第43号

交通运输部关于发布高速公路复合通行卡(CPC)技术要求的公告

为贯彻落实党中央、国务院决策部署，加快推动高速公路不停车快捷收费发展，交通运输部组织制定了《高速公路复合通行卡(CPC)技术要求》，现予以公布，自公布之日起施行。

该技术要求的管理权和解释权归交通运输部，日常解释和管理工作由主编单位交通运输部公路科学研究院负责。请各有关单位注意总结经验，及时将发现的问题和修改意见函告交通运输部公路科学研究院（地址：北京市海淀区西土城路8号，邮编：

100088)，以便修订时参考。

交通运输部

2019 年 6 月 9 日

高速公路复合通行卡（CPC）技术要求

2019 年 6 月

目　　录

1 总则

为保障取消高速公路省界收费站相关工作开展，在《收费公路联网收费多义性路径识别技术要求》（交通运输部公告2015年第40号）和《高速公路复合通行卡（CPC）技术要求（试行）》（交办公路函〔2018〕1677号）文件基础上，根据《取消高速公路省界收费站总体技术方案》（交办公路函〔2019〕320号）文件规定，对复合通行卡（CPC）相关要求进行调整和补充规定。

2 规范性引用文件

下列文件中的条款通过本技术要求的引用而成为本技术要求的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本技术要求。凡是不注日期的引用文件，其最新版本适用于本技术要求。

（1）GB/T 20851.2《电子收费 专用短程通信 第 2 部分：数据链路层》。

（2）GB/T 20851.3《电子收费 专用短程通信 第 3 部分：应用层》。

（3）GB/T 2423.10–2008《电工电子产品环境试验 第2 部分: 试验方法 试验Fc: 振动(正弦)》。

（4）GB/T 2423.5《电工电子产品环境试验 第二部分: 试验方法试验 Ea 和导则: 冲击》。

（5）《收费公路联网收费技术要求》（原交通部 2007 年第 35 号公告）。

（6）《收费公路联网电子不停车收费技术要求》（交通运输部2011年第13号公告）。

（7）《收费公路联网收费多义性路径识别技术要求》（交通运输部公告2015年第40号公告）。

（8）《取消高速公路省界收费站总体技术方案》（交办公路函〔2019〕320 号文件）。

（9）《高速公路复合通行卡（CPC）技术要求（试行）》（交办公路函〔2018〕1677号文件）。

（10）《电子收费 单片式车载单元（OBU）技术要求》（交通运输部公告2019年第35号）。

（11）《高速公路ETC门架系统技术要求》（交办公路函〔2019〕856号文件）。

3 术语、定义和缩略语

3.1 术语和定义

《收费公路联网收费多义性路径识别技术要求》（交通运输部公告2015年第40号）中确定的术语适用于本技术要求。

3.2 分段计费

将高速公路全线划分为若干路段，各路段分别计算通行费额。

3.3 ETC门架系统

在高速公路沿线断面建设的，具备通行费分段计费、车牌图像识别等功能的专用系统及配套设施。

3.4 缩略语

下列缩略语适用于本技术要求。

CPC——复合通行卡（Compound Pass Card）

DSRC——专用短程通信（Dedicated Short Range Communication）

ETC——电子收费（Electronic Toll Collection）

FID ——文件标识（File Identifier）

MAC——信息鉴别码（Message Authentication Code）

OBU——车载单元（On Board Unit）

RSU——路侧单元（Roadside Unit）

SM4——国产密码算法 SM4

3DES——三重数据加密标准（Triple Data Encryption Standard）

4 基本规定

按照《取消高速公路省界收费站总体技术方案》（交办公路函〔2019〕320号）文件，取消高速公路省界收费站，设置ETC门架系统，MTC车辆采用5.8GHz复合通行卡（CPC）作为通行介质，实现“分段计费、出口收费”。

CPC卡应满足以下要求：

1. 收费车道系统与CPC卡间的通信应具备双向认证功能，即CPC卡应验证收费车道终端设备的合法性，收费车道终端设备也应验证CPC卡的合法性。双向认证通过后，收费车道系统才能对CPC卡进行写操作。
2. ETC门架系统与CPC卡间采用5.8GHz DSRC通信方式将计费信息和过站信息写入CPC卡内。
3. CPC卡采用部省两级密钥体系，ETC门架系统及入/出口收费车道系统的PSAM卡或PCI密码卡应统一装载部级主密钥。
4. CPC卡相关加解密运算采用SM4国产对称密码算法。

5 技术指标

5.1 物理层参数指标

CPC卡的13.56MHz物理层参数指标应符合ISO/IEC 14443 TYPE-A标准的相关规定。

CPC卡的5.8GHz物理层参数指标应符合表5.1-1规定。

表5.1-1 CPC卡5.8GHz物理层参数指标

序号	指标		要求
1	载波频率		信道 1：5.79GHz
			信道 2：5.80GHz
2	频率容限		±200ppm
3	占用带宽		≤5MHz
4	e.i.r.p.		≤10dBm
5	杂散 发射	30MHz-1000MHz	≤-36dBm/100kHz
		2400MHz-2483.5MHz	≤-40dBm/1MHz
		3400MHz-3530MHz	≤-40dBm/1MHz
		5725MHz-5850MHz	≤-33dBm/100kHz
		其他 1GHz-20GHz	≤-30dBm/1MHz
6	邻道泄漏功率比		≤-30dB
7	天线极化		线极化或右旋圆极化
8	天线方向性	水平	全向
		垂直	全向
9	调制方式		ASK
10	调制系数		0.7～0.9
11	编码方式		FM0
12	位速率		512kbit/s
13	位时钟精度		$\pm 1000\times 10^{-6}$
14	唤醒方式		14k 方波唤醒或者正常通信帧信号唤醒

15	唤醒灵敏度	≤-50dBm
16	接收灵敏度	≤-65dBm
17	接收带宽	5.825GHz-5.845GHz

表5.1-1 CPC卡5.8GHz物理层参数指标（续）

序号	指标	要求
18	BER	10×10^{-6}
19	前导码	16 位“1”加 16 位“0”
20	后导码	最多 8 位

5.2 应用要求

CPC卡与IC卡读写器之间的通信应符合ISO/IEC 14443 TYPE-A标准的相关规定，CPC卡入/出口车道交互流程详见附录A。

CPC卡与ETC门架系统之间的DSRC通信应符合GB/T 20851.2、GB/T 20851.3及本技术要求的相关规定。非省界路段ETC门架系统RSU与CPC卡间的DSRC通信流程见《高速公路ETC门架系统技术要求》7.4，省界ETC门架系统RSU与CPC卡间的DSRC通信流程应见《高速公路ETC门架系统技术要求》7.4。

CPC卡发行流程详见附录B。

CPC卡应符合GB/T 20851.2、GB/T 20851.3中OBU服务原语的相关规定。

CPC卡应支持微波唤醒，定时周期唤醒功能可选。

CPC卡应支持使用IC卡读写器打开、关闭等管理功能。

5.3 应用命令集

5.3.1 EXTERNAL AUTHENTICATION 命令

5.3.1.1 定义和范围

EXTERNAL AUTHENTICATION命令利用CPC卡内部的计算结果，有条件地修改安全状态。计算的方法是利用CPC卡的外部认证密钥，对CPC卡产生的随机数（使用GET CHALLENGE命令）和接口设备传输进来的认证数据进行验证。

5.3.1.2 命令报文

EXTERNAL AUTHENTICATION命令报文编码见表5.3-1。

表5.3-1 EXTERNAL AUTHENTICATION命令报文

代码	值
CLA	‘00’
INS	‘82’
P1	‘00’
P2	外部认证密钥标识
Lc	‘08’
Data	认证数据
Le	不存在

5.3.1.3 命令报文数据域

命令报文数据域中包含8字节的加密数据，该数据是用P2指定的密钥对此命令前一条命令“GET CHALLENGE”命令获得的随机数做SM4加密运算产生的16字节密文前后8字节异或的结果。

5.3.1.4 响应报文数据域

响应报文数据域不存在。

5.3.1.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

CPC卡回送的错误状态码见5.3-2。

表 5.3-2 EXTERNAL AUTHENTICATION 错误状态

SW1	SW2	说　明
‘63’	‘CX’	认证失败，‘X’为剩余的可尝试次数
‘67’	‘00’	Lc 不正确
‘69’	‘83’	认证方法锁定
‘6A’	‘86’	参数 P1、P2 不正确
‘6D’	‘00’	INS 错
‘6E’	‘00’	CLA 错

5.3.2 GET CHALLENGE 命令

5.3.2.1 定义和范围

GET CHALLENGE命令请求一个用于安全相关过程（如安全报文）的随机数。

该随机数只能用于下一条指令，无论下一条指令是否使用了该随机数，该随机数都将立即失效。

5.3.2.2 命令报文

GET CHALLENGE命令报文见5.3-3。

表 5.3-3 GET CHALLENGE 命令报文

代码	值
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’
Lc	不存在
Data	不存在
Le	‘04’，‘08’

5.3.2.3 命令报文数据域

命令报文数据域不存在。

5.3.2.4 响应报文数据域

响应报文数据域包括随机数，长度为4字节或8字节。

5.3.2.5 响应报文状态码

CPC卡回送的响应信息中出现的状态码见5.3-4。

表5.3-4 GET CHALLENGE 响应报文状态码

SW1	SW2	说　明
‘90’	‘00’	命令执行成功
‘67’	‘00’	Le 长度错误
‘6A’	‘81’	功能不支持
‘6A’	‘86’	P1、P2 参数错
‘6D’	‘00’	INS 错
‘6E’	‘00’	CLA 错

5.3.3 GET RESPONSE 命令

5.3.3.1 定义和范围

当APDU不能用现有协议传输时，GET RESPONSE命令提供了一种从CPC卡向接口设备传送APDU（或APDU的一部分）的传输方法。

5.3.3.2 命令报文

GET RESPONSE命令报文见表5.3-5。

表5.3-5 GET RESPONSE命令报文

代码	值
CLA	‘00’
INS	‘C0’
P1	‘00’
P2	‘00’
Lc	不存在
Data	不存在
Le	响应的最大数据长度

5.3.3.3 命令报文数据域

命令报文数据域不存在。

5.3.3.4 响应报文数据域

响应报文数据域的长度由Le的值决定。

如果Le的值为零，在附加数据有效时，CPC卡应回送状态码‘6CXX’，否则回送状态码‘6F00’。

5.3.3.5 响应报文状态码

CPC卡回送的响应信息中出现的状态码见5.3-6。

表5.3-6 GET RESPONSE响应报文状态码

SW1	SW2	说　明
‘90’	‘00’	命令执行成功
‘61’	‘XX’	还有‘XX’字节需要返回
‘62’	‘81’	回送数据有错
‘67’	‘00’	Lc 或 Le 长度错误
‘6A’	‘86’	P1、P2 参数错
‘6C’	‘XX’	长度错误，‘XX’表示实际长度
‘6D’	‘00’	INS 错
‘6E’	‘00’	CLA 错
‘6F’	‘00’	数据无效

5.3.4 Get SN 命令

5.3.4.1 定义和范围

读取CPC卡安全模块中卡商唯一的芯片序列号，自由读取。

5.3.4.2 命令报文

Get SN命令报文见表5.3-7。

表5.3-7 Get SN命令报文

代码	值
CLA	‘80’
INS	‘F6’
P1	‘00’
P2	‘03’

Lc	不存在
Data	不存在
Le	‘04’

5.3.4.3 命令报文数据域

命令报文数据域不存在。

5.3.4.4 响应报文数据域

响应报文数据域包括4字节芯片序列号。

5.3.4.5 响应报文状态码

CPC卡回送的响应信息中出现的状态码见表5.3-8。

表5.3-8 Get SN响应报文状态码

SW1	SW2	说　明
‘90’	‘00’	命令执行成功
‘6A’	‘86’	P1、P2 参数错
‘6C’	‘XX’	Le 错误。‘XX’表示实际长度
‘6D’	‘00’	命令不存在
‘6E’	‘00’	CLA 错

5.3.5 INTERNAL AUTHENTICATION 命令

5.3.5.1 定义和范围

INTERNAL AUTHENTICATION命令提供了利用接口设备发来的随机数和自身存储的相关密钥进行数据认证的功能。

5.3.5.2 命令报文

INTERNAL AUTHENTICATION命令报文编码见表5.3-9。

表5.3-9 INTERNAL AUTHENTICATION 命令报文

代码	值
CLA	‘00’
INS	‘88’

P1	‘00’
P2	内部认证密钥标识
Lc	认证数据的长度
Data	认证数据
Le	‘00’

5.3.5.3 命令报文数据域

命令报文数据域的内容是应用专用的认证数据。

5.3.5.4 响应报文数据域

响应报文数据域内容是相关认证数据。

5.3.5.5 响应报文状态字

此命令执行成功的状态字是“9000”。CPC卡可能回送的警告状态字见表5.3-10。

表5.3-10 INTERNAL AUTHENTICATION 警告状态

SW1	SW2	说　明
‘62’	‘81’	回送的数据可能有错

CPC卡可能回送的错误状态字见表5.3-11。

表5.3-11 INTERNAL AUTHENTICATION 错误状态

SW1	SW2	说　明
‘64’	‘00’	标志状态位未变
‘67’	‘00’	Lc 域不存在
‘68’	‘82’	不支持安全报文
‘69’	‘85’	不满足使用条件
‘6A’	‘80’	数据域参数不正确
‘6A’	‘86’	P1、P2 参数错
‘6D’	‘00’	INS 错

5.3.6 READ BINARY 命令

5.3.6.1 定义和范围

READ BINARY命令用于读出二进制文件的内容（或部分内容）。

5.3.6.2 命令报文

READ BINARY命令报文见表5.3-12。

表5.3-12 READ BINARY命令报文

代码	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								
Lc	1）不存在——明文方式 2）‘04’——校验方式								
Data	1）不存在 2）MAC								
Le	期望返回的数据长度								

5.3.6.3 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。

5.3.6.4 响应报文数据域

当Le的值为零时，只要文件的最大长度在256字节（短长度）或65536字节（扩展长度）之内，则其全部字节将被读出。

5.3.6.5 响应报文状态码

CPC卡回送的响应信息中的状态码见表5.3-13。

表5.3-13 READ BINARY响应报文状态码

SW1	SW2	说 明
‘90’	‘00’	命令执行成功
‘61’	‘XX’	还有 XX 字节要返回
‘62’	‘81’	部分回送的数据有错

‘62’	‘82’	文件长度<Le
‘65’	‘81’	写 EEPROM 失败
‘67’	‘00’	Lc 长度错误
‘69’	‘81’	当前文件不是二进制文件
‘69’	‘82’	不满足安全状态
‘69’	‘83’	认证密钥锁定
‘69’	‘84’	引用数据无效（未申请随机数）
‘69’	‘85’	使用条件不满足
‘69’	‘86’	没有选择当前文件
‘69’	‘88’	安全信息（MAC 和加密）数据错误
‘6A’	‘81’	功能不支持
‘6A’	‘82’	未找到文件
‘6A’	‘86’	P1、P2 参数错
‘6A’	‘88’	未找到密钥数据
‘6B’	‘00’	起始地址超出范围
‘6C’	‘XX’	Le 长度错误。‘XX’表示实际长度
‘6D’	‘00’	INS 错
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用永久锁定

5.3.7 READ RECORD 命令

5.3.7.1 定义和范围

READ RECORD命令读记录文件中的内容。

5.3.7.2 命令报文

READ RECORD命令报文见表5.3-14。

表5.3-14 READ RECORD命令报文

代码	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 指定的记录号
	其他值								保留
Lc	1）不存在——明文方式 2）‘04’—— 命令 报文校验方式								
DATA	1）不存在——明文方式 2）MAC——校验方式								
Le	期望返回的记录数据								

5.3.7.3 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。

5.3.7.4 响应报文数据域

所有执行成功的READ RECORD命令的响应报文数据域由读取的记录组成。

5.3.7.5 响应报文状态码

CPC卡回送的响应信息中的状态码见表5.3-15。

表5.3-15 READ RECORD响应报文状态码

SW1	SW2	说　明
‘90’	‘00’	命令执行成功
‘61’	‘XX’	还有 XX 字节需要返回
‘62’	‘81’	回送的数据有错
‘64’	‘00’	标志状态位没变
‘65’	‘81’	写 EEPROM 失败
‘67’	‘00’	Lc 长度错误
‘69’	‘81’	当前文件不是记录文件

表5.3-15 READ RECORD响应报文状态码（续）

SW1	SW2	说　明
‘69’	‘82’	不满足安全状态
‘69’	‘83’	认证密钥锁定
‘69’	‘84’	引用数据无效(未申请随机数)

‘69’	‘85’	使用条件不满足
‘69’	‘86’	没有选择当前文件
‘69’	‘88’	安全信息（MAC 和加密）数据错误
‘6A’	‘81’	功能不支持
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录
‘6A’	‘85’	Lc 与 TLV 结构不匹配
‘6A’	‘86’	P1、P2 参数错
‘6A’	‘88’	未找到密钥数据
‘6C’	‘XX’	Le 错误，‘XX’表示实际长度
‘6D’	‘00’	INS 错
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用永久锁定

5.3.8 SELECT FILE 命令

5.3.8.1 定义和范围

—— SELECT FILE 命令通过文件标识或应用名选择 CPC 卡中的 MF、DDF、ADF 或 EF 文件。

—— 成功执行该命令设定 MF、DDF 或 ADF 的路径。

—— 应用到 EF 的后续命令将采用 SFI 方式联系到所选定的 MF、DDF 或 ADF。

—— 从 CPC 卡返回的应答报文包含回送 FCI。

—— FCI 数据从数据分组中获得。

5.3.8.2 命令报文

SELECT FILE命令报文见表5.3-16。

表5.3-16 SELECT FILE命令报文

代码	值
CLA	‘00’
INS	‘A4’
P1	‘00’通过 FID 选择 DF、EF，当 Lc=‘00’时，选 MF ‘04’通过 DF 名选择应用
P2	‘00’ ‘02’选择下一个文件（P1=‘04’时）
Lc	P1=‘00’时，Lc=‘00’或‘02’ P1=‘04’时，Lc=‘05’~‘10’
Data	文件标识符（FID—2 字节） 应用名（App-Name，P1=‘04’）
Le	FCI 文件的信息长度（选择 DF 时）

5.3.8.3 命令报文数据域

命令报文数据域应包括所选择的DDF名、DF名或FID，以及EF的FID。

5.3.8.4 响应报文数据域

响应报文数据域中的数据应包括所选择的MF、DDF、ADF的FCI。

成功选择MF后回送的FCI定义见表5.3-17。

表5.3-17 成功选择MF响应报文FCI

标识	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

成功选择DDF后回送的FCI定义见表5.3-18。

表5.3-18 成功选择DDF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

成功选择ADF后回送的FCI定义见表5.3-19。

表5.3-19 成功选择ADF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

5.3.8.5 响应报文状态码

CPC卡回送的响应信息中的状态码见表5.3-20。

表5.3-20 SELECT FILE响应报文状态码

SW1	SW2	说　明
'90'	'00'	命令执行成功
'62'	'83'	选择文件无效
'62'	'84'	FCI 格式与 P2 指定的不符
'64'	'00'	标志状态位没变
'67'	'00'	Lc 长度错误
'6A'	'81'	功能不支持
'6A'	'82'	未找到文件
'6A'	'86'	P1、P2 参数错
'6A'	'87'	Lc 与 P1、P2 不匹配
'6D'	'00'	INS 错
'6E'	'00'	CLA 错
'93'	'03'	应用永久锁定

5.3.9 UPDATE BINARY 命令

5.3.9.1 定义和范围

UPDATE BINARY命令用于更新二进制文件中的数据。

5.3.9.2 命令报文

UPDATE BINARY命令报文见表5.3-21。

表5.3-21 UPDATE BINARY命令报文

代码	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 域数据长度								
Data	明文方式：　　明文数据 加密方式：　　密文数据 校验方式：　　明文数据||校验码 校验加密方式：密文数据||校验码								
Le	不存在								

5.3.9.3 命令报文数据域

命令报文数据域包括更新原有数据的数据域。

5.3.9.4 响应报文数据域

响应报文数据域不存在。

5.3.9.5 响应报文状态码

CPC卡回送的响应信息中的状态码见表5.3-22。

表5.3-22 UPDATE BINARY响应报文状态码

SW1	SW2	说　明
‘90’	‘00’	命令执行成功
‘65’	‘81’	写 EEPROM 失败
‘67’	‘00’	Lc 长度错误
‘69’	‘81’	当前文件不是二进制文件
‘69’	‘82’	不满足安全状态
‘69’	‘83’	认证密钥锁定
‘69’	‘84’	引用数据无效（未申请随机数）
‘69’	‘85’	使用条件不满足
‘69’	‘86’	未选择文件
‘69’	‘88’	安全信息（MAC 和加密）数据错误

表5.3-22 UPDATE BINARY响应报文状态码（续）

SW1	SW2	说　明
‘6A’	‘81’	功能不支持
‘6A’	‘82’	未找到文件
‘6A’	‘86’	P1、P2 参数错
‘6A’	‘88’	未找到密钥数据
‘6B’	‘00’	起始地址超出范围
‘6D’	‘00’	INS 错
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用永久锁定

5.3.10UPDATE RECORD 命令

5.3.10.1 定义和范围

UPDATE RECORD命令用于更新记录文件中的数据。

在使用当前记录地址时，该命令将在修改记录成功后重新设定记录指针。

5.3.10.2 命令报文

UPDATE RECORD命令报文见表5.3-23。

表5.3-23 UPDATE RECORD命令报文

代码	值								
CLA	‘00’或‘04’								
INS	‘DC’								
P1	P1= ’00’ 表示当前记录 P1≠ ‘00’ 表示指定的记录号								
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 指定的记录号
	-	-	-	-	-	0	0	0	第一条记录
	-	-	-	-	-	0	0	1	最后一条记录
	-	-	-	-	-	0	1	0	下一条记录
	-	-	-	-	-	0	1	1	前一条记录
	任何其他值								保留
Lc	DATA 域数据长度								

表5.3-23 UPDATE RECORD命令报文（续）

Data	明文方式：　　明文记录数据 加密方式：　　密文记录数据 校验方式：　　明文记录数据||校验码 校验加密方式：密文记录数据||校验码
Le	不存在

5.3.10.3 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组成。

5.3.10.4 响应报文数据域

响应报文数据域不存在。

5.3.10.5 响应报文状态码

CPC卡回送的响应信息中的状态码见表5.3-24。

表5.3-24 UPDATE RECORD响应报文状态码

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

5.3.11 UPDATE KEY 命令

5.3.11.1 定义和范围

UPDATE KEY命令用于更新一个已经存在的密钥。（用于装载正式密钥）

本命令可支持8字节或16字节的密钥，密钥写入应采用密文+MAC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CPC卡取一个4字节的随机数。

5.3.11.2 命令报文

UPDATE KEY命令报文见表5.3-25。

表5.3-25 UPDATE KEY命令报文

代 码	值
CLA	‘84’
INS	‘D4’
P1	‘01’
P2	‘00’--更新主控密钥 ‘FF’--更新其他密钥
Lc	‘24’
Data	密文密钥信息||MAC
Le	不存在

5.3.11.3 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

——密钥标识

——版本

——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

5.3.11.4 响应报文数据域

响应报数据域不存在。

5.3.11.5 响应报文状态码

响应信息中的状态码见表5.3-26。

表5.3-26 UPDATE KEY响应报文状态码

SW1	SW2	说　明
‘90’	‘00’	命令执行成功
‘65’	‘81’	写 EEPROM 失败
‘67’	‘00’	Lc 长度错误
‘69’	‘82’	不满足安全状态
‘69’	‘83’	认证密钥锁定
‘69’	‘84’	引用数据无效（未申请随机数）
‘69’	‘85’	使用条件不满足
‘69’	‘88’	安全信息（MAC 和密文）数据错误
‘6A’	‘80’	数据域参数错误
‘6A’	‘81’	功能不支持
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到密钥数据
‘6A’	‘84’	文件空间已满
‘6A’	‘86’	P1、P2 参数错
‘6A’	‘88’	未找到密钥数据
‘6D’	‘00’	INS 错
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用永久锁定

5.4 安全

CPC 卡所有初始化数据应采用安全保护方式写入。

CPC 卡应支持 SM4 国产对称密码算法的数据存取和访问控制。

CPC 卡应提供安全访问模块或达到同等安全等级的芯片。

CPC 卡所使用安全访问模块或芯片的安全等级应达到 GM/T 0008《安全芯片密码检测准则》规定的 2 级或以上级别。

5.5 信息存储及应用更新

CPC卡内的数据信息存储宜采用数据块的方式，寻址应采用目录树和文件的方式。

CPC卡内应具有不小于3k字节作为应用信息存储空间。

CPC卡应支持应用更新，更新应采用13.56MHz通信方式，可选5.8GHz通信方式。

5.6 电池

CPC卡电池应通过UL 1642和UN 38.3认证。

5.7 外观规格

外观规格应符合：

1. 尺寸：长85.5±0.2mm，宽54±0.2mm，厚5±0.2mm。
2. 颜色：外观颜色为浅蓝色PT304U，色值为R:148，G:219，B:236。
3. 标识：卡片正面的卡号、背面的生产日期（年、月）及产品型号信息用激光雕刻，其他固定标识信息采用模具成型方式，下凹光面，其余表面为磨砂面，字体为黑体，字符间距为20%。“中国公路”及“使用须知”字高5mm，“车辆通行卡”字高7.8mm，其余文字高2.5mm，“使用须知”下两条水平线粗为1.5pt。文字位置见图5.7-1，单位mm，其中卡号编码规则见7.1.6要求。

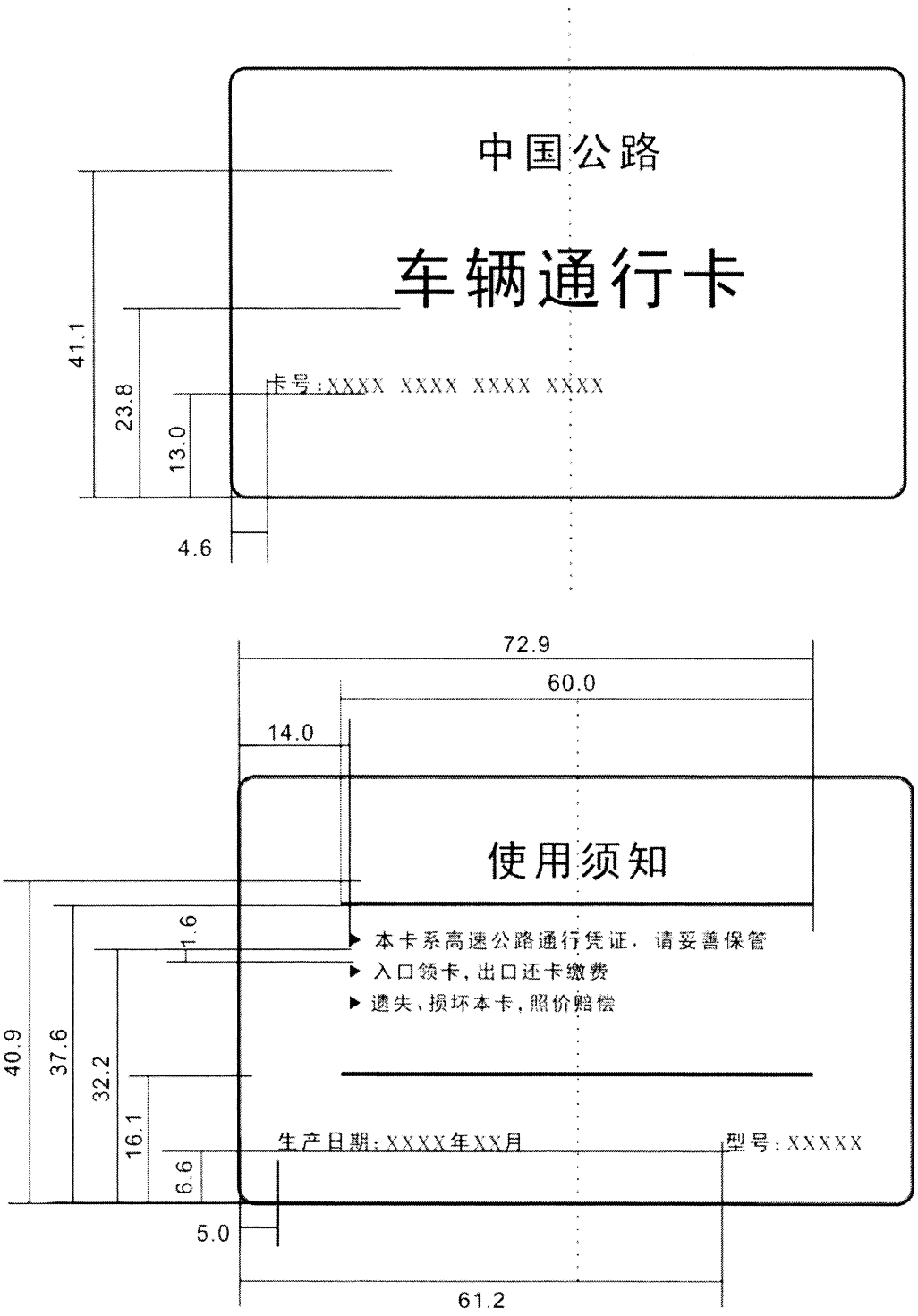
中国公路
车辆通行卡
卡号：XXXX XXXX XXXX XXXX
41.1
23.8
13.0
4.6
72.9
60.0
14.0
使用须知
本卡系高速公路通行凭证，请妥善保管
入口领卡，出口还卡缴费
遗失、损坏本卡，照价赔偿
1.6
40.9
37.6
32.2
16.1
6.6
生产日期：XXXX年XX月
型号：XXXXX
5.0
61.2

图 5.7 -1 外观规格

5.8 可靠性

MTBF：≥45,000小时。

5.9 环境条件

环境条件应符合：

1. 工作温度：-25℃～+75℃；
2. 存储温度：-40℃～+75℃；
3. 相对工作湿度：5%～100%；
4. 静电：≥8kV（空气放电）；
5. 振动：应符合GB/T 2423.10-2008《电工电子产品环境试验 第2 部分: 试验方法 试验Fc: 振动(正弦)》；
6. 冲击：应符合GB/T 2423.5《电工电子产品环境试验 第二部分: 试验方法试验Ea和导则:冲击》试验Eb和导则；
7. 外壳防护等级：IP65；
8. 防紫外线老化。

5.10 使用寿命

CPC的使用寿命：≥5年。

6 应用安全

6.1 外部认证流程

CPC 卡外部认证流程，如图 6.1-1 所示。

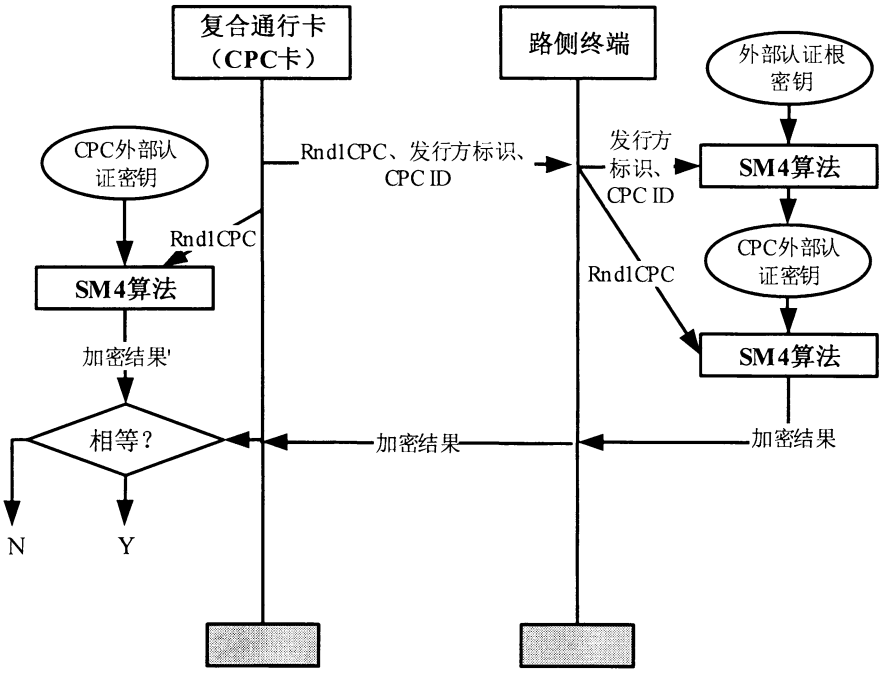

图 6.1-1 CPC 卡外部认证流程

6.2 内部认证流程

CPC 卡内部认证流程，如图 6.2-1 所示。

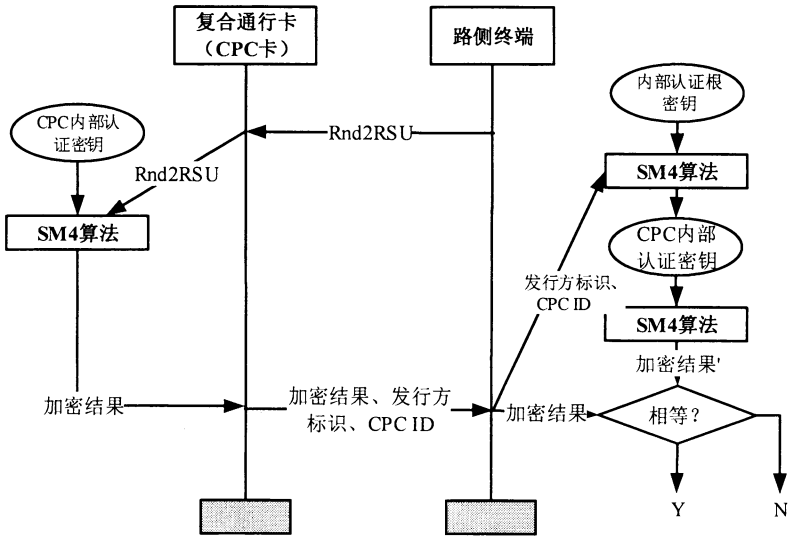

图 6.2-1 CPC 卡内部认证流程

7 关键信息编码及信息存储

7.1 关键信息编码

7.1.1 过站信息编码

过站信息由6个字节组成，包括3字节ETC门架编号及3字节本站计费金额，具体定义如图7.1-1所示。

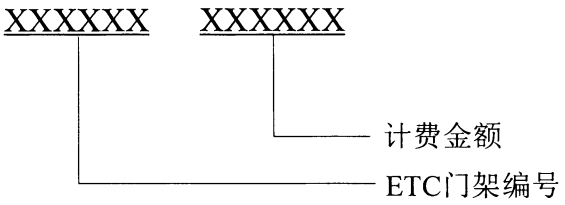

图7.1-1 过站信息编码规则

注：①ETC 门架编号规则见《高速公路 ETC 门架系统技术要求》；
②计费金额：单位为分，十六进制编码。

7.1.2 计费信息编码

计费信息由10个字节组成，包括3字节ETC门架编号、4字节通行时间及3字节计费金额，具体定义如图7.1-2所示。

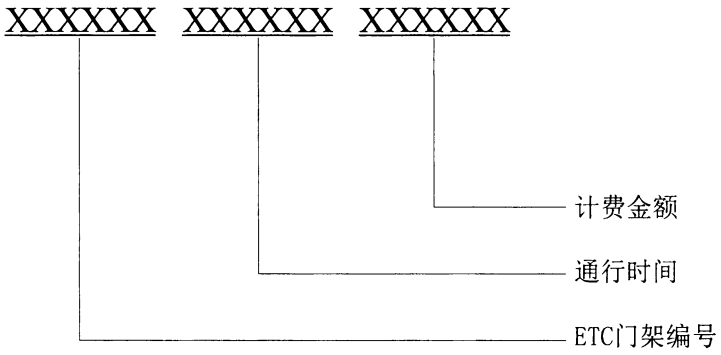

图7.1-2 计费信息编码规则

注：①ETC 门架编号规则见《高速公路 ETC 门架系统技术要求》；
②通行时间为 UNIX 时间，起始：1970 年 1 月 1 日 0 时 0 分 0 秒；
③计费金额：单位为分，十六进制编码。

7.1.3 CPC 卡发行方标识编码

“CPC卡发行方标识”是指CPC卡中“系统信息文件”（EF01）的第1～8字节，发行方标识由收费公路电子收费密钥管理单位统一分配并登记备案。CPC卡发行方标识编码规则见图7.1-3。

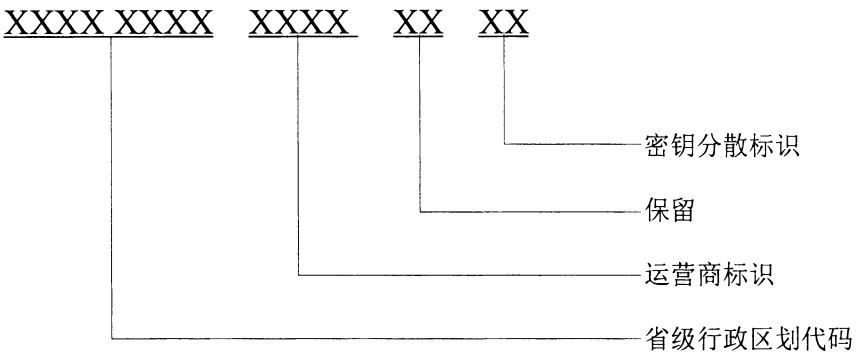

图7.1-3 CPC卡发行方标识编码规则

注：①省级行政区域代码为各省、直辖市、自治区的唯一标识，用 2 个汉字（4 个字节）表示；

②运营商标识为省内运营商的唯一标识，采用压缩 BCD 编码方式，由 2 个字节组成：第 1 字节为省级行政区划代码，依照标准 GB/T 2260；第 2 字节为运营商序号，由收费公路电子收费密钥管理单位分配并登记；

③保留字节暂定一个字节 0x00；

④密钥分散标识定义：目前取值为 01，通过两级分散得到卡片密钥，第一级采用区域代码（复制一次变为 8 个字节）作为分散因子，第二级采用 CPC 卡 ID 作为分散因子。

7.1.4 CPC 卡 MAC 地址编码

CPC卡的专用MAC地址采用4字节的十六进制数进行编码，由1个字节“卡片提供商标识”和3个字节“卡片提供商内部编码”组成，如图7.1-4所示。

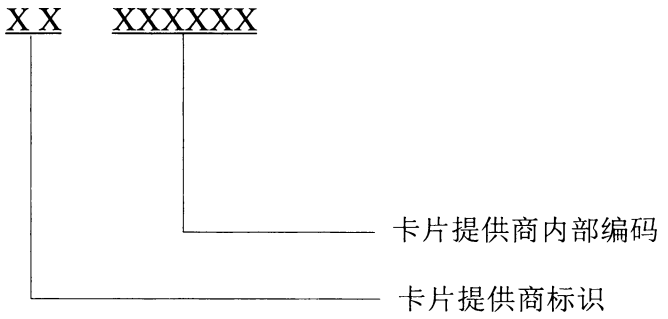

图7.1-4 CPC卡的专用MAC地址规则

注：①卡片提供商标识由收费公路电子收费密钥管理单位统一分配和管理。取值范围为：0x00～0xFF，其中：0x00～0x9E 分配给 OBU 厂商，0XA0～0xFE 分配给 CPC 卡厂商，0x9F、0xFF 保留做测试等用途。

②卡片提供商内部编码由 CPC 卡制造商根据其生产、管理等方面的需要自行定义，应确保其唯一性。其取值范围为：0x000000～0xFFFFFF。

7.1.5 CPC 卡 ID 编码

CPC卡ID编码是指系统信息文件（EF01）的第9～16字节。CPC卡ID由1字节“省级行政区域代码”、1字节“运营商序号”、2字节“卡片提供商标识”、4字节“卡片序列号”组成，见图7.1-5。

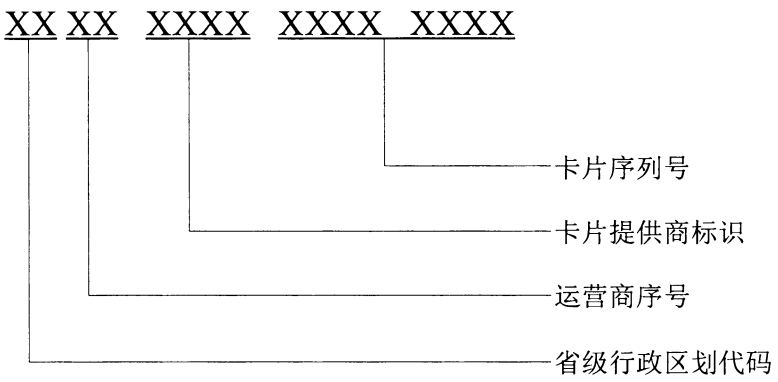

图7.1-5 CPC卡ID编码规则

注：①省级行政区划代码、运营商序号、卡片提供商标识、卡片序列号均采用压缩 BCD 编码方式。

②省级行政区划代码按照 GB/T 2260 执行，运营商序号由收费公路电子收费密钥管理单位分配并登记；卡片提供商标识由收费公路电子收费密钥管理单位统一管理。

③卡片序列号采用顺序编号的方式。

7.1.6 CPC 卡表面序号编码

CPC卡表面序号编码用于表面光刻打印。CPC卡表面序号编码与ID编码一致，如7.1-5所示。打印时，采用2字节为一组的方式，组与组之间用一个空格隔开。

7.1.7 CPC 卡分散代码

CPC卡应用采用两级密钥分散。第一级分散采用省级行政区域代码（复制一次变为8个字节）作为分散因子，第二级分散采用CPC卡ID（8个字节）作为分散因子。

7.2 信息存储

7.2.1 文件结构

CPC 卡的文件结构，如图 7.2-1 所示。

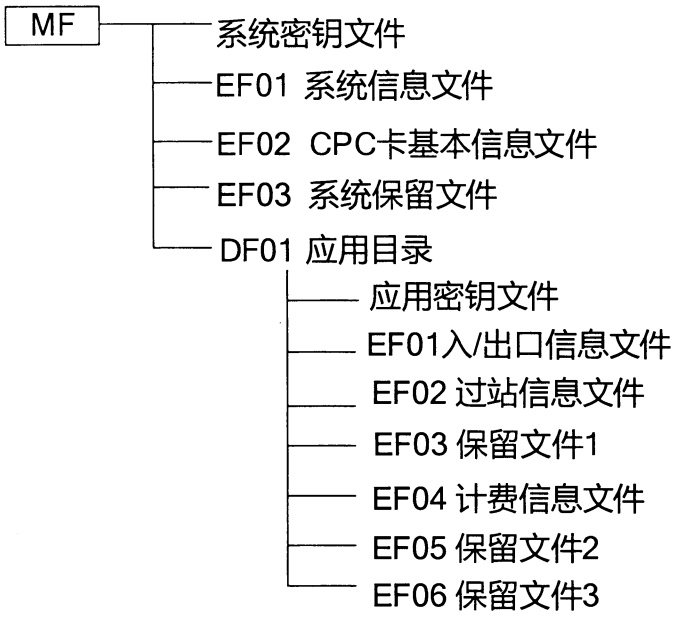

图 7.2-1 CPC 卡的文件结构图

7.2.2 数据文件说明

1. MF 根目录下的密钥文件

MF 下的密钥文件结构见表 7.2-1。

表7.2-1 MF下密钥文件结构

密钥名称	用途	标识	版本	长度	算法标识	错误计数器
卡片主控密钥 $MK_{\_MF}$	00	00	00	10H	04	15
卡片维护密钥 $DAMK_{\_MF}$	01	01	00	10H	04	15

密钥用途与用法：

a) 卡片主控密钥 $MK_{\_MF}$ 的用途是控制 MF 目录下文件的建立和密钥的写入；

b) 卡片维护密钥 $DAMK_{\_MF}$ 的用途是发卡方或应用提供方用于产生更新二进制

文件或记录命令的 MAC。

2. DF01 应用目录下的密钥文件

DF01 下的密钥文件结构见表 7.2-2。

表7.2-2 DF01下密钥文件结构

密钥名称	用途	标识	版本	长度	算法标识	错误计数器
应用主控密钥 MK_{DF01}	00	00	00	10H	04	15
应用维护子密钥 $DAMK_{DF01}$	01	01	00	10H	04	15
内部认证子密钥 1 $IK1_{DF01}$	02	01	00	10H	04	--
内部认证子密钥 2 $IK2_{DF01}$	02	02	00	10H	04	--
外部认证子密钥 1 $UK1_{DF01}$	00	01	00	10H	04	15
外部认证子密钥 2 $UK2_{DF01}$	00	02	00	10H	04	15
外部认证子密钥 3 $UK3_{DF01}$	00	03	00	10H	04	15
外部认证子密钥 4 $UK4_{DF01}$	00	04	00	10H	04	15

密钥用途与用法：

c) 应用主控密钥在卡片主控密钥的线路保护控制下装载（密文+MAC）；

d) 应用主控密钥在自身的控制下更新（密文+MAC）；

e) 本密钥文件下其它密钥在应用主控密钥的线路保护控制下装载、更新（密文+MAC）；

f) 应用主控密钥外部认证通过后，可以在 DF01 目录下进行文件创建（应用密钥文件、入/出口信息文件、过站信息文件、计费信息文件、保留文件等）；

g) 应用维护子密钥用于 DF01 区域的应用数据维护；

h) 内部认证子密钥 1 用于终端设备验证卡片的合法性，内部认证子密钥 2 作为备份密钥版本保留；

i) 外部认证子密钥 1 认证通过后可对 DF01 下的入/出口信息文件及过站信息文件、保留文件等进行更新，外部认证子密钥 2 认证通过后只可对 DF01 下的过站信息文件、保留文件等进行更新，不能对入/出口信息文件进行更新，

外部认证子密钥 3 和外部认证子密钥 4 分别作为外部认证密钥 1 和外部认证密钥 2 的备用版本用于未来密钥更新。

3. 系统信息文件

系统信息文件结构见表 7.2-3。

表7.2-3 系统信息文件结构

文件标识（FID）		‘EF01’
文件类型		二进制文件
文件大小		30 字节
读取：自由		写入：$DAMK_{_MF}$线路保护（明文 +MAC）
字节	长度（字节）	内容
1-8	8	CPC 卡发行方标识，编码见 7.1.3
9-16	8	CPC 卡 ID，编码见 7.1.5
17	1	版本号，当前版本号为 0x01
18-21	4	合同签署日期 格式：CCYYMMDD
22-25	4	合同过期日期 格式：CCYYMMDD
26-30	5	自定义，不使用时写入 0xFF

4. CPC 卡基本信息文件

CPC 卡基本信息文件结构见表 7.2-4。该文件内容由 CPC 卡内部操作系统自行维护，仅用于查询，外部写入无效[1]。

注 1：该文件主要用于由 CPC 卡 MCU 来控制改写自身状态，外部设备不应操作本文件，若被外部设备修改，将不能准确反应 CPC 卡的设备状态。

表7.2-4 CPC卡基本信息文件结构

文件标识（FID）		‘EF02’
文件类型		二进制文件
文件大小		64 字节
读取：自由		写入：自由
字节	长度（字节）	内容

1	1	CPC 电量信息，最高 bit 位：0 正常 1 低电；其他 7bit 位：剩余电量百分比
2	1	5.8GHz 工作状态，0：关闭；1：打开
3-64	62	厂商自定义

5. MF 下保留文件

MF 下保留文件结构见表 7.2-5。

表7.2-5 MF下保留文件结构

文件标识（FID）		‘EF03’
文件类型		二进制文件
文件大小		128 字节
读取：自由		写入：$DAMK_{MF}$ 线路保护（明文 +MAC）
字节	长度（字节）	内容
1-128	128	保留

6. DF01 下的入/出口信息文件

系统密钥文件结构见表 7.2-6。

表7.2-6 入/出口信息文件结构

文件标识（FID）		‘EF01’
文件类型		二进制文件
文件大小		128 字节
读取：自由		写入：$UK1_{DF01}$ 外部认证写入
字节	长度（字节）	内容
1	1	车型，编码方式应符合《电子收费 单片式车载单元（OBU）技术要求》表 5-5 车型定义
2-13	12	车牌号码，全牌照（汉字+字母+数字）信息，采用字符型存储，汉字采用 GB2312 码，如：“京”编码为“BEA9”； 牌照信息不足 12 字节，后补 0x00
14	1	车牌颜色，0x00–蓝色；0x01–黄色；0x02–黑色；0x03–白色；0x04-渐变绿色；0x05-黄绿双拼色；0x06-蓝白渐变；0x07～0xFF 保留
15 -16	2	入口收费路网号，见《收费公路联网收费技术要求》表 4.3
17-18	2	入口收费站号，见《收费公路联网收费技术要求》表 4.3

19	1	入口收费车道号，见《收费公路联网收费技术要求》表 4.3
20-23	4	入口时间，UNIX 时间，从格林威治标准时间 1970 年 1 月 1 日 0 时 0 分 0 秒起至现在的总秒数，不包括闰秒。
24	1	5.8GHz 模块工作状态控制字节，0x01：打开；0x02：关闭
25	1	出、入口状态，0x01：封闭式 MTC 入口；00x2：封闭式 MTC 出口；0x10：封闭式自助入口，其他详见《收费公路联网收费技术要求》表 4.3，采用十六进制编码

表7.2-6 入/出口信息文件结构（续）

字节	长度（字节）	内容
26	1	车种，十六进制编码，举例：绿通车-0x15。 0-普通车；6-公务车；8-军警车；10-紧急车；12-免费；14-车队；0～20 内其他：自定义应用；增加车种定义：21-绿通车 22-联合收割机 23-抢险救灾 24-集装箱 25-大件运输 26 -应急保障车 27-货车列车或半挂汽车列车；28～255 保留。
27-29	3	入口收费员工号
30	1	入口班次
31	1	货车轴数
32-35	4	货车总重，单位：kg。无总重信息时全部填 0xFF
36-38	3	核定载重，单位：kg。无核定载重信息时全部填 0xFF
39	1	特殊货车信息，默认值为 0xFF。
40-128	89	保留，不使用时写入 0xFF
注：入口车道不具有写入本文件定义字段的功能时，写入 0xFF。		

7. DF01 下的过站信息文件

过站信息文件结构见表 7.2-7。

表7.2-7 过站信息文件结构

文件标识（FID）	‘EF02’
文件类型	二进制文件
文件大小	512 字节
读取：自由	写入：$UK1_{\_DF01}$ 或 $UK2_{\_DF01}$ 外部认证写入

字节	长度（字节）	内容
1	1	已写入的有效过站信息总个数
2-4	3	已写入的最新 ETC 门架信息，3 字节 ETC 门架编码
5-508	504	过站信息，第 5 字节开始记录过站信息，每个过站信息由 3 字节 ETC 门架编号+3 字节计费金额组成
509-512	4	保留，不使用时写入 0xFF
注 1 .ETC 门架系统写过站信息时，应根据第 2-4 字节判断，避免重复写。 2.超出最大记录数，不再写入新的过站信息，仅“已写入的有效过站信息总个数”继续累加。		

8. DF01 下的保留文件 1

保留文件 1 结构见表 7.2-8。

表7.2-8 保留文件1结构

文件标识（FID）		‘EF03’
文件类型		二进制文件
文件大小		512 字节
读取：自由		写入：自由
字节	长度（字节）	内容
1-512	512	保留，写为 0xFF

9. DF01 下的计费信息文件

计费信息文件结构见表 7.2-9。

表7.2-9 计费信息文件结构

文件标识（FID）		‘EF04’
文件类型		二进制文件
文件大小		512 字节
读取：自由		写入：$UK1_{\_DF01}$ 或 $UK2_{\_DF01}$ 外部认证写入
字节	长度（字节）	内容
1-10	10	北京市辖区高速公路通行计费信息，计费信息由 3 字节 ETC 门架编号+4 字节通行时间+3 字节计费金额组成
11-20	10	天津市辖区高速公路通行计费信息

……		依次各省（区、市）计费信息存储[注]
341-512	171	保留字节，写入 0xFF

注：本文件应按以下顺序分配计费信息存储空间（省区市名称，代码）：
（1）北京市，第 1-10 字节；（2）天津市，第 11-20 字节；（3）河北省，第 21-30 字节；（4）山西省，第 31-40 字节；（5）内蒙古自治区，第 41-50 字节；（6）辽宁省，第 51-60 字节；（7）吉林省，第 61-70 字节；（8）黑龙江省，第 71-80 字节；（9）上海市，第 81-90 字节；（10）江苏省，第 91-100 字节；（11）浙江省，第 101-110 字节；（12）安徽省，第 111-120 字节；（13）福建省，第 121-130 字节；（14）江西省，第 131-140 字节；（15）山东省，第 141-150 字节；（16）河南省，第 151-160 字节；（17）湖北省，第 161-170 字节；（18）湖南省，第 171-180 字节；（19）广东省，第 181-190 字节；（20）广西壮族自治区，第 191-200 字节；（21）重庆市，第 201-210 字节；（22）四川省，第 211-220 字节；（23）贵州省，第 221-230 字节；（24）云南省，第 231-240 字节；（25）陕西省，第 241-250 字节；（26）宁夏回族自治区，第 251-260 字节；（27）甘肃省，第 261-270 字节；（28）青海省，第 271-280 字节；（29）新疆维吾尔自治区，第 281-290 字节；（30）海南省，第 291-300 字节；（31）西藏自治区，第 301-310 字节；（32）台湾省，第 311-320 字节；（33）香港特别行政区，第 321-330 字节；（34）澳门特别行政区，第 331-340 字节。

10. DF01 下的保留文件 2

保留文件 2 结构见表 7.2-10。

表7.2-10 保留文件2结构

文件标识（FID）		‘EF05’
文件类型		二进制文件
文件大小		512 字节
读取：自由		写入：$DAMK_{DF01}$ 线路保护（明文 +MAC）
字节	长度（字节）	内容
1-512	512	保留

11. DF01 下的保留文件 3

保留文件 3 结构见表 7.2-11。

表7.2-11 保留文件3结构

文件标识（FID）	‘EF06’
文件类型	二进制文件
文件大小	128 字节

读取：自由		写入：自由
字节	长度（字节）	内容
1-128	128	保留

附录 A　CPC 卡出/入口车道交互流程

A.1 CPC 卡封闭式入口交互流程

CPC 卡封闭式入口交互流程见表 A-1。

表A-1封闭式入口交互流程

CPC 卡		13.56MHz 读写器		PSAM 卡/PCI 密码卡
卡片复位	←	复位 CPC 卡		
	←	读 CPC 基本信息文件 EF02		
返回 EF02 文件	→	获得 EF02 文件内容，系统解析卡片电量等信息并做出判断		
	←	读系统信息文件 EF01		
返回 EF01 文件	→	获得 EF01 文件内容		
		将省级行政区域代码、卡号发给 PSAM 分散密钥	→	Delivery Key
		确认分散密钥成功	←	分散密钥成功
	←	选择 DF01 应用		
进入 DF01 应用	→			
	←	取 8 字节随机数 Rnd1		
返回随机数 Rnd1	→	将 Rnd1 后面补充 8 字节 00 后组成 16 字节输入数据，发给 PSAM 加密	→	Cipher Data
	←	$UK1_{\_DF01}$ 外部认证	←	返回加密结果
返回外部认证结果	→	确认外部认证成功		
内部认证指令	←	产生 8 字节随机数 Rnd2，Rnd2 后面补充 8 字节 00 后组成 16 字节作为内部认证指令的输入数据		
返回加密结果 2	→	接收加密结果 2		
		将卡号发给 PSAM 分散密钥	→	Delivery Key
		确认分散密钥成功	←	分散密钥成功
		将随机数 2 发给 PSAM 加密	→	Cipher Data
		对比加密结果 2 与加密结果 2’，若一致则内部认证成功	←	返回加密结果 2’
	←	写入口信息文件 EF01		
返回写入口信息结果	→	确认成功写入		
	←	清除过站信息文件 EF02 文件内容和计费信息 EF04 文件内容		
更新 EF02 和 EF04 文	→	确认清除成功		

件				
卡片复位	←	复位 CPC 卡		

A.2 CPC 卡封闭式出口交互流程

CPC 卡封闭式出口交互流程见表 A-2。

表A-2 封闭式出口交互流程

CPC 卡		13.56MHz 读写器		PSAM 卡/PCI 密码卡
卡片复位	←	复位 CPC 卡		
	←	读系统信息文件 EF01		
返回 EF01 文件	→	获得 EF01 文件内容		
		将省级行政区域代码、卡号发给 PSAM 分散密钥	→	Delivery Key
		确认分散密钥成功	←	分散密钥成功
	←	选择 DF01 应用		
进入 DF01 应用	→			
	←	取 8 字节随机数 Rnd1		
返回随机数 Rnd1	→	将 Rnd1 后面补充 8 字节 00 后组成 16 字节输入数据，发给 PSAM 加密	→	Cipher Data
	←	$UK1_{\_DF01}$ 外部认证	←	返回加密结果 1
返回外部认证结果	→	确认外部认证成功		
内部认证指令	←	产生 8 字节随机数 Rnd2，Rnd2 后面补充 8 字节 00 后组成 16 字节作为内部认证指令的输入数据		
返回加密结果 2	→	接收加密结果 2		
		将卡号发给 PSAM 分散密钥	→	Delivery Key
		确认分散密钥成功	←	分散密钥成功
		将随机数 2 发给 PSAM 加密	→	Cipher Data
		对比加密结果 2 与加密结果 2’，若一致则内部认证成功	←	返回加密结果 2’
	←	读入/出口信息文件 EF01		
返回 EF01 文件	→	获得 EF01 文件内容		
	←	更新入/出口信息文件 EF01 第 24 字节为出口状态		
返回写出口信息结果	→	确认成功写入		
	←	读过站信息文件 EF02 和计费信息文件 EF04		
返回 EF02 文件内容	→	获得 EF02、EF04 文件内容		
	←	按规则缴费后，清除 EF02、EF04		

		文件内容		
更新 EF02、EF04 文件	→	确认清除成功		
卡片复位	←	复位 CPC 卡		

附录 B CPC 卡发行流程

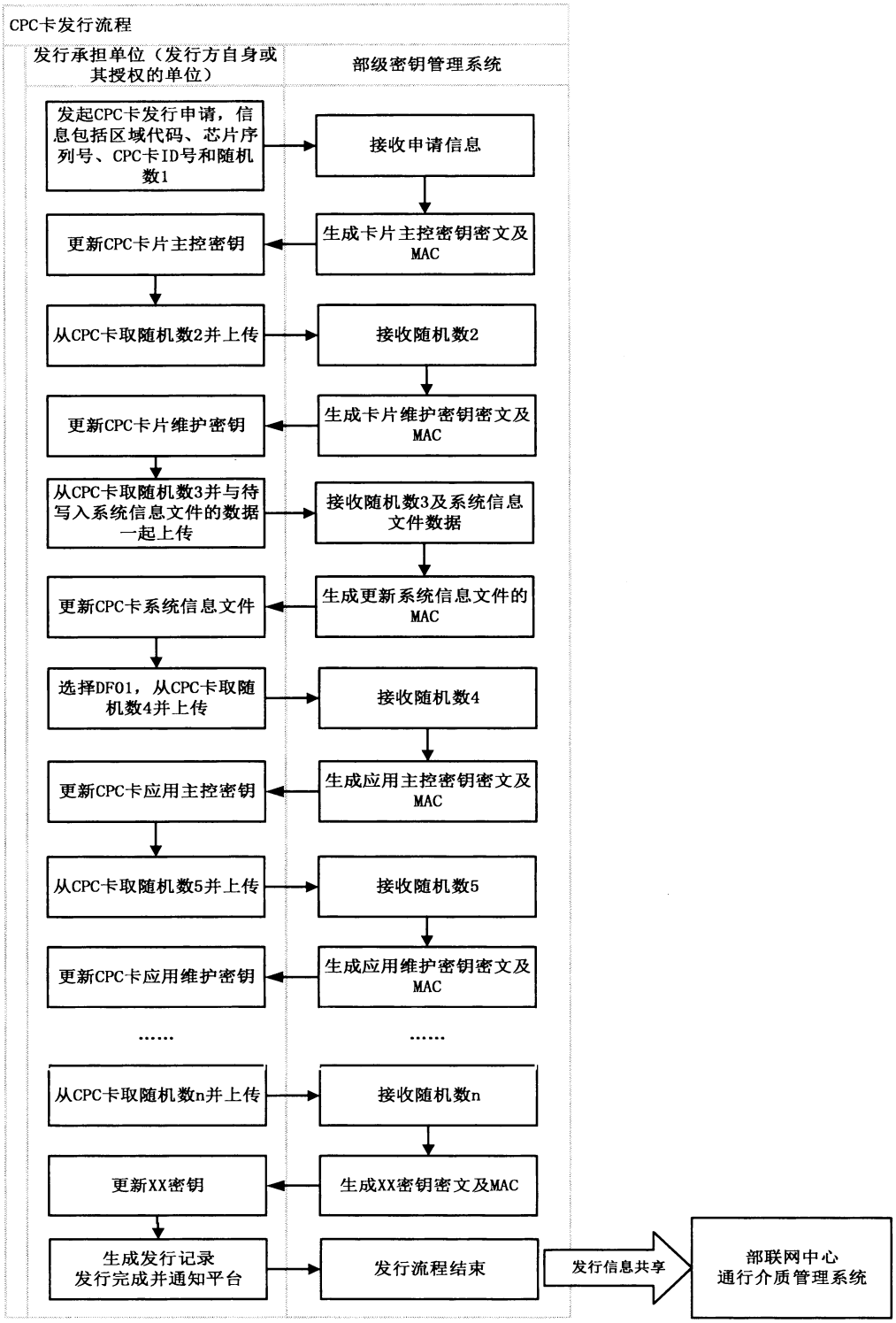

图 B-1 CPC 卡发行流程

分送：各省、自治区、直辖市、新疆生产建设兵团交通运输厅(局、委)。

交通运输部办公厅　　2019年6月13日印发