接触式 CPU 卡;
——卡片通信协议符合 ISO/IEC 14443 规定的通信协议;
——存储容量不小于 16kbytes;
——芯片程序存储器为 Mask ROM,数据存储器为 NVM;
——内部含有真随机数发生器,加解密、MAC 计算使用硬件算法实现;
——芯片工作温度 -25℃ ~ +70℃,静电保护 2 000V 以上;
——数据保存时间在 10 年以上,擦写次数 10 万次以上;
——支持多应用环境,一卡多用,各应用之间相互独立;
——支持多种文件类型,包括二进制文件、定长记录文件、变长记录文件、循环记录文件;
——在通信过程中支持多种安全保护机制(信息的机密性和完整性保护);
——支持多种安全访问方式和权限(内、外部认证功能);
——支持第 8 章所规定的 3DES 算法,支持国家认可的加密算法。

5.2 TSAM 卡的基本技术要求

TSAM 卡应满足以下要求:
——具备多种封装方式,可为卡片式封装或集成电路式封装;
——接触界面应支持 PPS,握手通信速率从 9 600bit/s 开始,可以支持更高通信速率;
——接触界面传输协议应支持 T=0 协议;
——存储容量不小于 8kbytes,存储器为 NVM;

——数据保存时间在 10 年以上,擦写次数 10 万次以上;
——芯片工作温度 -25℃ ~ +70℃,静电保护 4 000V 以上;
——支持多应用环境,一卡多用,各应用之间相互独立;
——支持多种文件类型,包括二进制文件、定长记录文件、变长记录文件、循环文件;
——应采用硬件 3DES 协处理器和硬件真随机数发生器;
——在通信过程中支持多种安全保护机制(信息的机密性和完整性保护);
——支持多种安全访问方式和权限(内、外部认证功能);
——支持第 8 章所规定的 3DES 算法,支持国家认可的加密算法;
——支持多级密钥分散机制,用分散后的密钥作为临时密钥对数据进行加密、MAC 等运算,以完成终端与卡片之间的合法性认证等功能。

6 物理特性、信号接口及传输协议

6.1 IC 卡道路运输证件的物理特性、信号接口及传输协议

6.1.1 物理特性

IC 卡道路运输证件的物理特性应符合 ISO/IEC 14443-1 中有关物理特性的要求。

6.1.2 射频功率和信号接口

IC 卡道路运输证件的射频功率应符合 ISO/IEC 14443-2 的要求,信号接口应符合 ISO/IEC 14443-2 中通信接口的要求。

6.1.3 初始化和防冲突

IC 卡道路运输证件的初始化和防冲突应符合 ISO/IEC 14443-3 中的初始化、防冲突等要求。在初始化和防冲突过程中,应能获取厂商标识及卡片 COS 版本信息,格式见表 1。

表 1 厂商标识及卡片 COS 版本信息格式

厂商标识	卡片 COS 标识符	卡片 COS 版本号	卡片 COS 修订号
一个字节	一个字节	一个字节	一个字节
注:卡片 COS 标识符使用 A ~ Z 中的任意一个字母表示。			

6.2 TSAM 卡的物理特性、信号接口及传输协议

6.2.1 物理特性

接触式 CPU 卡封装形式的 TSAM 卡的物理特性应符合 GB/T 16649.1 的要求。

6.2.2 通信特性

TSAM 卡的通信特性应符合 GB/T 16649.3 的要求。

6.2.3 电气特性

TSAM 卡的电气特性应符合 GB/T 16649.3 的要求。

7 文件和命令

7.1 文件

7.1.1 文件存储方式

数据文件中数据元以记录方式或二进制方式存储。

7.1.2 文件结构

7.1.2.1 基本要求

本部分文件结构符合 GB/T 16649.4 的相关规定。

IC 卡中 RTSA 的路径可以通过明确选择 RTSE 来激活。一个成功的 RTSE 选择能够对目录结构进行访问。

从终端角度来看,RTSA 相关的 RTSE 文件呈一种可通过目录结构访问的树形结构。树的每一分支是一个 ADF。一个 ADF 是一个或多个 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。

7.1.2.2 应用数据文件

ADF 的树形结构应满足以下要求:

——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 FCI 中纯数据对象的文件。

7.1.2.3 应用基本文件

一个 AEF 包含一个或多个原始基本编码规则——标签、长度、值(BER-TLV)数据对象。但在选择了某一应用后,AEF 可通过文件标识符(FID)或 SFI 进行查询。

7.1.2.4 文件结构中文件的映象

文件结构中文件的映象应符合 ISO/IEC 7816-4 中的相关规定,使用下列映象表:

——包含一个 FCI 的 DF(ISO/IEC 7816-4 中定义)被映象为 ADF,可通过它来访问 EF 和 DF,在卡中处于最高层的 DF 称为主控文件(MF);

——包含一组记录中的 EF(ISO/IEC 7816-4 中定义)被映象为 AEF,EF 不能作为进入另一个不同 DF 文件的入口点。

在本部分中,DF 中相连的 EF 的访问是透明的。

7.1.2.5 目录结构

IC 卡支持用于 RTSE 应用列表的目录结构,RTSE 由发卡方通过目录选择。目录结构包括一个必备的道路运输系统 DIR 文件和一些可选的由 DDF 引用的附加目录。

目录结构采用以其 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 RTSE 选择的响应报文中对 DIR 文件进行编码(参见 SELECT 命令)。

DIR 文件是一个 AEF(即一个记录结构的 EF),它包含 ISO/IEC7816-5 中定义的数据对象。

在 IC 卡中道路运输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。

7.1.3 文件查询

7.1.3.1 通过文件名查询

卡中的任何 ADF、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。

7.1.3.2 通过文件标识符(FID)查询

卡中的任何 ADF、DDF、EF 可通过其文件标识符查询,每个文件的标识符在给定的应用中应是唯一的。

7.1.3.3 通过短文件标识符(SFI)查询

SFI 用于选择 AEF。对给定应用中的任何 AEF,可以通过 SFI(五位代码,取值范围 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。

7.2 APDU 命令

7.2.1 APDU 命令的内容及格式

命令 APDU 由四个字节长的必备头后跟一个可变长的条件体组成,见图 1。

CLA	INS	P1	P2	Lc	Data	Le
←必备头→				←条件体→		

图 1 命令 APDU 结构

命令 APDU 中发送的数据字节数用 Lc(命令数据域的长度)表示。

响应 APDU 中期望返回的数据字节数用 Le(期望数据长度)表示。当 Le 存在且值为 0 时,表示需要最大字数(256 个字节)。在命令报文需要时,Le 始终被设为“00”。

命令 APDU 报文的内容见表 2。

表 2 命令 APDU 的内容

代　码	描　述	长　度(字节)
CLA	命令类别	1
INS	指令代码	1
P1	指令参数 1	1
P2	指令参数 2	1
Lc	命令数据域中存在的字节数	0 或 1
Data	命令发送的数据位串(= Lc)	可变
Le	响应数据域中期望的最大数据字节数	0 或 1

7.2.2 APDU 响应的内容及格式

响应 APDU 格式由一个变长的条件体后随两个字节长的必备尾组成,见图 2。

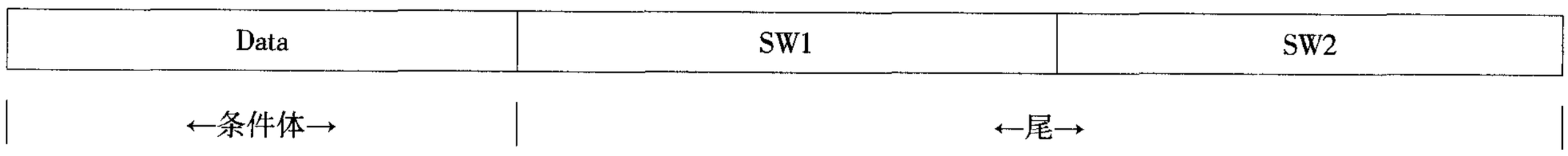

图 2　响应 APDU 结构

响应 APDU 的内容见表 3。

表 3　响应 APDU 的内容

代　　码	描　　述	长　　度(字节)
Data	响应中接收的数据位串(=Lr)	变长
SW1	命令处理状态	1
SW2	命令处理限定	1

7.2.3　命令集

7.2.3.1　基本命令集

IC 卡道路运输证件基本命令集见表 4。

表 4　IC 卡道路运输证件基本命令集

编号	指 令 名 称	CLA	INS	功 能 描 述
1	APPLICATION BLOCK	84	1E	应用锁定
2	APPLICATION UNBLOCK	84	18	应用解锁
3	CARD BLOCK	84	16	卡片锁定
4	CHANGE PIN	80	5E	修改个人识别码
5	PIN UNBLOCK	84	24	解锁个人识别码
6	RELOAD PIN	80	5E	重装个人识别码
7	VERIFY	00	20	校验个人识别码
8	GET CHALLENGE	00	84	取随机数
9	GET RESPONSE	00	C0	取响应数据
10	EXTERNAL AUTHENTICATE	00	82	外部认证
11	INTERNAL AUTHENTICATE	00	88	内部认证
12	READ BINARY	00 或 04	B0	读二进制文件
13	READ RECORD	00 或 04	B2	读记录文件
14	UPDATE BINARY	00 或 04	D6	写二进制文件
15	UPDATE RECORD	00 或 04	DC	写记录文件
16	APPEND RECORD	00 或 04	E2	添加记录
17	SELECT	00	A4	选择文件
注:编号 1 ~9 命令参见 JR/T 0025。				

TSAM 卡基本命令集见表 5。

表 5　TSAM 卡基本命令集

编号	指 令 名 称	CLA	INS	功 能 描 述
1	GET CHALLENGE	00	84	取随机数
2	GET RESPONSE	00	C0	取响应数据
3	EXTERNAL AUTHENTICATE	00	82	外部认证
4	SELECT FILE	00	A4	选择文件
5	READ BINARY	00	B0	读二进制文件
6	UPDATE BINARY	00 或 04	D6	写二进制文件
7	READ RECORD	00	B2	读记录文件
8	UPDATE RECORD	00 或 04	DC	写记录文件
9	WRITE KEY	84	D4	装载/更新密钥
10	INIT_FOR_DESCRYPT	80	1A	准备密钥为数据计算
11	CIPHER DATA	80	FA	对数据进行安全计算
注：编号 1～2 命令参见 JR/T 0025。				

7.2.3.2　EXTERNAL AUTHENTICATION 命令

7.2.3.2.1　定义和范围

EXTERNAL AUTHENTICATION 命令要求 IC 卡中的应用验证密码。

IC 卡的响应包括命令处理状态的回送。

7.2.3.2.2　命令报文

EXTERNAL AUTHENTICATION 命令报文编码见表 6。

表 6　EXTERNAL AUTHENTICATION 命令报文

代码	数　值								
CLA	00								
INS	82								
P1	00								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说　明
	0	x	x	x	x	x	x	x	全局密钥标识
	1	x	x	x	x	x	x	x	局部密钥标识
	0	0	0	0	0	0	0	0	当前 DF 下的 MK
Lc	08								
DATA	认证数据								
Le	不存在								

EXTERNAL AUTHENTICATION 命令使用的算法参考值(P1)编码为“00”,表示无信息。算法参考值在命令发出之前是已知的,或者在数据域中提供。

7.2.3.2.3 命令报文数据域

命令报文数据域中包含对取随机数命令(GET CHALLENGE)取回的数据按照第8章定义计算的3DES加密值。

如果取随机数命令(GET CHALLENGE)取回八个字节数据,则作为输入数据进行3DES计算。

7.2.3.2.4 响应报文数据域

响应报文数据域不存在。

7.2.3.2.5 响应报文状态字

IC卡可能回送的响应信息状态码见表7。

表7 EXTERNAL AUTHENTICATION响应信息状态码

SW1	SW2	说 明	SW1	SW2	说 明
90	00	命令执行成功	69	85	使用条件不满足
63	Cx	认证失败,还可以认证x次	6A	81	功能不支持
65	81	写EEPROM失败	6A	86	P1、P2参数错
67	00	Lc长度错误	6A	88	未找到密钥数据
69	82	不满足安全状态	6D	00	命令不存在
69	83	认证密钥锁定	6E	00	CLA错
69	84	引用数据无效(未申请随机数)	93	03	应用永久锁定

7.2.3.3 INTERNAL AUTHENTICATION命令

7.2.3.3.1 定义和范围

INTERNAL AUTHENTICATION命令提供了利用接口设备发来的数据(随机数或双方定义好的数据)和自身存储的相关密钥进行数据认证的功能。

7.2.3.3.2 命令报文

INTERNAL AUTHENTICATION命令报文编码见表8。

表8 INTERNAL AUTHENTICATION命令报文

代码	数 值								
CLA	00								
INS	88								
P1	00								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	x	x	x	x	x	x	x	全局密钥标识
	1	x	x	x	x	x	x	x	局部密钥标识
	0	0	0	0	0	0	0	0	当前DF下的MK
Lc	08								
DATA	输入数据								
Le	08								

INTERNAL AUTHENTICATION 命令的参数 P1 为“00”时的含义是无信息。P1 的值可事先得到,也可以在数据域中提供。

7.2.3.3.3 命令报文数据域

命令报文数据域的内容是接口设备发来的数据(随机数或双方定义好的数据)。

7.2.3.3.4 响应报文数据域

响应报文数据域的内容是相关认证数据,是以命令报文数据域的内容作为输入,以 P2 参数所指示的密钥索引对应的密钥为加密密钥进行 3DES 加密运算的结果。

7.2.3.3.5 响应报文状态字

IC 卡可能回送的响应信息状态码见表 9。

表 9 INTERNAL AUTHENTICATION 响应信息状态码

SW1	SW2	说 明	SW1	SW2	说 明
90	00	命令执行成功	6A	81	功能不支持
62	81	返回数据可能有错	6A	86	P1、P2 参数错
64	00	标志状态位未变	6A	88	未找到密钥数据
67	00	Lc 长度错误	6D	00	命令不存在
69	82	不满足安全状态	6E	00	CLA 错
69	85	使用条件不满足	93	03	应用永久锁定

7.2.3.4 READ BINARY 命令

7.2.3.4.1 定义和范围

READ BINARY 命令用于读出二进制文件的内容。

7.2.3.4.2 命令报文

READ BINARY 命令报文编码见表 10。

表 10 READ BINARY 命令报文

代码	数 值								
CLA	00 或 04								
INS	B0								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	x	x	x	x	x	x	x	当前文件高位地址
	1	0	0	x	x	x	x	x	通过 SFI 方式访问
P2	若 P1 的 b8 = 0,P2 为文件的低位地址 若 P1 的 b8 = 1,P2 为文件地址								

表 10 （续）

代码	数　值
Lc	CLA = 00 时，不存在 CLA = 04 时，Lc = 04
DATA	CLA = 00 时，不存在 CLA = 04 时，为 MAC 数据
Le	期望返回的数据长度

7.2.3.4.3 命令报文数据域

一般情况下，命令报文数据域不存在。当使用安全报文时，命令报文数据域中应包含 MAC。MAC 的计算方法和长度由应用决定。

7.2.3.4.4 响应报文数据域

响应报文数据域的内容是明文或密文数据。

7.2.3.4.5 响应报文状态字

IC 卡可能回送的响应信息状态码见表 11。

表 11 READ BINARY 响应信息状态码

SW1	SW2	说　明	SW1	SW2	说　明
90	00	命令执行成功	69	88	安全信息（MAC 和加密）数据错误
61	xx	还有 xx 个字节数据要返回	6A	81	功能不支持
62	81	返回数据可能有错	6A	82	未找到文件
65	81	写 EEPROM 失败	6A	86	P1、P2 参数错
67	00	Lc 长度错误	6A	88	未找到密钥数据
69	81	当前文件不是二进制文件	6B	00	起始地址超出范围
69	82	不满足安全状态	6C	xx	Le 长度错误，xx 表示实际长度
69	83	认证密钥锁定	6D	00	命令不存在
69	84	引用数据无效（未申请随机数）	6E	00	CLA 错
69	85	使用条件不满足	93	03	应用永久锁定
69	86	没有选择当前文件			

7.2.3.5 READ RECORD 命令

7.2.3.5.1 定义和范围

READ RECORD 命令用于读出记录文件的内容。

7.2.3.5.2 命令报文

READ RECORD 命令报文编码见表 12。

表 12　READ RECORD 命令报文

代码	数　值								
CLA	00 或 04								
INS	B2								
P1	记录号								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说　明
	0	0	0	0	0	—	—	—	当前文件
	x	x	x	x	x	—	—	—	通过 SFI 方式访问
						1	0	0	P1 作为记录号
Lc	CLA = 00 时，不存在 CLA = 04 时，Lc = 04								
DATA	CLA = 00 时，不存在 CLA = 04 时，为 MAC 数据								
Le	期望返回的记录数据								

7.2.3.5.3　命令报文数据域

一般情况下，命令报文数据域不存在。当使用安全报文时，命令报文数据域中应包含 MAC。MAC 的计算方法和长度由应用决定。

7.2.3.5.4　响应报文数据域

响应报文数据域的内容是明文或密文数据。

7.2.3.5.5　响应报文状态字

IC 卡可能回送的响应信息状态码见表 13。

表 13　READ RECORD 响应信息状态码

SW1	SW2	说　明	SW1	SW2	说　明
90	00	命令执行成功	69	86	没有选择当前文件
61	xx	还有 xx 个字节数据要返回	69	88	安全信息(MAC 和加密)数据错误
62	81	返回数据可能有错	6A	81	功能不支持
64	00	标志状态位未变	6A	82	未找到文件
65	81	写 EEPROM 失败	6A	83	未找到记录
67	00	Lc 长度错误	6A	86	P1、P2 参数错
69	81	当前文件不是记录文件	6A	88	未找到密钥数据
69	82	不满足安全状态	6B	00	起始地址超出范围
69	83	认证密钥锁定	6C	xx	Le 长度错误，xx 表示实际长度
69	84	引用数据无效(未申请随机数)	6E	00	CLA 错
69	85	使用条件不满足	93	03	应用永久锁定

7.2.3.6 UPDATE BINARY 命令

7.2.3.6.1 定义和范围

UPDATE BINARY 命令用于更新二进制文件的内容。

7.2.3.6.2 命令报文

UPDATE BINARY 命令报文编码见表 14。

表 14 UPDATE BINARY 命令报文

代码	数值								
CLA	00 或 04								
INS	D6								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说明
	0	x	x	x	x	x	x	x	当前文件高位地址
	1	0	0	x	x	x	x	x	通过 SFI 方式访问
P2	若 P1 的 b8 = 0,P2 为文件的低位地址 若 P1 的 b8 = 1,P2 为文件地址								
Lc	DATA 数据域长度								
DATA	修改用的数据 + 报文鉴别代码(MAC)数据元(四个字节)								
Le	不存在								

7.2.3.6.3 命令报文数据域

命令报文数据域包括更新原有数据的新数据。

报文鉴别代码(MAC)数据元:四个字节。

7.2.3.6.4 响应报文数据域

响应报文数据域不存在。

7.2.3.6.5 响应报文状态字

IC 卡可能回送的响应信息状态码见表 15。

表 15 UPDATE BINARY 响应信息状态码

SW1	SW2	说明	SW1	SW2	说明
90	00	命令执行成功	69	88	安全信息(MAC 和加密)数据错误
65	81	写 EEPROM 失败	6A	81	功能不支持
67	00	Lc 长度错误	6A	82	未找到文件
69	81	当前文件不是二进制文件	6A	86	P1、P2 参数错
69	82	不满足安全状态	6A	88	未找到密钥数据
69	83	认证密钥锁定	6B	00	起始地址超出范围
69	84	引用数据无效(未申请随机数)	6D	00	命令不存在
69	85	使用条件不满足	6E	00	CLA 错
69	86	没有选择当前文件	93	03	应用永久锁定

7.2.3.7 UPDATE RECORD 命令

7.2.3.7.1 定义和范围

UPDATE RECORD 命令用于更新记录文件中指定记录的内容。

7.2.3.7.2 命令报文

UPDATE RECORD 命令报文编码见表 16。

表 16 UPDATE RECORD 命令报文

代码	数 值								
CLA	00 或 04								
INS	DC								
P1	记录号								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	0	0	0	0	—	—	—	当前文件
	x	x	x	x	x	—	—	—	通过 SFI 方式访问
						1	0	0	P1 作为记录号
						0	0	0	第一个记录
						0	0	1	最后一个记录
						0	1	0	上一个记录
						0	1	1	下一个记录
Lc	DATA 数据域长度								
DATA	更新原有记录的新记录 + 报文鉴别代码(MAC)数据元(四个字节)								
Le	不存在								

7.2.3.7.3 命令报文数据域

命令报文数据域由更新原有记录的新记录和报文鉴别代码(MAC)数据元(四个字节)组成。

7.2.3.7.4 响应报文数据域

响应报文数据域不存在。

7.2.3.7.5 响应报文状态字

IC 卡可能回送的响应信息状态码见表 17。

表 17 UPDATE RECORD 响应信息状态码

SW1	SW2	说 明	SW1	SW2	说 明
90	00	命令执行成功	69	81	当前文件不是记录文件
65	81	写 EEPROM 失败	69	82	不满足安全状态
67	00	Lc 长度错误	69	83	认证密钥锁定

表 17 （续）

SW1	SW2	说　明	SW1	SW2	说　明
69	84	引用数据无效(未申请随机数)	6A	84	存储空间不够
69	85	使用条件不满足	6A	86	P1、P2 参数错
69	86	没有选择当前文件	6A	88	未找到密钥数据
69	88	安全信息(MAC 和加密)数据错误	6B	00	起始地址超出范围
6A	81	功能不支持	6D	00	命令不存在
6A	82	未找到文件	6E	00	CLA 错
6A	83	未找到记录	93	03	应用永久锁定

7.2.3.8 APPEND RECORD 命令

7.2.3.8.1 定义和范围

APPEND RECORD 命令用于向记录文件中添加新记录。对循环记录文件,可无限添加记录;对其他记录文件,只能添加到文件的最后一条记录。

APPEND RECORD 命令的执行应满足访问文件的添加权限和添加属性。

7.2.3.8.2 命令报文

APPEND RECORD 命令报文格式见表 18。

表 18 APPEND RECORD 命令报文

代码	数　值								
CLA	00 或 04								
INS	E2								
P1	00								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说　明
	0	0	0	0	0	0	0	0	当前的 EF 文件
	x	x	x	x	x	0	0	0	用 SFI 方式
Lc	DATA 域数据长度								
DATA	添加新记录用的数据 + 报文鉴别代码(MAC)数据元(四个字节)								
Le	不存在								

7.2.3.8.3 命令报文数据域

命令报文数据域包括添加新记录的新数据。

报文鉴别代码(MAC)数据元:四个字节。

7.2.3.8.4 响应报文数据域

响应报文数据域不存在。

7.2.3.8.5 响应报文状态码

响应信息中可能出现的状态码见表19。

表19 APPEND RECORD 响应信息状态码

SW1	SW2	说 明	SW1	SW2	说 明
90	00	命令执行成功	6A	81	功能不支持
65	81	写 EEPROM 失败	6A	82	未找到文件
67	00	Lc 长度错误	6A	84	记录空间已满
69	81	当前文件不是记录文件	6A	85	Lc 与 TLV 结构不匹配
69	82	不满足安全状态	6A	86	P1、P2 参数错
69	83	认证密钥锁定	6A	88	未找到密钥数据
69	84	引用数据无效(未申请随机数)	6D	00	命令不存在
69	85	使用条件不满足	6E	00	CLA 错
69	86	没有选择当前文件	93	03	应用永久锁定
69	88	安全信息(MAC 和加密)数据错误			

7.2.3.9 SELECT 命令

7.2.3.9.1 定义和范围

SELECT 命令通过文件标识或文件名选择 IC 卡中的 MF、DDF、ADF 或 EF 文件。SELECT 命令无使用条件限制。该命令不能用于选择安全文件(SF)。

7.2.3.9.2 命令报文

SELECT 命令报文编码见表20。

表20 SELECT 命令报文

代码	数 值	代码	数 值
CLA	00	P2	00 02,选择下一个文件(P1 =04)
INS	A4		
P1	00,通过 FID 选择 DF、EF,当 Lc = 00 时,选 MF 01,通过 FID 选择 DF 02,通过 FID 选择当前 DF 下的 EF 03,选择父目录(Lc =00) 04,通过 DF 名选择应用	Lc	P1 =00 时,Lc =00 或 02 P1 =01 ~02 时,Lc =02 P1 =03 时,Lc =00 P1 =04 时,Lc =01 ~10
		Data	文件标识符(FID——两个字节) 文件名(P1 =04)
		Le	FCI 文件的信息长度(选择 DF 时)

7.2.3.9.3 命令报文数据域

命令报文数据域包括文件标识符或文件名。

7.2.3.9.4 响应报文数据域

响应报文数据域应包括所选择的 DDF 或 ADF 的 FCI。本部分不规定 FCI 中回送的附加标志。

表 21 定义了成功选择 DDF 后回送的 FCI。

表 21 SELECT DDF 的响应报文(FCI)

标签	值			存在性
6F	FCI 模板			M
	84	DF 名		M
	A5	FCI 数据专用模板		M
		88	目录基本文件的 SFI	M
		9F0C	FCI 文件内容	O
注:M——必备,O——可选。				

表 22 定义了成功选择 ADF 后回送的 FCI。

表 22 SELECT ADF 的响应报文(FCI)

标签	值			存在性
6F	FCI 模板			M
	84	DF 名		M
	A5	FCI 数据专用模板		M
		9F0C	FCI 文件内容	O
		9F08	版本信息	O
注:M——必备,O——可选。				

7.2.3.9.5 响应报文状态码

响应信息中可能出现的状态码见表 23。

表 23 SELECT 响应报文

SW1	SW2	说 明	SW1	SW2	说 明
90	00	命令执行成功	6A	81	功能不支持
62	83	选择文件无效	6A	82	未找到文件
62	84	FCI 格式与 P2 指定的不符	6A	86	P1、P2 参数错误
64	00	标志状态位未变	6A	87	Lc 与 P1、P2 不匹配
67	00	Lc 长度错误	6D	00	命令不存在

7.2.3.10 WRITE KEY 命令

7.2.3.10.1 定义和范围

WRITE KEY 命令可向卡中装载密钥或更新卡中已存在的密钥。本命令可支持八个字节或 16 个字节的密钥,密钥写入应采用加密的方式,在主控密钥的控制下进行。

在密钥装载前应用 GET CHALLENGE 命令从 TSAM 卡取一个四个字节的随机数。

7.2.3.10.2 命令报文

WRITE KEY 命令报文编码见表 24。

表 24 WRITE KEY 命令报文

代码	数 值	代码	数 值
CLA	84	Lc	14 或 1C
INS	D4	Data	加密后的密钥信息和报文鉴别代码(MAC)数据元
P1	00	Le	不存在
P2	00		

7.2.3.10.3 命令报文数据域

命令报文数据域包括要装载的密钥密文信息和 MAC。

密钥密文信息是用主控密钥对以下数据加密(按所列顺序)产生的:

——密钥用途;

——密钥版本;

——密钥算法标识;

——密钥值。

MAC 是用主控密钥对以下数据进行 MAC 计算(按所列顺序)产生的:

——CLA;

——INS;

——P1;

——P2;

——Lc;

——密钥密文信息。

加密和 MAC 计算的方法遵循 8.6.3.5 的规定。

装载八个字节的单长度密钥时,数据长度为 14h;装载 16 个字节的双长度密钥时,数据长度为 1Ch。

7.2.3.10.4 响应报文数据域

响应报文数据域不存在。

7.2.3.10.5 响应报文状态字

无论应用是否已经失效,此命令执行成功的状态字是“9000”。

TSAM 卡可能回送的错误状态字见表 25。

表 25　WRITE KEY 警告状态

SW1	SW2	说　明	SW1	SW2	说　明
65	81	内存失败	6A	81	不支持此功能
67	00	Lc 长度错	6A	86	参数 P1、P2 不正确
69	83	认证密钥锁定	6A	88	未找到密钥参数
69	84	引用数据无效(未取随机数)	6D	00	命令不存在
69	85	使用条件不满足(应用非永久锁定)	6E	00	CLA 错
69	88	安全报文数据项不正确	93	03	应用永久锁定
6A	80	数据域参数不正确			

7.2.3.11　INIT_FOR_DESCRYPT 命令

7.2.3.11.1　定义和范围

INIT_FOR_ DESCRYPT 命令用来初始化通用密钥计算过程。TSAM 卡将利用卡中指定的密钥进行运算,产生一个临时密钥。运算方式由指定的密钥类型、密钥分散级数和密钥算法标识确定。

不支持计算临时密钥计算的密钥类型有:

——主控密钥;

——维护密钥。

双长度密钥产生双长度临时密钥的密钥类型有:

——PIN 解锁密钥;

——IC 卡道路运输证件应用维护密钥。

双长度密钥左右异或产生单长度临时密钥的密钥类型有:

——重装 PIN 密钥。

双长度密钥产生双长度临时密钥,单长度密钥产生单长度临时密钥的密钥类型有:

——MAC 密钥;

——加密密钥;

——MAC、加密密钥。

指定密钥经过几级处理由密钥分散级数和 Lc 确定,若二者不一致,则返回错误信息。

临时密钥在 TSAM 卡下电后自动消失,不允许读。

临时密钥产生后,与原密钥的属性一致。

7.2.3.11.2　命令报文

INIT_FOR_DESCRYPT 命令报文编码见表 26。

表 26　INIT_FOR_DESCRYPT 命令报文

代码	数　　值	代码	数　　值
CLA	80	Lc	待处理数据的长度 00,分散级数为 0 时 08,分散级数为 1 时 10,分散级数为 2 时 其他值保留
INS	1A		
P1	密钥用途		
P2	密钥标识	Data	分散因子(Lc = “00”,不存在)
		Le	不存在

7.2.3.11.3 命令报文数据域

命令报文数据域包括待处理的输入数据。数据长度为 8 的整数倍,长度也可以为 0。密钥类型取密钥用途的低五位,密钥分散级数取密钥用途的高三位。

如待处理的输入数据包括多级分散因子,按最后一次分散因子在前、最先一次分散因子在后的顺序输入。

7.2.3.11.4 响应报文数据域

响应报文数据域不存在。

7.2.3.11.5 响应报文状态字

无论应用是否已经失效,此命令执行成功的状态字是“9000”。

TSAM 卡可能回送的错误状态字见表 27。

表 27 APPLICATION BLOCK 警告状态

SW1	SW2	说 明	SW1	SW2	说 明
67	00	Lc 长度错	6A	86	参数 P1、P2 不正确
69	82	不满足安全状态	6A	88	未找到密钥数据
69	83	认证密钥锁定	6D	00	命令不存在
69	85	使用条件不满足(应用非永久锁定)	6E	00	CLA 错
6A	81	不支持此功能	93	03	应用永久锁定

7.2.3.12 CIPHER DATA 命令

7.2.3.12.1 定义和范围

CIPHER DATA 命令利用指定的密钥进行运算。若一条命令无法传输所有的待处理数据,可分几条命令输入。

加密计算采用 ECB 模式,数据的填充在卡片外面进行,卡片只支持长度为 8 的整数倍数据的加密。

MAC 计算遵循 8.6.3.5 的规定,数据的填充在卡片外面进行,卡片只支持长度为 8 的整数倍数据的 MAC 计算。

CIPHER DATA 命令应在 INIT_FOR_ DESCRYPT 命令成功执行后才能进行。卡片状态在执行无后续块计算后,复原为通用 DES 计算初始化执行前的状态。

7.2.3.12.2 命令报文

CIPHER DATA 命令报文编码见表 28。

表 28 CIPHER DATA 命令报文

代码	数 值	代码	数 值
CLA	80	Lc	要加密的数据长度
INS	FA	DATA	要加密的数据
P1	命令引用控制参数,见表 29	Le	不存在
P2	00		

表 29　CIPHER DATA 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含　义
							x	计算模式： ——0，加密； ——1，MAC 计算
						x		后续块： ——0，无后续块； ——1，有后续块
					x			初始值(仅对 MAC 计算有效)： ——0，无初始值； ——1，有初始值

P1 值如下：

——00h，无后续块加密；

——01h，下一块 MAC 计算；

——02h，有后续块加密；

——03h，最后一块 MAC 计算；

——05h，唯一一块 MAC 计算；

——07h，第一块 MAC 计算；

——其他，保留。

7.2.3.12.3　命令报文数据域

命令报文数据域包括要加密的数据，加密数据的长度为 8 的整数倍。

在 P1 的 b3 位为 1 时，待处理数据的前八个字节为 MAC 计算的初始值。

7.2.3.12.4　响应报文数据域

在 P1 的 b1 位为 0 时，响应报文数据域包括加密结果，数据长度是 8 的整数倍。

在 P1 的 b1 位为 1，且 P1 的 b2 位为 0 时，响应报文数据域包括四个字节的 MAC。

7.2.3.12.5　响应报文状态字

此命令执行成功的状态字是“9000”。

TSAM 卡可能回送的错误状态字见表 30。

表 30　CIPHER DATA 警告状态

SW1	SW2	含　义	SW1	SW2	含　义
67	00	Lc 长度错	6A	86	参数 P1、P2 不正确
69	82	不满足安全状态	6A	88	未找到密钥数据
69	83	认证密钥锁定	6D	00	命令不存在
69	85	使用条件不满足(应用非永久锁定)	6E	00	CLA 错
6A	81	不支持此功能	93	03	应用永久锁定

8 安全机制

8.1 基本安全要求

8.1.1 共存应用

为了独立地管理一张卡上不同应用间的安全问题,每一个应用应该放在一个单独的 ADF 中,即在应用之间应该设计一道“防火墙”,以防止跨过应用进行非法访问。另外,每一个应用也不应该与个人化要求和卡中共存的其他应用规则发生冲突。

8.1.2 密钥的独立性

用于一种特定功能(如年审)的加密/解密密钥不能被任何其他功能所使用,包括保存在 IC 卡中的密钥和用来产生、派生、传输这些密钥的密钥。

8.2 密钥的关系

8.2.1 密钥关系表

IC 卡中使用的密钥均为双倍长 DEA 密钥(128bit 长),表 31 描述了 IC 卡密钥的推导方法和密钥产生的方法(个人化密钥不在本范围之内)。

表 31 密 钥 关 系 表

密　　钥	发 卡 方	IC　　卡
内部认证密钥	内部认证主密钥(MIAK)	内部认证子密钥(DIAK),由 MIAK 分散推导获得
外部认证密钥	外部认证主密钥(MEAK)	外部认证子密钥(DEAK),由 MEAK 分散推导获得
应用维护密钥	应用维护主密钥(MAMK)	应用维护子密钥(DAMK),由 MAMK 分散推导获得
文件维护密钥	文件维护主密钥(MFMK)	文件维护子密钥(DFMK),由 MFMK 分散推导获得
用于解锁 PIN 的密钥	PIN 解锁主密钥(MPUK)	PIN 解锁子密钥(DPUK),由 MPUK 分散推导获得
用于重装 PIN 的密钥	PIN 重装主密钥(MPRK)	PIN 解锁子密钥(DPRK),由 MPRK 分散推导获得

8.2.2 子密钥的推导方法

简称 Diversify,是指将一个双长度的密钥 MK,对八个字节的分散数据进行处理,推导出一个双长度的密钥 DK。

推导 DK 左半部分的方法是:

——将分散数据作为输入数据;

——将 MK 作为加密密钥;

——用 MK 对输入数据进行 3DES 运算。

推导 DK 右半部分的方法是:

——将分散数据求反,作为输入数据;

——将 MK 作为加密密钥;

——用 MK 对输入数据进行 3DES 运算。

8.3 密钥和个人密码的存放

IC 卡应该能够保证用于 3DES 算法的对称密钥及个人密码 PIN(如果使用)在 IC 卡中的安全存放,

不允许直接被导出。

8.4 内部认证

内部认证命令(INTERNAL AUTHENTICATION)用于终端设备认证卡片的合法性。其过程是IC卡利用终端设备发来的随机数和自身存储的密钥进行加密计算,由终端设备根据计算结果认证IC卡的合法性。

8.5 外部认证

外部认证命令(EXTERNAL AUTHENTICATION)用于卡片认证终端设备的合法性。其过程是IC卡利用自身存储的卡片主控密钥、应用主控密钥或应用外部认证密钥和卡片自身产生的随机数(使用GET CHALLENGE命令)进行加密计算,与接口设备传输进来的认证数据进行验证。

命令报文数据域中包含八个字节的加密数据,该数据是用主控密钥或外部认证密钥对此命令前一条命令"GET CHALLENGE"命令获得的八个字节随机数进行3DES加密运算产生的。

8.6 安全报文传送

8.6.1 目的

安全报文传送的目的是保证数据的可靠性、完整性和对发送方的认证。数据完整性和对发送方的认证通过使用MAC来实现。数据的可靠性通过对数据域的加密来得到保证。

8.6.2 安全报文传送格式

本部分中定义的安全报文传送格式符合ISO/IEC 7816-4的规定。当CLA字节的第二个半字节等于十六进制数字"4"时,表明对发送方命令数据要采用安全报文传送。卡中的FCI表明某个命令的数据域的数据是否需要加密传输,是否应该以加密的方式处理。

8.6.3 报文完整性和验证

8.6.3.1 使用MAC验证

MAC是使用命令的所有元素(包括命令头)产生的。一条命令的完整性,包括命令数据域(如果存在的话)中的数据元,通过安全报文传送得以保证。

8.6.3.2 MAC的位置

MAC是命令数据域中最后一个数据元。

8.6.3.3 MAC的长度

本标准中,MAC的长度规定为四个字节。

8.6.3.4 MAC密钥的产生

在安全信息处理过程中用到的MAC密钥,是按照7.2中描述的方式产生的。

8.6.3.5 MAC的计算

按照以下方式使用3DEA加密方式产生MAC:

——第一步:终端向IC卡发送"GET CHALLENGE",获取八个字节的随机数或获取四个字节的随机数,后补"00 00 00 00"作为初始变量;

——第二步:按照顺序将以下数据连接在一起形成数据块:

1) CLA,INS,P1,P2,Lc

注:Lc 包括命令数据域后面四个字节 MAC 数据的长度,例如:APPLICATION BLOCK 命令需要产生一个 MAC,计算 MAC 的 Lc 的输入值是 4~FE,而不是 0,CLA 包括安全报文的表明("X4")。

2) 在命令的数据域中(如果存在)包含明文或加密的数据(例如:如果要更改车辆年审信息,加密后的车辆年审信息数据块放在命令数据域中传输)。

对于 RELOAD PIN 中的 MAC 计算,上述步骤为:

——第一步:将一个八个字节长的初始变量设定为十六进制的"0x 00 00 00 00 00 00 00 00";

——第二步:新 PIN 值为输入数据块;

——第三步:将该数据块分成八个字节为单位的数据块,标号为 D1、D2、D3、D4 等,最后一个数据块的长度有可能是一个至八个字节;

——第四步:如果最后一个数据块的长度是八个字节,则在其后加上十六进制数字"80 00 00 00 00 00 00 00",转到第五步;如果最后一个数据块的长度不足八个字节,则在其后加上十六进制数字"80",如果达到八个字节长度,则转入第五步;否则在其后加入十六进制数字"0",直到长度达到八个字节;

——第五步:对这些数据块使用指定的 MAC 密钥进行加密,密钥按照 8.2 描述的方式产生;安全报文传送的处理支持双长度 MAC DEA 密钥,则使用 MAC 计算密钥 A 和 B(MAC 的产生见图 3);

注:根据第二步产生的数据块的长度,计算过程有可能多于或少于四步。

——第六步:最终得到从计算结果左侧取得的四个字节长度的 MAC。

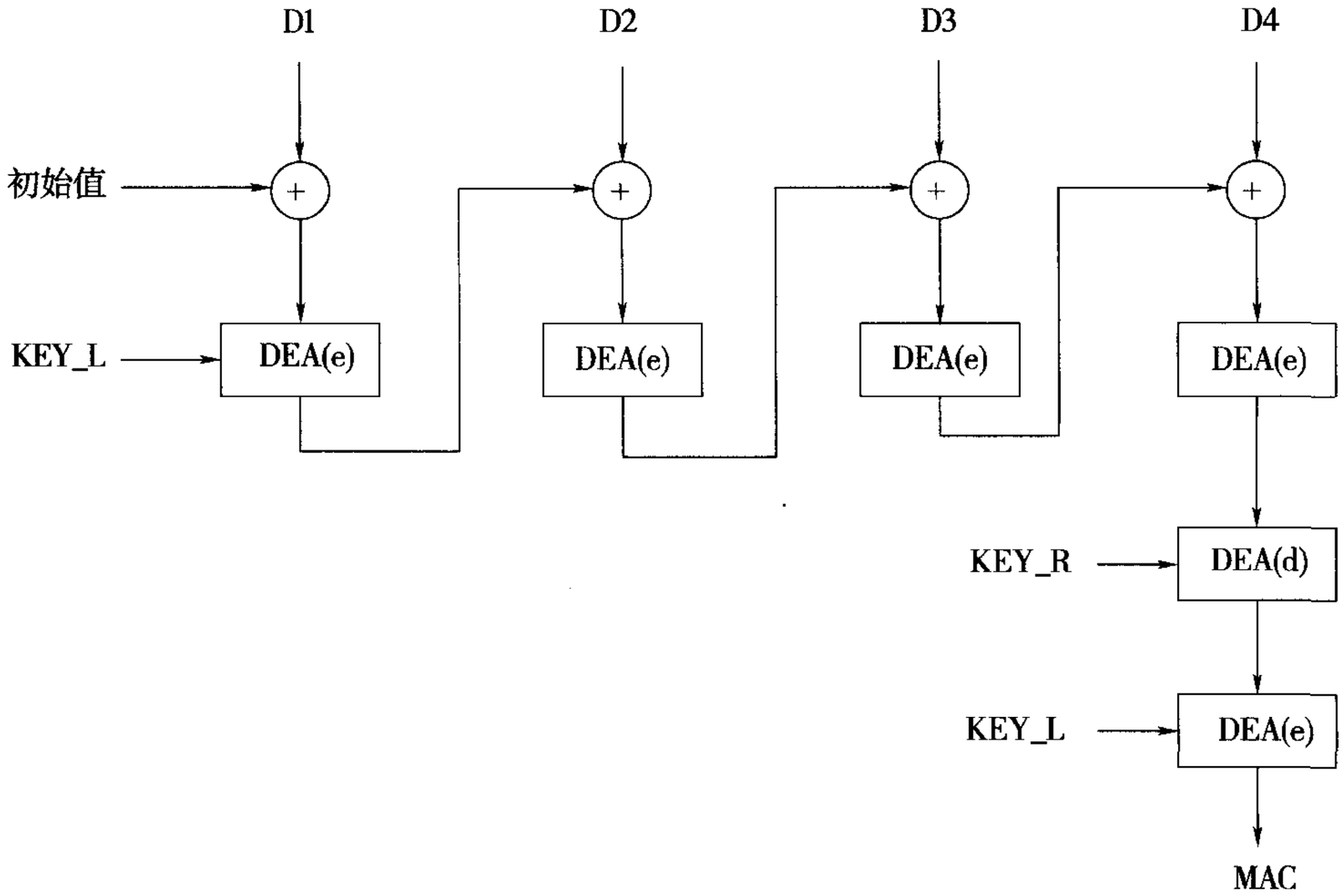

图 3 双长度 DEA KEY 的 MAC 算法

8.6.4 数据可靠性

8.6.4.1 数据加密密钥的计算

在安全报文处理过程中用到的数据,加密过程中用到的密钥是按照 8.2 中描述的方式产生的。

8.6.4.2 被加密数据的结构

当命令中要求的明文数据需要加密时,它先要被格式化为以下形式的数据块:

——明文数据的长度,不包括填充字符(LD);
——明文数据块;
——填充字符(根据 8.6.4.3)。
然后整个数据块使用 8.6.4.3 中描述的数据加密技术进行加密。

8.6.4.3 数据加密计算

数据加密技术如下:
——第一步:用 LD 表示明文数据的长度,在明文数据前加上 LD 产生新的数据块;
——第二步:将第一步中生成的数据块分解成八个字节数据块,标号为 D1、D2、D3、D4 等,最后一个数据块的长度有可能不足八位;
——第三步:如果最后(或唯一)一个数据块的长度等于八个字节,转入第四步;如果不足八个字节,在右边添加十六进制数字“80”,如果长度已达八个字节,转入第四步;否则,在其右边添加十六进制数字“0”,直到长度达到八个字节;
——第四步:每一个数据块使用 8.6.4.1 中描述的数据加密方式加密,加密过程见图 4;
——第五步:计算结束后,所有加密后的数据块依照原顺序连接在一起(加密后的 D1、加密后的 D2 等),并将结果数据块插入到命令数据域中。

8.6.4.4 数据解密计算

卡片接收到命令之后,需要将包含在命令中的加密数据进行解密。数据解密的技术如下:
——第一步:将命令数据域中的数据块分解成八个字节长的数据块,标号为 D1、D2、D3、D4 等;每个数据块使用按 8.6.4 所描述的方法产生的数据加密过程密钥进行解密;采用双长度数据加密的 DEA 密钥,则数据块的解密见图 5(使用数据加密过程密钥 A 和 B 来进行解密);

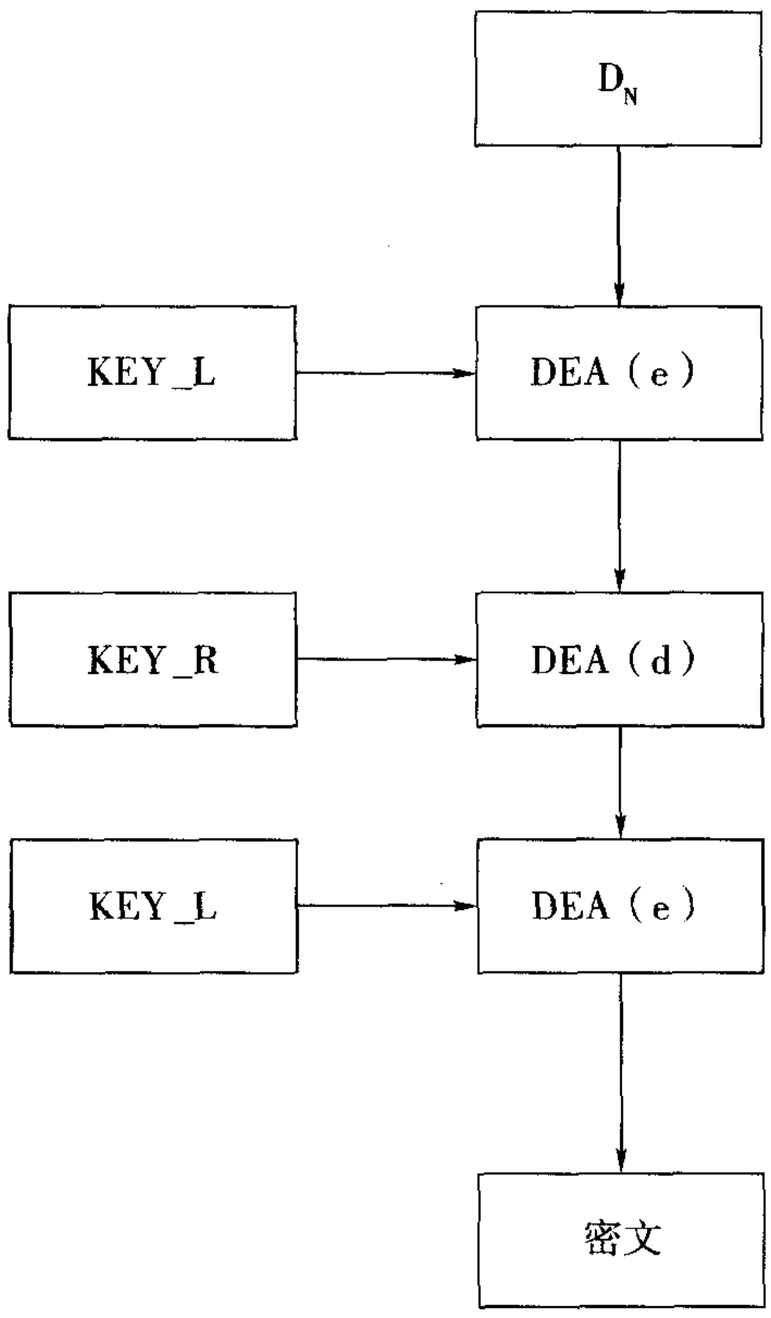

图 4 使用双长度 DEA 密钥的数据加密

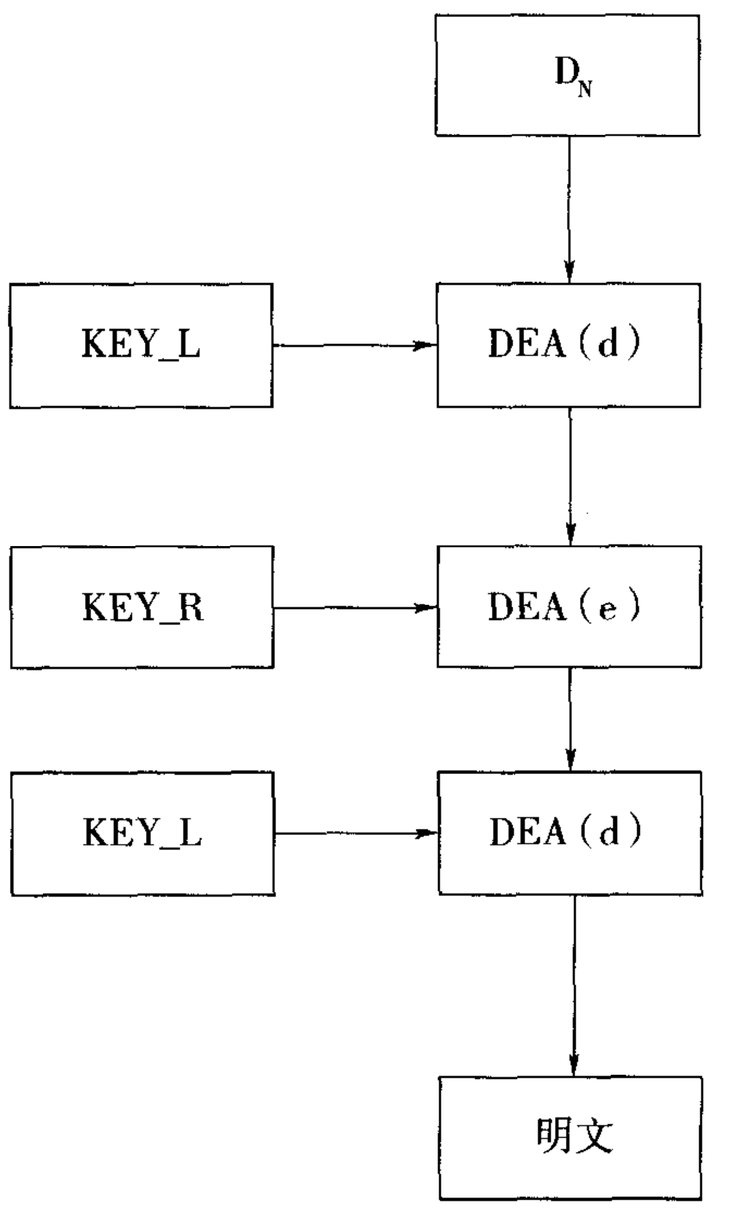

图 5 使用双长度 DEA 密钥的数据解密

——第二步:计算结束后,所有解密后的数据块依照顺序(解密后的 D1、解密后的 D2 等)连接在一

起,数据块由 LD、明文数据、填充字符(如果在 8.6.4.3 描述的加密过程中增加的话)组成;

——第三步:因为 LD 表示明文数据的长度,因此,它被用来恢复明文数据。

8.6.5 安全报文传送的命令情况

在 ISO/IEC 7816-4 中定义了四种命令情况,本节简单地讨论这些情况对命令 APDU 的作用。

情况一:这种情况下,没有数据传送到 ICC(Lc)中,也没有数据从卡中返回(Le)。

没有安全报文传送要求的命令情况如下:

CLA	INS	P1	P2

有安全报文传送要求的命令情况如下:

CLA	INS	P1	P2	Lc	MAC

CLA 的第二个半字节是“4”,表明支持第二种情况的安全报文传送技术。Lc 为 MAC 的长度。

情况二:这种情况下,命令中没有数据传送到卡中,但有数据从卡中返回。

没有安全报文传送要求的命令情况如下:

CLA	INS	P1	P2	Le

有安全报文传送要求的命令情况如下:

CLA	INS	P1	P2	Lc	MAC	Le

CLA 的第二个半字节是“4”,表明支持第二种情况的安全报文传送技术。Lc 为 MAC 的长度。

情况三:这种情况下,命令中有数据传送到卡中,但没有数据从卡中返回。

没有安全报文传送要求的命令情况如下:

CLA	INS	P1	P2	Lc	命令数据

有安全报文传送要求的命令情况如下:

CLA	INS	P1	P2	Lc	命令数据	MAC

CLA 的第二个半字节是“4”,表明支持第二种情况的安全报文传送技术。Lc 为命令数据加上 MAC 的长度。

情况四:这种情况下,命令中有数据传送到卡中,也有数据从卡中返回。

没有安全报文传送要求的命令情况如下:

CLA	INS	P1	P2	Lc	命令数据	Le

有安全报文传送要求的命令情况如下:

CLA	INS	P1	P2	Lc	命令数据	MAC	Le

CLA 的第二个半字节是“4”,表明支持第二种情况的安全报文传送技术。Lc 为命令数据加上 MAC 的长度。

8.7 加密算法

8.7.1 认可的加密算法

采用国家认可和推荐的算法,可以随着系统的深入进行算法升级。

8.7.2 对称算法(3DES)

安全报文允许使用 3DES 加密算法,以下定义的 3DES 加密版本都可以用在加密运算和 MAC 机制中。

3DES 加密是指使用双长度(16 个字节)密钥 K = (KL||KR)将八个字节明文数据块加密成密文数据块,如下所示:

$$Y = DES(KL)[DES^{-1}(KR)[DES(KL)[X]]]$$

解密的方式如下:

$$X = DES^{-1}(KL)[DES(KR)[DES^{-1}(KL)[Y]]]$$

9 应用选择

9.1 应用选择方式及步骤

应用的选择可通过文件标识符(FID)或 AID 方式直接进行。

本节从卡片和终端两个角度描述了采用 AID 方式进行应用选择的过程。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道路运输系统应用进行交易,其过程分两个步骤:

——步骤 1:建立卡与终端两者共同支持的应用列表;

——步骤 2:在步骤 1 生成的应用列表中选择一个将要运行的应用。

本节描述了为完成正确的应用选择所需要的卡上的必要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。

一种道路运输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;

—— 一套卡和终端共同遵守的应用协议。

所有应用可以由唯一的一个 AID 标识或者文件标识符标识。应用标识符的格式符合 ISO/IEC 7816-5 的有关规定。

这里描述的道路运输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,这些终端能够支持符合本部分的 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道路运输应用;

—— 尽可能保护现存应用;

—— 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 ADF,ADF 中定义了 IC 卡中所支持某种应用的一组数据。

9.2 应用标识符的编码

AID 的结构符合 ISO/IEC 7816-5 的有关规定,由道路运输证件系统自行指定。

9.3 道路运输系统环境结构 MF-AID

在 IC 卡道路运输证件上,道路运输系统环境起始于一个名为 1RTS. SYS. DDF01 的 DDF。该文件是

必须存在的。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。与其他 DDF 类似,这个 DDF 包含了道路运输系统的目录。初始 DDF 所附属的目录包含了 ADF 的入口地址,该目录也可以包含其他 DDF 的入口地址。

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,才具备国际互通性。

9.4 道路运输系统目录编码

道路运输系统目录(下文简称目录)是一个线性文件,用 1 ~ 10 的 SFI 标识。

该目录附属于 DDF,目录的 SFI 包含在 DDF 文件控制信息中。目录可以使用 READ RECORD 命令进行读取。

目录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。

道路运输系统目录的每一个入口地址都是一个应用模板。

9.5 目录入口中执行的命令的使用

一个目录入口地址总是与卡中的一个 DF 相对应。

如果在目录入口地址中没有指定一个“执行的命令”,则需执行 SELECT 命令来选择入口地址中指定的 DF,并使用目录中 ADF 名或 DDF 名作为文件名。有些 IC 卡对 SELECT 命令的解释具有二义性,比如对于支持 DF 部分名的 IC 卡就有可能将其入口地址中指定的文件名当成另一 DF 文件的部分名而造成选择应用错误。

“执行的命令”作为一种机制提供给 IC 卡,使得 IC 卡可以利用这个机制准确地选择正确的 DF,即选择与目录入口地址对应的 DF。“执行的命令”可以是 SELECT 命令的变形,即不一定是“按名称选择”的形式(例如按路径或文件标识选择);也可以是其他命令,通过这些命令也能实现正确选择 DF 的结果并返回 FCI。当“执行的命令”数据项存在时,终端会利用它代替“按名称选择”命令来选择相关的 DF。

9.6 其他目录的编码

除了初始目录之外,其他目录在道路运输系统环境下都是可选的,对此类目录的存在数目没有明确限制。每一个目录由一个目录 SFI 定位,SFI 存放在每个 DDF 的 FCI 中。目录 SFI 包括执行 READ RECORD 命令读目录时所用的 SFI。当包含该目录的 DDF 为当前选定的文件时,SFI 可用来读此目录。

目录 SFI 数据应出现在一个 DDF(FCI 专用模板)的 FCI 专用数据区域内。一个 DDF 最多包含一个目录,因此目录 SFI 数据只在 FCI 中出现一次。

除了初始目录之外,所有目录入口均为 ADF 文件,或以包含目录 DDF 名称开始的 DDF。所有目录(包括初始目录)的格式相同。

9.7 终端的应用选择

9.7.1 直接选择应用

如果一个终端支持的应用不多,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 SW1SW2 =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 SW1SW2 不等于“9000”,或者即使 IC 卡回送 SW1SW2 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,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。

直接选择适用于那些仅支持较少应用的终端,并且不能支持持卡人潜在的应用。这种方式不支持终端访问应用标签或应用优先名称,这些名称仅存在于目录中。

9.7.2 道路运输系统目录的使用

如果终端支持大量的应用,可以通过使用 IC 卡的目录(或多个目录)来确定卡片所支持的应用。应保证 IC 卡目录的结构设计正确。

终端正确使用目录的步骤如下:

——终端首先在道路运输系统环境下用 SELECT 命令对文件“1RTS. SYS. DDF01”直接选择,由此建立道路运输系统环境并进入初始目录;

——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 SW1SW2 =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 SW1SW2 =6A83,则表示目录为空;

——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;

——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 1234 的 DDF 可与一个名为 12345678 的 AID 匹配),则终端选择该 DDF;如果该入口包含一个“执行的命令”,则执行该命令完成选择;如果不存在“执行的命令”,终端发出带 DDF 名的 SELECT 命令;使用所选 DDF 的文件控制信息(FCI)中的目录短文件标识符(SFI),读出目录并按照步骤 2 到步骤 5 的过程进行处理,之后终端继续回到上一个目录处理;

——当终端处理完第一个目录的列表后,所有能够按此方式找到的 ADF 就确定了,查找完毕;

——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 找出本地的或非道路运输应用的专用选择方式),但不在本部分范围之内。

9.7.3 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。可通过以下方法实现:

——如果没有互相支持的应用,业务处理终止;

——如果只有一个相互支持的应用,终端核查应用优先表明符的 b8 位;如果 b8 等于“0”,终端选择该应用;如果 b8 等于“1”并且终端规定要有持卡人的确认,在这种情况下,终端需要向持卡人提出确认请求,如持卡人同意,即选择该应用;如果终端没有规定要有持卡人的确认,或者终端请求确认被拒绝,终端终止该业务;

——建议显示应用列表请持卡人选择,将采用级别优先方式为持卡人提供应用列表目录,高优先级别的应用在先,如果卡中没有指定优先顺序,则以终端的应用优先顺序为准;如果终端也没有指定优先顺序,则按照应用在卡中出现的顺序为准;如果出现多个应用重复指定优先顺序,或个别入口地址缺少应用优先表明符的情况,也可采用类似的方法,也就是说,在这种情况下终端可以使用自己的优先顺序,也可以按卡上顺序将有重复优先符或无优先符的应用显示出来;

——终端可在没有持卡人协助的情况下选择应用,在这种情况下,终端应从相互支持的应用列表中选择优先级别最高的应用,如果终端不能对选择的应用提供确认,则应用选择禁止(应用优先表明符的 b8 等于“1”)。

一旦终端或持卡人确定了待执行的应用，则该应用被选中。如果与应用相关的目录入口地址指定了一个“执行的命令”，终端执行该命令进行应用的选择。如果不存在“执行的命令”，终端发出一个 SELECT 命令进行应用的选择。无论使用哪种命令，如果命令回送的 SW1SW2 值不等于“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，或者选择下一个优先级高的应用，重新进行应用选择。在合适的情况下，终端要给持卡人以提示。