ICS 35.240.99
L 67

中华人民共和国国家标准

GB/TXXXXX.1—XXXX

教育卡应用规范
第1部分：教育IC卡技术规范

Application specification for IC education card

Part 1: Technical specification for IC education card

（报批稿）

XXXX-XX-XX 发布　　XXXX-XX-　实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

GB/T XXXX-XXXX《教育卡应用规范》预计分为11个部分：

——第1部分：教育IC卡技术规范；

——第2部分：教育卡发卡发证流程规范；

——第3部分：教育卡数据处理规范；

——第4部分：教育卡个人化写卡写证制作系统建设规范；

——第5部分：教育卡安全保障技术规范；

——第6部分：教育卡应用安全模块技术开发规范；

——第7部分：教育卡应用与开发规范；

——第8部分：教育卡网络副本技术规范；

——第9部分：教育电子证件技术规范；

——第10部分：教育电子证件制作系统建设规范；

——第11部分：教育电子证件验证终端技术要求。

本部分为GB/T XXXX-XXXX的第1部分。

本部分按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由全国信息技术标准化技术委员会（SAC/TC28）提出并归口。

本部分起草单位:教育部教育管理信息中心、中国电子技术标准化研究院、中育至诚科技有限公司、中国银联股份有限公司、网络空间身份认证与数据安全湖南省工程实验室、公安部第一研究所、南方城墙信息安全科技有限公司、上海复旦微电子集团股份有限公司、直通云数据安全技术有限公司、长城信息产业股份有限公司、东方新诚信数字认证中心有限公司、广东楚天龙智能卡有限公司、华南理工大学、长沙理工大学。

本部分主要起草人：罗方述、蔡燕、马亮、颜星、张鹏、余云涛、王刚、丁林润、钟梁、杨清贵、程聂、李莹、欧阳晖、李春欢、陈朋、陈安新、张纲、倪以金、齐德昱、罗晓奔、傅明、李峰、蒋才平、谭武征、罗继东、王瑾、邵飞。

引　言

本部分凡涉及商用密码算法相关内容，按国家有关法规以及国家商用密码主管部门颁布的密码算法相关标准规范实施。

本部分凡涉及支付、金融IC卡等的相关内容，按中国人民银行颁布的支付相关标准规范、金融集成电路（IC）卡相关标准规范实施。

本部分凡涉及法定身份证件相关内容，按国家有关法规以及法定身份证件主管部门颁布的相关标准规范实施。

教育卡应用规范 第1部分：教育IC卡技术规范

1 范围

本部分规定了教育卡应用相关的文件系统、命令、应用流程、卡表面信息、应用接口，以及教育卡应用安全体系的技术要求。

本部分适用于教育卡的设计、制造、检测、发行、应用和管理。

2 规范性引用文件

下列文件对于本部分的应用是必不可少的。凡是注明日期的引用文件，仅注明日期的版本可适用于本文件。凡是不注明日期的引用文件，其最新版本（包括所有的修改版本）适用于本文件。

GB/T 14916-2006 识别卡 物理特性

GB/T 16649.4-2010 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 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

GB 18030-2005 信息技术 中文编码字符集

GB/T 2260-2007 中华人民共和国行政区划代码

GB/T 4880.1-2005 语种名称代码 第1部分：字母代码

GM/T 0002-2012 SM4分组密码算法

GM/T 0003-2012 SM2椭圆曲线公钥密码算法

GM/T 0004-2012 SM3密码杂凑算法

GM/T 0009-2012 SM2算法使用规范

JY/T 1001-2012 教育管理信息 教育管理基础代码

JY/T 1002-2012 教育管理信息 教育管理基础信息

JY/T 1003-2012 教育管理信息 教育行政管理信息

JR/T 0025-2013 中国金融集成电路（IC）卡规范

3 术语与定义

下列术语与定义适用于本文件。

3.1

教育卡 education card

面向在校学生、毕业生、教职员工、以及教育管理部门的管理人员等对象发放，满足教育领域安全性要求、具备身份鉴别功能、具有可识别的全国唯一的教育电子身份号，可支持教育管理应用、学校应用、网络空间应用、以及社会化应用的无触点集成电路（IC）卡。教育卡分为实体卡和网络副本两种类型。

基于教育卡的应用功能进行分类，教育卡分为学生卡、教师卡、毕业生卡、教育电子证件、电子校徽等类型。

3.2

教育电子身份号 education security number

教育卡持卡人的唯一电子身份鉴别标识，用于持卡人及其相关教育可信信息在网络空间环境的识别。

3.3

学生卡 education card for students

面向在校学生发行的教育卡。

3.4

教师卡 education card for teachers

面向学校的教职员工、教育管理部门的管理人员发行的教育卡。

3.5

毕业生卡 education card for graduate students

面向毕业生发行的教育卡。

3.6

教育电子证件 education electronic diploma

教育电子证件是在教育行业的纸质本式证件的封底嵌入封装无触点集成电路芯片，并将持证人的基本身份信息、证件信息等数据安全写入芯片内的证件。教育电子证件分为电子毕业/电子结业证、电子学位证等类型。

3.7

电子校徽 electronic school badge

在徽章介质中嵌入无触点集成电路芯片的校徽。校徽内的无触点集成电路芯片与学生卡内的无触点集成电路芯片技术性能相同。

3.8

教育卡网络副本 education card online copy

采用公开密钥技术，与教育卡数据同时生成的一种特殊数据，与教育卡唯一绑定。在网络环境下使用教育卡网络副本，具有与实体教育卡相同的身份鉴权等功能。

3.9

居民身份证网上副本 identity card online copy

由居民身份证主管部门根据居民身份证生成的一种特殊数据，用于居民身份证持证人在网络环境下的法定身份验证。

3.10

报文 message

由终端向教育卡或教育卡向终端发出的，不含传输控制字符的字节串。

3.11

报文鉴别代码 message authentication code

对报文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。

3.12

路径 path

没有分隔的文件标识符的连接。

3.13

命令 command

终端向教育卡发出的一条报文。该报文启动一个操作或请求一个响应。

3.14

数字证书 digital certificate

关于实体的一种数据。该数据由第三方电子认证服务机构签发，并无法伪造。

3.15

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人伪造或抵赖。

3.16

数据完整性 data integrity

数据没有遭受以非授权方式所作的篡改或破坏的性质。

3.17

SM2 算法 SM2 algorithm

一种椭圆曲线密码算法，密钥长度为256位。

3.18

SM3 算法 SM3 algorithm

一种杂凑算法，输出长度为256位。

3.19

SM4 算法 SM4 algorithm

一种分组密码算法，分组长度为128位，密钥长度为128位。

3.20

终端 terminal

用于完成教育卡的读写操作的设备。

3.21

教育卡发行单位 education card issuing unit

承担教育卡发行与管理工作的县（区）教育管理机构、中等职业学校与高等院校。

3.22

教育卡应用单位 education card application unit
使用教育卡对持卡人进行管理或服务的单位（例如，学校等）。

4 缩略语

下列缩略语适用于本文件。
AC：应用密文（Application Cryptogram）
ADF：应用数据文件（Application Dedicated File）
AEF：应用基本文件（Application Elementary File）
AID：应用标识符（Application Identifier）
ARPC：授权响应密文（Authorization Response Cryptogram）
CLA：命令报文的类别字节（Class Byte of The Command Message）
COS：嵌入式芯片操作系统（Chip Opration System）
DEA：数据加密算法（Data Encryption Algorithm）
DF：专用文件（Dedicated File）
ESN：教育电子身份号（Education Security Number）
EF：基本文件（Elementary File）
FCI：文件控制信息（File Control Information）
FID：文件标识符（File Identifier）
INS：命令报文的指令字节（Instruction Byte of Command Message）
MAC：报文鉴别代码（Message Authentication Code）
PIN：个人识别码（Personal Identification Number）
PKI：公钥密码基础设施（Public Key Infranstructure）
SFI：短文件标识符（Short File Identifier）
SW：状态字（Status Word）

5 教育卡文件系统

5.1 文件总则

5.1.1 文件结构

教育卡的教育应用的文件结构应符合GB/T 16649.4-2010规定。
各个应用所对应的DF与EF，构成教育应用的文件结构的各个分支。

5.1.2 专用文件

通过FCI对DF下的EF进行访问。

5.1.3 基本文件

EF的文件类型如下：
a) 变长记录文件；
b) 循环记录文件；

c) 二进制文件；
d) 扩展记录文件。

5.1.4 文件选择

教育应用的文件选择方式如下：

a) DF 可用 AID 进行选择。成功选择了 DF 后，该 DF 被设置成当前 DF，允许使用相关命令对其进行操作；
b) EF 可使用 READ 或 UPDATE 命令通过 SFI 来选择。

5.2 文件引用

教育应用的各个DF，可用FID或者AID进行引用。

5.3 文件结构

教育应用的文件结构如表1所示，文件定义描述见附录A，卡片数据元格式见附录B。

表1 教育应用的文件结构

序号	应用	文件名称	文件信息	备注
1	公共应用（ADF00）	教育卡发行信息文件(EF01)	厂商代码、发卡方专用代码等信息	由发卡方写入。
		持卡人基本身份信息文件(EF02)	持卡人姓名、籍贯、教育电子身份号等信息	
		照片信息文件(EF03)	持卡人的照片信息	
		生物特征识别信息文件(EF04)	持卡人的生物特征识别信息	
2	法定身份证件网上应用（ADF01）	居民身份证网上副本文件（EF01）	持卡人的居民身份证网上副本信息	由发卡方写入。
3	学校应用（ADF02）	工作信息文件(EF01)	持卡人工作情况的基本信息	仅用于教师卡。
		学籍信息文件(EF02)	持卡人的基本学籍信息	仅用于学生卡。
		学籍注册文件(EF03)	学生的注册信息，每学期一条记录	仅用于学生卡。
		体质健康信息文件(EF04)	持卡人身体健康状况信息	仅用于学生卡。
		学生助学贷款信息文件(EF05)	持卡人所申请助学贷款的信息	仅用于学生卡。
		营养餐资格信息文件(EF06)	持卡人营养餐资格信息	仅用于学生卡。
		营养餐领餐信息文件(EF07)	持卡人领用营养餐的信息	仅用于学生卡。

表1 （续）

序号	应用	文件名称	文件信息	描述
4	机构应用（ADF03）	毕业/结业证书文件(EF01)	持卡人的毕业/结业证书信息	
		学位证书文件(EF02)	持卡人的学位证书信息	
		资格水平信息文件(EF03)	持卡人所获得国家认可的专业资格、岗位证书信息	
		考务基本信息文件(EF04)	准考证信息	仅用于学生卡。
		学生首次就业信息文件(EF05)	学生报到证编号、首次就业日期、就业单位名称等信息	仅用于毕业生卡。
		教育经历信息文件(EF06)	持卡人的教育相关经历信息	
5	PKI 应用（ADF04）	教育卡发卡中心证书（EF01）	签发持卡人的签名证书和加密证书的证书	
		签名密钥文件(EF02)	签名私钥信息	
		加密密钥文件(EF03)	加密私钥信息	
		人员签名证书文件(EF04)	签名证书	
		人员加密证书文件(EF05)	加密证书	
		发卡方预留信息文件（EF06）	发卡方自定义	
		签名公钥文件（EF07）	签名公钥信息	
		加密公钥文件（EF08）	加密公钥信息	
		证书管理文件（EF09）	签名证书和加密证书的管理信息	
6	教育管理应用(ADF05)	国家教育管理应用保留文件 1～9（EF01～EF09）	存储国家教育管理信息应用相关信息	保留，文件结构由国家教育主管部门定义。
7	行业扩展应用(ADF06)	交通票务优惠信息文件(EF01)	学生搭乘交通工具的控制信息	由其他行业应用写入的信息。
		交通票务使用信息文件(EF02)	学生搭乘交通工具的日期、交通工具类型以及总使用次数等信息	
		行业应用文件 3～9（EF03～EF09）	存储其他行业应用相关信息	

表1 （续）

序号	应用	文件名称	文件信息	描述
8	教育电子证件应用（ADF08）	电子毕业/结业证信息文件（EF01）	电子毕业/结业证的格式化信息	
		电子学位证信息文件（EF02）	电子学位证的格式化信息	
		电子毕业/结业证版式文件（EF03）	电子毕业/结业证的版式文件信息	
		电子学位证版式文件（EF04）	电子学位证的版式文件信息	
9	芯片管理应用(ADF09)	芯片验证身份认证码密钥文件(EF01)	芯片验证身份认证码的签名私钥	
		芯片验证身份认证码证书文件(EF02)	芯片验证身份认证码的签名证书	
10	省级教育管理应用（ADF10）	省级应用文件 1～9（EF01～EF09）	存储省级教育管理应用的信息	文件结构由省级教育管理部门定义。
11	市级教育管理应用（ADF11）	市级应用文件 1～9（EF01～EF09）	存储市级教育信息化应用的信息	文件结构由市级教育管理部门定义。
12	卡发行单位应用（ADF12）	卡发行单位应用文件1～9（EF01～EF09）	存储卡发行单位教育信息化应用的信息	文件结构由卡发行单位定义。
13	卡应用单位应用（ADF13）	卡应用单位应用文件1～9（EF01～EF09）	存储卡应用单位教育信息化应用的信息	文件结构由卡应用单位定义。

6 教育卡命令

6.1 命令总则

教育卡命令、命令响应的格式与内容符合GB/T 16649.4-2010的规定，命令规范见附录C。

教育卡命令分为通用命令与专有命令两类。

a) 通用命令：主要包括以下命令：
   1) 选择（SELECT）；
   2) 身份鉴别（PERSONAL AUTHENTICATE）；
   3) 卡片鉴别（CARD AUTHENTICATE）；
   4) 取随机数（GET CHALLENGE）；
   5) 交易认证（TRANS AUTHENTICATE）；
   6) 添加记录（APPEND RECORD）；
   7) 更新记录（UPDATE RECORD）；
   8) 读记录（READ RECORD）；
   9) 读二进制信息（READ BINARY）；
   10) 更新二进制信息（UPDATE BINARY）；
   11) PIN码校验（VERIFY PIN）；
   12) PIN码修改（CHANGE PIN）；

13) PIN 码解锁（PIN UNBLOCK）；
14) 应用锁定（APPLICATION BLOCK）；
15) 应用解锁（APPLICATION UNBLOCK）；
16) 取应用交易计数器（GET ATC）；
17) 联机圈存（CREDIT FOR ONLINE LOAD）；
18) 联机消费（DEBIT FOR ONLINE PURCHASE）
19) 取数据（GET DATA）；
20) 外部认证（EXTERNAL AUTHENTICATE）；
21) 导出会话密钥（EXPORT SESSION KEY）；
22) 导入会话密钥（IMPORT SESSION KEY）；
23) 对称加密/解密（ENCRYPT/DECRYPT）；
24) SM2 密钥对生成（GENERATE SM2 KEY PAIR）；
25) SM2 公钥导出（EXPORT PUBLIC KEY）；
26) SM2 密钥导入（IMPORT SM2 KEY）；
27) SM2 公钥运算（SM2 PUBLIC KEY CAL）；
28) SM2 私钥运算（SM2 PRIAVTE KEY CAL）；
29) 数据压缩（DATA HASH）；
30) 证书验证（VERIFY CERT DATA）。

b) 专有命令：主要包括以下命令：
1) 写教育电子证件（WRITE DIPLOMA）；
2) 读教育电子证件（READ DIPLOMA）；
3) 禁止修改教育电子证件（DISABLE DIPLOMA MODIFIED）；
4) 读教育卡认证码（READ AUTHCODE）。

6.2 命令报文格式

命令报文由命令头和可变长的命令体组成。命令报文格式如图1所示。命令报文的内容见表2。

CLA	INS	P1	P2	Lc	Data	Le
←命令头→				←命令体→		

图1 命令格式

表2 命令报文内容

代码	长度（字节）	描述
CLA	1	命令类别
INS	1	指令字节
P1	1	指令参数 1
P2	1	指令参数 2
Lc	0 或 1	数据域中存在的字节数
Data	可变	命令发送的数据位串（长度=Lc）
Le	0 或 1	响应数据域中期望的最大数据字节数。当 Le 值为 0 时，表示需要最大字节数（256 字节）。

6.3 命令响应报文格式

命令响应由一个变长的响应数据体和两字节的响应尾组成。命令响应报文格式如图2所示。

Data	SW1	SW2
响应数据体	←响应尾→	

图2 命令响应报文格式

命令响应报文的内容见表3。

表3 命令响应报文内容

代码	长度（字节）	描述
Data	变长	响应报文的数据位串
SW1	1	状态字1
SW2	1	状态字2

7 教育卡应用流程

7.1 应用流程概述

教育卡应用流程主要包括：应用预处理、身份鉴别、卡片鉴别、信息读取、信息更改、学籍注册、营养改善计划用餐登记、学位证书写入、毕业/结业证书写入、学位证书读取、毕业/结业证书读取、交通优惠信息写入、ESN读取、交易认证、联机圈存、联机消费、教育卡认证码读取，以及相关的应用维护、防拨等。

7.2 应用预处理

7.2.1 卡片数据

应用预处理使用的卡片数据元和描述见表4。卡片数据元格式见附录B。

表4 应用选择——卡片数据

数据元	描述
AID	由注册应用提供商标识和扩展的专用应用标识扩展码组成。它标识了在GB/T 16649.5-2002中描述的应用。
ADF	AEF的入口文件，AEF包含以下应用数据元： a)FCI 模板： b)DF 名称 c)FCI 专有模板（可选） d)应用标签（可选） e)算法指示位（可选） f)首选文种（可选） g)发卡方代码表索引（可选。若应用首选名称存在） h)应用优先名称（可选） i)FCI发卡方自定义数据（可选）

表4 （续）

数据元	描述
AEF	应用基本文件，包括应用处理过程中使用的数据元（可选）。
应用标签（50）	用于应用选择。存在于ADF（可选）。
算法指示位（3FB1）	用于指示当前被选择应用所使用的算法（可选）。
FCI	SELECT命令的响应信息，选择不同类型的文件，响应信息不同。
发卡方代码表索引	指明在终端显示应用首选名称时使用的代码表（可选）。
注：注册应用提供商标识，由国家IC卡注册中心赋予。	

7.2.2 终端数据

应用预处理使用的终端数据见表5。

表5 应用选择——终端数据

数据元	描述
AID	AID 由注册应用提供商标识和扩展的专用应用标识扩展码组成。它标识了在GB/T 16649.5-2002中描述的应用。
应用选择指示器	表明终端是否支持部分AID选择。
终端支持的应用列表	终端维护的一个表，包括支持的应用和它们各自的AID。

7.2.3 相关命令

7.2.3.1 选择命令

终端发送SELECT命令给卡片，获取卡片FCI。命令中包括所选择ADF的AID。
SELECT命令的定义和描述见附录C。

7.2.3.2 确定和选择应用

终端使用AID列表选择方式，建立卡片和终端均支持的应用列表。
教育卡的AID列表选择方式如下：
步骤1：卡片收到SELECT命令，检查卡片中是否有匹配的AID应用。
步骤2：若匹配的卡片AID长度比终端AID长，卡片在SELECT命令响应报文中返回完整的AID给终端。

7.2.4 处理流程

应用预处理是教育卡所有应用流程所共有的预处理过程，其流程如图3所示。

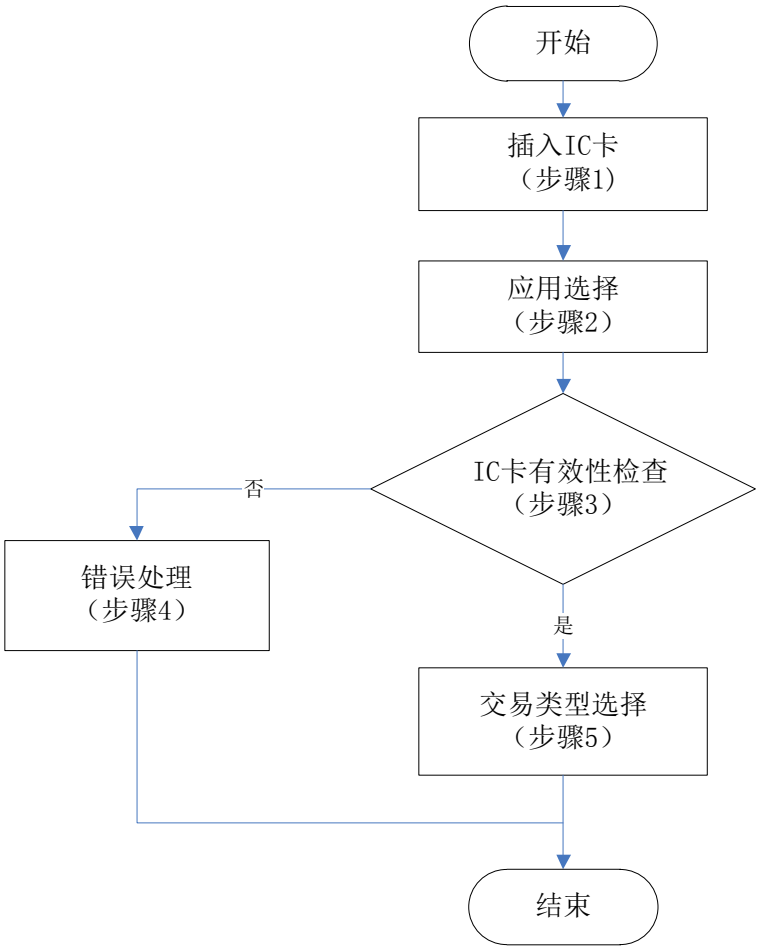


图3　应用预处理流程

处理过程如下：

a) 插入教育卡（步骤 1）：终端应具有检测教育卡是否已经插入的功能。若教育卡已经插入，终端将执行以下处理。

b) 应用选择（步骤 2）：应用选择处理决定了选择一个卡片和终端均支持的应用来完成后续处理。这一处理分为两个步骤：

   1) 终端建立终端和卡片均支持的应用列表；

   2) 从列表中确定一个应用进行处理。

c) 教育卡有效性检查（步骤 3）：终端对 SELECT 命令以及 READ BINARY 命令回送的数据进行以下检查：

   1) 卡片是否在终端存储的黑名单列表中（使用发卡方标识和应用序列号）；

   2) 终端是否支持该卡片的发卡方标识符；

   3) 终端是否支持该卡片上的应用（使用应用类型标识）；

   4) 终端是否支持标签为 3FB2 的应用版本号所代表的应用版本；

   5) 应用是否在有效期内；

   6) 教育卡认证码和教育卡芯片身份认证是否合法。

   若以上任一条件不满足时，转入步骤5。

d) 应用类型选择（步骤 4）：终端应具有让持卡人选择应用的功能，每次只能选择一种应用；

e) 错误处理（步骤 5）：终端根据返回的信息，进行相应的错误处理。

7.3 身份鉴别

7.3.1 卡片数据

身份鉴别使用的数据元见表6。

表6 身份鉴别——使用的数据元

数据元	描述
发卡方公钥索引	由发卡方提供。指明了用于验证人员签名证书的发卡方公钥。
人员签名证书	包含人员签名公钥，在卡片个人化时写入卡中。
参数 1	保留参数，用于身份鉴别算法的扩展。
签名的动态应用数据	卡片生成的动态应用数据及签名。

在身份鉴别处理中，卡片内部使用的数据元见表7。

表7 身份鉴别——卡片内部使用的数据元

数据元	描述
卡片随机数	由卡片内部产生。
签名私钥	用于对动态应用数据进行签名。
脱机 PIN	用于验证 PIN 码的正确性。

7.3.2 终端数据

身份鉴别使用的终端数据见表8。

表8 身份鉴别——使用的终端数据

数据元	描述
终端随机数	由终端生成。
PIN 码	由持卡人输入的 PIN 码，用于 PIN 码校验。

7.3.3 相关命令

7.3.3.1 PIN 码校验命令

在身份鉴别处理过程中，终端使用VERIFY PIN命令校验PIN码的正确性，以获得使用签名私钥的权限。

VERIFY PIN命令的定义和描述见附录C。

7.3.3.2 身份鉴别命令

终端使用PERSONAL AUTHENTICATE命令请求进行身份鉴别。

当卡片接收到PERSONAL AUTHENTICATE命令之后，使用教育卡内存储的签名私钥生成签名的动态应用数据。在PERSONAL AUTHENTICATE命令响应报文中包含该数据。

发送PERSONAL AUTHENTICATE命令前，需要发送READ BINARY命令与READ RECORD命令，从卡片中读出处理身份鉴别的签名证书及其他相关数据。

PERSONAL AUTHENTICATE命令的定义和描述见附录C。

7.3.4 处理流程

身份鉴别是指通过读取持卡人身份鉴别相关数据，采用动态数据认证的方式，验证持卡人身份的过程。身份鉴别处理流程如图4所示。

a) 输入 PIN 码（步骤 1）：持卡人输入 PIN 码。
b) 校验 PIN 码（步骤 2）：终端使用 VERIFY PIN 命令校验持卡人输入的 PIN 码是否正确。教育卡收到 VERIFY PIN 命令后，进行以下处理：
   1) 检查 PIN 尝试计数器。若 PIN 尝试计数器为零，教育卡回送状态字“6983”，转入步骤 3；
   2) 检查命令数据中的 PIN 码和教育卡中存放的 PIN 码是否相同。若两个 PIN 码不同，教育卡将 PIN 尝试计数器减 1，并回送状态字“63Cx”，“x”是 PIN 尝试计数器的新值，并转入步骤 3；
   3) 若两个 PIN 码相同，教育卡将 PIN 尝试计数器置为允许 PIN 重试的最大次数，并回送状态字“9000”，转入步骤 4（教育卡应记住 PIN 码校验成功的结果，直到断电、卡片复位、PIN 再次校验错误或选择了其他应用）。
c) 回送错误状态（步骤 3）：若不接受身份鉴别处理，应通知终端。
d) 发出/处理读 READ RECORD 命令或 Read Binary 命令（步骤 4、步骤 5）：终端使用 READ RECORD 命令或 Read Binary 命令从教育卡读取身份鉴别的相关数据，并保存数据用于身份鉴别。
e) 发出 PERSONAL AUTHENTICATE 命令(步骤 6)：终端生成终端随机数，发出 PERSONAL AUTHENTICATE 命令。
f) 处理 PERSONAL AUTHENTICATE 命令（步骤 7）：教育卡收到 PERSONAL AUTHENTICATE 命令后，进行以下处理：
   1) 检查 PERSONAL AUTHENTICATE 命令是否包含终端随机数。若未包含终端随机数，则回送状态字“6985”；
   2) 生成签名数据 SIGN。SIGN 的生成方式见 9.3.7.1；
   3) 生成 PERSONAL AUTHENTICATE 的响应报文，并回送给终端。
g) 验证签名（步骤 8）：终端收到 PERSONAL AUTHENTICATE 命令的响应报文后，进行以下处理：
   1) 若回送的状态字不是“9000”，身份鉴别失败，应用处理过程终止；
   2) 检查发卡方公钥证书与人员签名证书相关信息是否存在。若不存在，身份鉴别失败，应用处理过程终止；
   3) 若发卡方公钥证书有效，使用发卡方公钥证书验证人员签名证书是否有效。若人员签名证书验证失败，身份鉴别失败，应用处理过程终止；
   4) 终端从人员签名证书中提取签名公钥，验证签名数据 SIGN 是否正确；若签名验证正确，身份鉴别成功；否则，身份鉴别失败，应用处理过程终止。
h) 应用处理及返回确认（步骤 9、步骤 10）：身份鉴别成功后，可执行后续的应用处理。

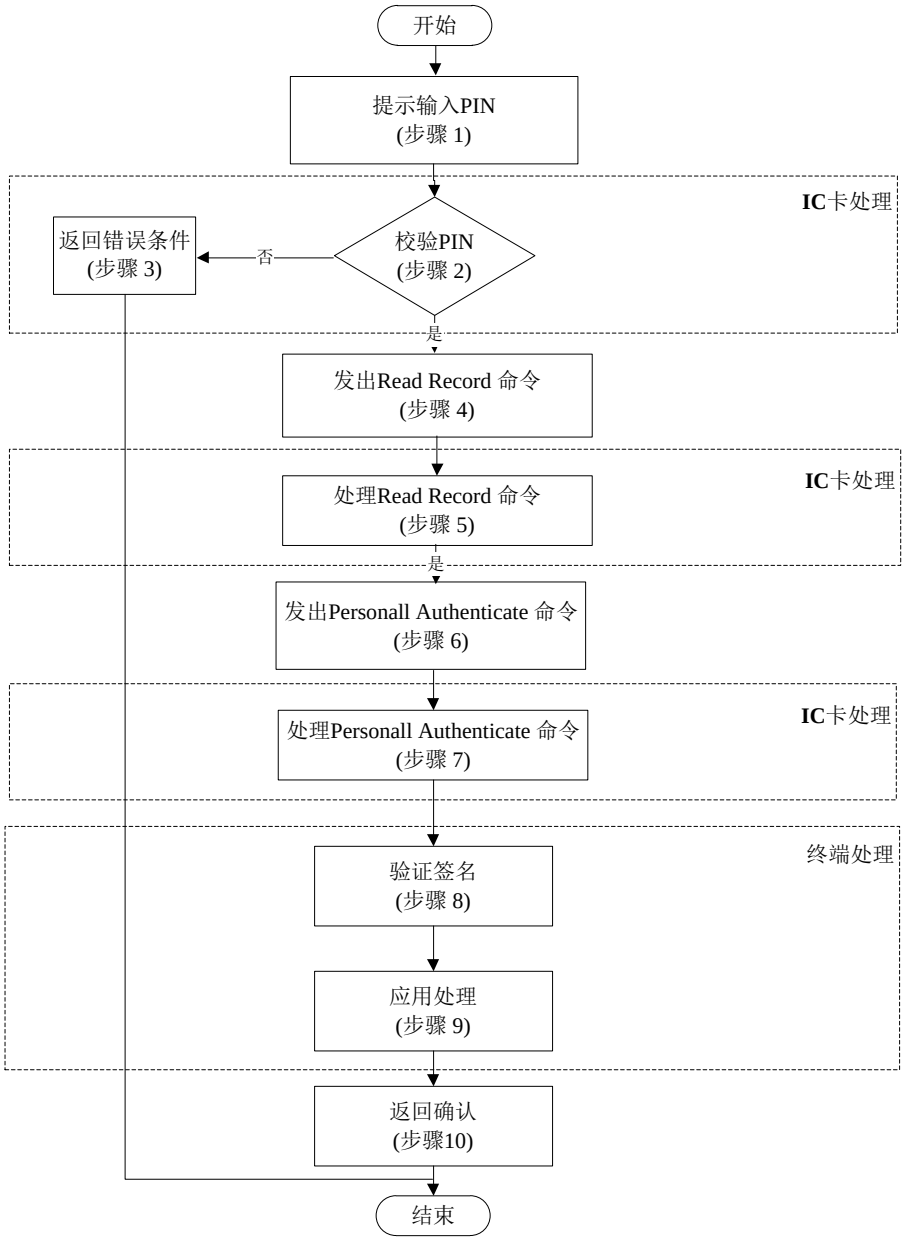


图4　身份鉴别处理流程

7.4　卡片鉴别

7.4.1　卡片数据

卡片鉴别使用的数据元见表9。

表9　卡片鉴别——使用的数据元

数据元	描述
发卡方公钥索引	由发卡方提供。指明了用于验证人员签名证书的发卡方公钥。
人员签名证书	包含人员签名公钥，在卡片个人化时写入卡中。
参数 1	保留参数，用于卡片鉴别算法的扩展。

表9 （续）

数据元	描述
参数 2	保留参数，用于卡片鉴别算法的扩展。
签名的动态应用数据	卡片生成的动态应用数据及签名

在卡片鉴别处理中，卡片内部使用的数据元见表10。

表10 卡片鉴别——卡片内部使用的数据元

数据元	描述
卡片随机数	由卡片内部产生。
签名私钥	用于对动态应用数据进行签名。

7.4.2 终端数据

卡片鉴别使用的终端数据见表11。

表11 卡片鉴别——终端数据

数据元	描述
终端随机数	由终端生成。

7.4.3 相关命令

7.4.3.1 卡片鉴别命令

终端使用CARD AUTHENTICATE命令请求进行卡片鉴别。

当卡片收到CARD AUTHENTICATE命令，使用签名私钥生成签名的动态应用数据。在CARD AUTHENTICATE命令的响应数据报文中包含该数据。

发送CARD AUTHENTICATE命令前，需要终端发送READ RECORD命令或READ BINARY命令，从卡片中读出处理卡片鉴别的人员签名证书以及其他相关数据。

CARD AUTHENTICATE命令的定义和描述见附录C。

7.4.4 处理过程

卡片鉴别是通过读取教育卡的卡片鉴别相关数据，采用动态数据认证的方式，验证教育卡是否合法。卡片鉴别处理过程如下：

a) 发出/处理 READ RECORD 或者 READ BINARY 命令：终端使用 READ RECORD 命令或者 READ BINARY 命令从教育卡读取卡片鉴别相关数据，并保存数据用于卡片鉴别。

b) 发出 CARD AUTHENTICATE 命令：终端生成终端随机数，发出 CARD AUTHENTICATE 命令。

c) 处理 CARD AUTHENTICATE 命令：教育卡收到 CARD AUTHENTICATE 命令后，进行以下处理：

   1) 检查 CARD AUTHENTICATE 命令是否包含终端随机数。若未包含终端随机数，回送状态字“6985”；

   2) 生成签名数据 SIGN。SIGN 的生成方式见 9.3.7.1；

   3) 生成 CARD AUTHENTICATE 的响应报文，回送给终端。

d) 验证签名：收到 CARD AUTHENTICATE 命令的响应报文后，终端进行以下处理：

   1) 若回送的状态字不是“9000”，卡片鉴别失败，应用处理过程终止；

2) 检查发卡方公钥证书及人员签名证书相关信息是否存在。若不存在，卡片鉴别失败，应用处理过程终止；
3) 若发卡方公钥证书有效，终端使用发卡方公钥证书验证人员签名证书是否有效。若人员签名证书验证失败，卡片鉴别失败，应用处理过程终止；
4) 终端从人员签名证书中提取签名公钥，验证签名数据 SIGN 是否正确。若签名验证正确，则卡片鉴别成功；若签名验证失败，应用处理过程终止。

e) 后续处理：卡片鉴别成功后，可执行后续的应用处理。

7.5 信息读取

7.5.1 卡片数据

信息读取所使用的卡片数据见表12。

表12 读记录数据——卡片数据

数据元	描述
AEF	即应用数据文件，包括应用处理使用的数据。每个 AEF 用 SFI 唯一标识。
SFI	用来唯一标识一个 AEF。

7.5.2 终端数据

信息读取不使用终端数据。

7.5.3 相关命令

7.5.3.1 读记录/读二进制文件命令

READ RECORD命令从变长记录文件、循环记录文件或扩展记录文件中读取数据。READ BINARY命令从二进制文件中读取数据。

READ RECORD命令、READ BINARY命令的定义和描述见附录C。

7.5.4 处理过程

终端通过发送READ RECORD命令或READ BINARY命令，从EF中读取数据。根据所读数据的不同，数据记录可自由读取或认证后读取。信息读取的处理过程如下：

a) 发出信息读取命令：终端发出 READ RECORD 命令或 READ BINARY 命令；
b) 处理信息读取命令:教育卡收到 READ RECORD 命令或 READ BINARY 命令,返回请求的数据内容；
c) 获取信息内容：终端从响应数据报文中获取数据内容。

7.6 信息更改

7.6.1 卡片数据

信息更改所使用的卡片数据见表13。

表13 修改记录数据——卡片数据

数据元	描述
AEF	即应用数据文件，包括应用处理使用的数据。每个 AEF 用 SFI 唯一标识。

表13 （续）

数据元	描述
SFI	用来唯一标识一个 AEF。
安全报文认证密钥	用于卡片验证 MAC。

7.6.2 终端数据

信息更改不使用终端数据。

7.6.3 相关命令

7.6.3.1 更新记录/更新二进制文件命令

UPDATE RECORD命令用于更新变长记录文件、循环记录文件或扩展记录文件的数据。UPDATE BINARY命令用于更新二进制文件的数据。

发送修改命令前，需要发送GET CHALLENG命令。

UPDATE RECORD命令、UPDATE BINARY命令的定义和描述见附录C。

7.6.4 处理过程

终端通过发送UPDATE RECORD或者UPDATE BINARY命令，修改EF中的数据。信息更改应满足信息的更新权限，该权限包括禁止读写和密钥保护。

信息更改的处理过程如下：

a) MAC 计算：卡片将提供给终端的卡片随机数作为过程密钥分散因子分散出过程密钥，按照附录 D 中安全报文的算法，使用安全报文认证密钥计算 MAC；
b) MAC 验证：新生成的 MAC 和命令中的 MAC 进行比较，若 MAC 验证失败，教育卡返回状态字“6988”；若 MAC 验证成功，进行后续处理；
c) 变更记录：判断 SFI 和记录号是否存在。若 SFI 不存在，卡片返回状态字“6A82”；若记录号不存在，卡片返回状态字“6A83”；若 SFI 和记录号存在，继续后续处理；
d) 更新指定文件内容。若更新成功，卡片返回状态字“9000”。

7.7 学籍注册

7.7.1 卡片数据

学籍注册使用的卡片数据元见表14。

表14 学籍注册——卡片数据

数据元	描述
发卡方公钥索引	由发卡方提供。指明了用于验证人员签名证书的发卡方公钥。
人员签名证书	包含人员签名公钥，在卡片个人化时放入卡中。
参数 1	保留参数，用于卡片鉴别算法的扩展。
参数 2	保留参数，用于卡片鉴别算法的扩展。
签名的动态应用数据	卡片生成的动态应用数据及签名。
AEF	即应用数据文件，包括应用处理使用的数据。每个 AEF 用 SFI 唯一标识。
SFI	用来唯一标识一个 AEF。

在学籍注册处理中，卡片内部使用的数据元见表15。

表15 学籍注册——卡片内部使用的数据元

数据元	描述
卡片随机数	由卡片内部产生。
签名私钥	用于动态应用数据签名。

7.7.2 终端数据

学籍注册使用的终端数据见表16。

表16 学籍注册——终端数据

数据元	描述
终端随机数	由终端生成。

7.7.3 相关命令

7.7.3.1 卡片鉴别

终端使用CARD AUTHENTICATE命令验证卡片的合法性。
CARD AUTHENTICATE命令的定义和描述见附录C。

7.7.3.2 读记录

终端使用READ RECORD读取卡片内存储的学籍信息、学籍注册信息。
READ RECORD命令的定义和描述见附录C。

7.7.3.3 添加记录

终端使用APPEND RECORD添加学籍注册信息。
APPEND RECORD命令的定义和描述见附录C。

7.7.3.4 更新记录

终端使用UPDATE RECORD更新学籍信息。
UPDATE RECORD命令的定义和描述见附录C。

7.7.4 处理过程

学籍注册用于学生入学报到登记，在教育卡内增加学籍注册信息。处理过程如下：

a) 发出/处理 CARDAUTHENTICATE 命令：终端使用 CARDAUTHENTICATE 命令以验证教育卡的有效合法性；
b) 发出/处理 READ RECORD 命令：终端使用 READ RECORD 命令从教育卡读取学籍信息记录、学籍注册信息等数据；
c) 发出/处理 APPEND RECORD 命令：终端使用 APPEND RECORD 命令新增学籍注册信息等数据；
d) 发出/处理 UPDATE RECORD 命令：终端使用 UPDATE RECORD 命令更新学籍状态等数据。

7.8 营养改善计划用餐登记

7.8.1 卡片数据

营养改善计划用餐登记使用的卡片数据元见表17。

表17 营养改善计划用餐登记——卡片数据

数据元	描述
发卡方公钥索引	由发卡方提供。指明了终端里用于验证教育卡公钥证书的发卡方公钥。
人员签名证书	包含人员签名公钥，在卡片个人化时放入卡中。
参数 1	保留参数，用于身份鉴别算法的扩展。
参数 2	保留参数，用于身份鉴别算法的扩展。
签名的动态应用数据	卡片生成的动态应用数据及签名。
AEF	即应用数据文件，包括应用处理使用的数据。每个 AEF 用 SFI 唯一标识。
SFI	用来唯一标识一个 AEF。

在营养改善计划用餐登记处理中，卡片内部使用的数据元见表18。

表18 营养改善计划用餐登记——卡片内部使用的数据元

数据元	描述
卡片随机数	由卡片内部产生。
签名私钥	用于动态应用数据的签名。

7.8.2 终端数据

营养改善计划用餐登记使用的终端数据见表19。

表19 营养改善计划用餐登记——终端数据

数据元	描述
终端随机数	由终端生成。

7.8.3 相关命令

7.8.3.1 卡片鉴别

终端使用CARD AUTHENTICATE命令验证卡片的合法性。
CARD AUTHENTICATE命令的定义和描述见附录C。

7.8.3.2 读记录

终端使用READ RECORD读取卡片内存储的营养餐资格信息、营养餐领餐信息。
READ RECORD命令的定义和描述见附录C。

7.8.3.3 添加记录

终端使用APPEND RECORD添加营养餐领餐信息。
APPEND RECORD命令的定义和描述见附录C。

7.8.3.4 更新记录

终端使用UPDATE RECORD更新营养餐领餐信息。

UPDATE RECORD命令的定义和描述见附录C。

7.8.4 处理过程

营养改善计划用餐登记功能是在教育卡中记录学生领用营养餐的信息。处理过程如下：

a) 发出/处理 CARD AUTHENTICATE 命令：终端使用 CARD AUTHENTICATE 命令以验证教育卡的有效合法性；
b) 发出/处理 READ RECORD 命令：终端使用 READ RECORD 命令从教育卡读取营养餐资格信息、营养餐领餐信息等数据；
c) 发出/处理 APPEND RECORD 命令：终端使用 APPEND RECORD 命令写入营养餐领餐信息等数据；
d) 发出/处理 UPDATE RECORD 命令：终端使用 UPDATE RECORD 命令更新营养餐领餐信息等数据。

7.9 学位证书写入

7.9.1 卡片数据

学位证书写入使用的卡片数据元见表20。

表20 学位证书写入——卡片数据

数据元	描述
发卡方公钥索引	由发卡方提供。指明了终端里用于验证教育卡公钥证书的发卡方公钥。
人员签名证书	包含人员签名公钥，在卡片个人化时放入卡中。
参数 1	保留参数，用于身份鉴别算法的扩展。
参数 2	保留参数，用于身份鉴别算法的扩展。
签名的动态应用数据	卡片生成的动态应用数据及签名。

在学位证书写入处理中，卡片内部使用的数据元见表21。

表21 学位证书写入——学位证书写入处理中卡片内部数据元

数据元	描述
卡片随机数	由卡片内部产生。
签名私钥	用于动态应用数据的签名。

7.9.2 终端数据

学位证书写入使用的终端数据见表22。

表22 学位证书写入——终端数据

数据元	描述
终端随机数	由终端生成。

7.9.3 相关命令

7.9.3.1 卡片鉴别

终端使用CARD AUTHENTICATE命令验证卡片的合法性。

CARD AUTHENTICATE命令的定义和描述见附录C。

7.9.3.2 电子学位证书写入

终端使用WRITE DIPLOMA命令写入电子学位证书信息。

WRITE DIPLOMA命令的定义和描述见附录C。

7.9.4 处理过程

学位证书写入是在教育电子证件中写入电子学位证书信息。处理过程如下：

a) 发出/处理 CARD AUTHENTICATE 命令：终端使用 CARD AUTHENTICATE 命令以验证教育电子证件的有效合法性；

b) 发出/处理 WRITE DIPLOMA 命令：终端使用 WRITE DIPLOMA 命令写入电子学位证书信息。

7.10 毕业/结业证书写入

7.10.1 卡片数据

毕业/结业证书写入使用的卡片数据元见表23。

表23 毕业/结业证书写入——卡片数据

数据元	描述
发卡方公钥索引	由发卡方提供。指明了终端里用于验证教育卡公钥证书的发卡方公钥。
人员签名证书	包含人员签名公钥，在卡片个人化时放入卡中。
参数 1	保留参数，用于身份鉴别算法的扩展。
参数 2	保留参数，用于身份鉴别算法的扩展。
签名的动态应用数据	卡片生成的动态应用数据及签名。

在毕业/结业证书写入处理中，卡片内部使用的数据元见表24。

表24 毕业/结业证书写入——卡片内部使用的数据元

数据元	描述
卡片随机数	由卡片内部产生。
签名私钥	用于动态应用数据的签名。

7.10.2 终端数据

毕业/结业证书写入使用的终端数据见表25。

表25 毕业/结业证书写入——终端数据

数据元	描述
终端随机数	由终端生成。

7.10.3 相关命令

7.10.3.1 卡片鉴别

终端使用CARD AUTHENTICATE命令验证卡片的合法性。

CARD AUTHENTICATE命令的定义和描述见附录C。

7.10.3.2 毕业/结业证书写入

终端使用WRITE DIPLOMA命令写入电子毕业证或电子结业证信息。
WRITE DIPLOMA命令的定义和描述见附录C。

7.10.4 处理过程

毕业/结业证书写入是在教育电子证件中写入电子毕业证或电子结业证信息。处理过程如下：

a) 发出/处理 CARD AUTHENTICATE 命令：终端使用 CARD AUTHENTICATE 命令以验证教育卡的有效合法性；
b) 发出/处理 WRITE DIPLOMA 命令：终端使用 WRITE DIPLOMA 命令写入电子毕业证或电子结业证信息。

7.11 交通优惠信息写入

7.11.1 卡片数据

交通优惠信息写入使用的卡片数据元见表26。

表26 交通优惠信息写入——卡片数据

数据元	描述
发卡方公钥索引	由发卡方提供。指明了终端里用于验证教育卡公钥证书的发卡方公钥。
人员签名证书	包含人员签名公钥，在卡片个人化时放入卡中。
参数 1	保留参数，用于身份鉴别算法的扩展。
参数 2	保留参数，用于身份鉴别算法的扩展。
签名的动态应用数据	卡片生成的动态应用数据及签名。
AEF	卡片数据文件，包括应用处理使用的数据。每个 AEF 用 SFI 唯一标识。
SFI	用来唯一标识一个 AEF。

在交通优惠信息写入处理中，卡片内部使用的数据元见表27。

表27 交通优惠信息写入——交通优惠信息写入处理中卡片内部数据元

数据元	描述
卡片随机数	由卡片内部产生。
签名私钥	用于动态应用数据的签名。

7.11.2 终端数据

交通优惠信息写入使用的终端数据见表28。

表28 交通优惠信息写入——终端数据

数据元	描述
终端随机数	由终端生成。

7.11.3 相关命令

7.11.3.1 卡片鉴别命令

终端使用CARD AUTHENTICATE命令验证卡片的合法性。
CARD AUTHENTICATE命令的定义和描述见附录C。

7.11.3.2 读记录命令

终端使用READ RECORD读取卡片内存储的交通票务优惠信息记录、使用记录等信息。
READ RECORD命令的定义和描述见附录C。

7.11.3.3 添加记录命令

终端使用APPEND RECORD添加建交通票务优惠信息使用记录等信息。
APPEND RECORD命令的定义和描述见附录C。

7.11.3.4 更新记录命令

终端使用UPDATE RECORD更新交通票务优惠信息使用记录等信息。
UPDATE RECORD命令的定义和描述见附录C。

7.11.4 处理过程

交通优惠信息写入功能是在教育卡中记录学生优惠票的购买记录信息。处理过程如下：

a) 发出/处理 CARD AUTHENTICATE 命令：终端使用 CARD AUTHENTICATE 命令以验证教育卡的有效合法性；
b) 发出/处理 READ RECORD 命令：终端使用 READ RECORD 命令实现从教育卡读取交通票务优惠信息记录、使用记录等信息；
c) 当终端收到交通优惠相关信息，根据相关业务规范验证持卡人是否可以享受交通优惠。若持卡人不能享受交通优惠，则终端应提示错误信息；
d) 发出/处理 APPEND RECORD 命令：终端使用 APPEND RECORD 命令新增交通票务优惠信息使用记录等信息；
e) 发出/处理 UPDATE RECORD 命令：终端使用 UPDATE RECORD 命令更新交通票务优惠信息使用记录等信息。

7.12 学位证书读取

7.12.1 卡片数据

学位证书读取使用的卡片数据元见表29。

表29 学位证书写入——卡片数据

数据元	描述
发卡方公钥索引	由发卡方提供。指明了终端里用于验证教育卡公钥证书的发卡方公钥。
人员签名证书	包含人员签名公钥，在卡片个人化时放入卡中。
参数 1	保留参数，用于身份鉴别算法的扩展。
参数 2	保留参数，用于身份鉴别算法的扩展。
签名的动态应用数据	卡片生成的动态应用数据及签名。

在学位证书读取处理中，卡片内部使用的数据元见表30。

表30　学位证书写入——卡片内部使用数据元

数据元	描述
卡片随机数	由卡片内部产生。
签名私钥	用于动态应用数据的签名。

7.12.2　终端数据

学位证书读取使用的终端数据见表31。

表31　学位证书写入——终端数据

数据元	描述
终端随机数	由终端生成。

7.12.3　相关命令

7.12.3.1　卡片鉴别命令

终端使用CARD AUTHENTICATE命令验证卡片的合法性。
CARD AUTHENTICATE命令的定义和描述见附录C。

7.12.3.2　读取学位证书命令

终端使用READ DIPLOMA命令读取教育电子证件中的电子学位证书等信息。
READ DIPLOMA命令的定义和描述见附录C。

7.12.4　处理过程

学位证书读取是从教育电子证件中读取电子学位证书信息。处理过程如下：

a) 发出/处理 CARD AUTHENTICATE 命令：终端使用 CARD AUTHENTICATE 命令以验证教育电子证件的有效合法性；
b) 发出/处理 READ DIPLOMA 命令：终端使用 READ DIPLOMA 命令读取电子学位证书等信息。

7.13　毕业/结业证书读取

7.13.1　卡片数据

毕业/结业证书读取使用的卡片数据元见表32。

表32　毕业证书读取——卡片数据

数据元	描述
发卡方公钥索引	由发卡方提供。指明了终端里用于认证教育卡公钥证书的发卡方公钥。
人员签名证书	包含人员签名公钥，在卡片个人化时放入卡中。
参数 1	保留参数，用于身份鉴别算法的扩展。
参数 2	保留参数，用于身份鉴别算法的扩展。
签名的动态应用数据	卡片生成的动态应用数据及签名。

在毕业/结业证书读取处理中，卡片内部使用的数据元见表33。

表33 毕业/结业证书读取——卡片内部使用数据元

数据元	描述
卡片随机数	卡片内部产生。
签名私钥	用于动态应用数据的签名。

7.13.2 终端数据

毕业/结业证书读取使用的终端数据见表34。

表34 毕业/结业证书读取——终端数据

数据元	描述
终端随机数	由终端生成。

7.13.3 相关命令

7.13.3.1 卡片鉴别命令

终端使用CARD AUTHENTICATE命令验证卡片的合法性。
CARD AUTHENTICATE命令的定义和描述见附录C。

7.13.3.2 读取毕业/结业证书命令

终端使用READ DIPLOMA命令读取教育电子证件中的电子毕业证或电子结业证信息。
READ DIPLOMA命令的定义和描述见附录C。

7.13.4 处理过程

毕业/结业证书读取是从教育电子证件中读取电子毕业证或电子结业证信息。处理过程如下：

a) 卡片鉴别：终端使用 CARD AUTHENTICATE 命令以验证教育卡的有效合法性；
b) 发出/处理 READ DIPLOMA 命令：终端使用 READ DIPLOMA 命令读取电子毕业证或电子结业证信息。

7.14 ESN 读取

7.14.1 卡片数据

ESN读取所使用的卡片数据见表35。

表35 ESN 读取——卡片文件

数据元	描述
AEF	即应用数据文件，包括应用处理使用的数据。每个 AEF 用 SFI 唯一标识。
SFI	用来唯一标识一个 AEF。

7.14.2 终端数据

ESN读取不使用终端数据。

7.14.3 相关命令

7.14.3.1 读二进制命令

终端使用READ BINARY命令读取ESN信息。

READ BINARY命令的定义和描述见附录C。

7.14.4 处理过程

ESN读取是从教育卡中读取持卡人的ESN。处理过程如下：

a) 收到命令并返回信息：卡片收到终端发送的读取 READ BINARY 命令，返回终端请求的数据内容给终端；

b) 获取 ESN 信息：终端从响应数据报文解析得出 ESN。

7.15 交易认证

7.15.1 卡片数据

交易认证使用的卡片数据元见表36。

表36 交易认证——卡片数据

数据元	描述
应用交易计数器	卡片内部应用处理计数器。
卡片随机数	卡片内部产生。
应用密文密钥	卡片验证 ARPC 使用的对称密钥。

7.15.2 终端数据

终端用交易认证命令使用ARPC和表37的数据，进行交易认证。

表37 交易认证——终端数据

数据元	描述
交易类型授权码	表明当前的交易类型： 01：联机圈存 02：联机消费 其他：RFU

7.15.3 相关命令

7.15.3.1 交易认证命令

终端使用TRANS AUTHENTICATE命令实现交易认证。

TRANS AUTHENTICATE命令的定义和描述见附录C。

7.15.4 处理过程

应用系统或终端通过交易认证，以验证联机圈存交易及终端的合法性。处理过程如下：

a) 生成 ARPC：主机产生一个 ARPC 和交易类型授权码，用于验证联机圈存交易及终端的合法性。ARPC 的计算方法见附录 E.4；

b) 发出 TRANS AUTHENTICATE 命令：终端向卡片发出 TRANS AUTHENTICATE 命令；
c) 处理 TRANS AUTHENTICATE 命令：教育卡收到 TRANS AUTHENTICATE 命令后，应验证 ARPC 的有效性。若 ARPC 有效，则交易认证成功。

7.16 联机圈存

7.16.1 卡片数据

联机圈存命令使用的卡片数据见表38。

表38 联机圈存——卡片文件

数据元	描述
应用交易计数器	卡片内部应用处理计数器。
联机圈存密钥	用于计算圈存报文签别码。
应用密文密钥	用于计算 AC。

7.16.2 终端数据

联机圈存命令使用的终端数据见表39。

表39 联机圈存——终端数据

数据元	描述
交易金额	圈存交易的交易金额。
交易类型授权码	表明当前的交易类型：01：联机圈存；02：联机消费。
终端机编号	终端机编号。
交易日期（主机）	交易日期。
交易时间（主机）	交易时间。

7.16.3 相关命令

7.16.3.1 联机圈存命令

终端使用CREDIT FOR ONLINE LOAD命令实现联机圈存交易处理。
CREDIT FOR ONLINE LOAD命令的定义和描述见附录C。

7.16.4 处理流程

通过联机圈存交易，持卡人可将其在银行相应账户上的资金划入教育卡应用账户中。这种交易应在指定的终端上联机进行并要求满足相关认证条件。联机圈存处理流程如下。

a) 发出 READ RECORD 命令：终端发出 READ RECORD 命令启动联机圈存交易；
b) 发出 CARD AUTHENTICATE 命令：终端进行卡片鉴别，以验证教育卡的合法性；
c) 发出 GET CHALLENGE 命令：终端发出 GET CHALLENGE 命令获取 8 字节随机数；
d) 交易认证：主机产生一个 ARPC 和交易类型授权码，用于验证联机圈存交易及终端的合法性。ARPC 的计算方法见附录 E.4；
e) 发出 TRANS AUTHENTICATE 命令：终端收到主机发来的交易认证交易接受报文后，发出 TRANS AUTHENTICATE 命令；

f) 验证 ARPC：教育卡收到 TRANS AUTHENTICATE 命令后，确认 ARPC 的有效性。若 ARPC 无效，向终端回送状态字“6300”，联机圈存交易处理中止；
a) 联机圈存交易处理：主机进行联机圈存交易处理后，生成一个 MAC，向终端发送联机圈存交易接受报文；
b) 发出 CREDIT FOR ONLINE LOAD 命令：终端收到主机发来的联机圈存交易接受报文后，向教育卡发出 CREDIT FOR ONLINE LOAD 命令；
c) 验证 MAC：教育卡收到 CREDIT FOR ONLINE LOAD 命令后，确认 MAC 的有效性。若 MAC 无效，向终端回送状态字“9302”；
d) 更新卡上余额：教育卡更新卡上钱包余额,生成 AC。AC 的计算方法见附录 E.3；
e) 返回确认：在交易成功后，教育卡通过 CREDIT FOR ONLINE LOAD 命令的响应报文将 AC 回送给终端。

7.17 联机消费

7.17.1 卡片数据

联机消费交易使用的卡片数据见表40。

表40 联机消费——卡片文件

数据元	描述
应用交易计数器	卡片内部应用处理计数器。
联机消费密钥	计算消费报文签别码的对称密钥。
应用密文密钥	卡片计算 AC 使用的对称密钥。

7.17.2 终端数据

联机消费交易使用的终端数据见表41。

表41 联机消费——终端数据

数据元	描述
交易金额	消费交易的交易金额。

7.17.3 相关命令

7.17.3.1 联机消费

终端使用DEBIT FOR ONLINE PURCHASE命令实现联机消费交易处理。
DEBIT FOR ONLINE PURCHASE命令的定义和描述见附录C。

7.17.4 处理流程

联机消费交易允许持卡人使用余额进行购物或获取服务。此交易可以在指定的终端上联机进行。联机消费处理流程如下：

a) 发出 READ RECORD 命令：终端发出 READ RECORD 命令启动联机消费交易；
b) 发出 CARD AUTHENTICATE 命令：终端进行卡片鉴别，以验证教育卡的合法性；
c) 发出 GET CHALLENGE 命令：终端发出 GET CHALLENGE 命令获取 8 字节随机数；

d) 交易认证：主机产生一个 ARPC 和交易类型授权码，用于验证联机消费交易及终端的合法性。ARPC 的计算方法见附录 E.4；
e) 发出 TRANS AUTHENTICATE 命令：终端收到主机发来的交易认证交易接受报文后，发出 TRANS AUTHENTICATE 命令；
f) 验证 ARPC：教育卡收到 TRANS AUTHENTICATE 命令后，确认 ARPC 的有效性。若 ARPC 无效，向终端回送状态字“6300”，联机消费交易中止；
g) 交易处理：主机进行联机消费交易处理，生成一个 MAC，向终端发送联机消费交易接受报文；
h) 发出 DEBIT FOR ONLINE PURCHASE 命令：终端收到主机发来的联机消费交易接受报文后，向教育卡发出 DEBIT FOR ONLINE PURCHASE 命令；
i) 验证 MAC：教育卡收到 DEBIT FOR ONLINE PURCHASE 命令后，确认 MAC 的有效性。若 MAC 无效，向终端回送状态字“9302”；
j) 更新卡上钱包余额：教育卡更新卡上钱包余额,生成 AC。AC 的计算方法见附录 E.3；
k) 返回确认：教育卡通过 DEBIT FOR ONLINE PURCHASE 命令的响应报文将 AC 回送给终端。

7.18 教育卡认证码读取

7.18.1 卡片数据

教育卡认证码读取所使用的卡片数据见表42。

表42 读记录数据——卡片文件

数据元	描述
教育卡认证码	教育卡芯片中内置的认证码信息，不可更改。

7.18.2 终端数据

教育卡认证码读取不使用终端数据。

7.18.3 相关命令

7.18.3.1 教育卡认证码读取

READ AUTHCODE命令的定义和描述见附录C。

7.18.4 处理过程

终端通过发送READ AUTHCODE命令，从教育卡芯片中读取教育卡认证码。处理过程如下：
a) 收到命令并返回信息：卡片收到终端发送的教育卡认证码读取命令，生成响应报文，返回教育卡认证码；
b) 获取教育卡认证码：终端从命令响应报文中获取教育卡认证码。

7.19 应用维护功能

7.19.1 概述

应用维护功能应在拥有相应密钥的设备上执行。

7.19.2 应用锁定

终端发出APPLICATION BLOCK命令来临时锁定应用或永久锁定应用。若为永久锁定应用，教育卡将设置一个内部标志以表明不允许执行APPLICATION UNBLOCK命令。

APPLICATION BLOCK命令的定义和描述见附录C。

APPLICATION BLOCK命令成功执行后，导致应用处于无效状态：

a) 选择此应用时，对 SELECT 命令，教育卡回送状态字“6A81”和 FCI；

b) 在应用被选择后，除以下情况外，教育卡对其他命令只回送状态字“6985”：

1) 当用 SELECT 命令选择此应用或其他应用时；

2) GET CHALLANGE 命令；

3) APPLICATION BLOCK 命令；

4) APPLICATION UNBLOCK 命令。

7.19.3 应用解锁

终端发出APPLICATION UNBLOCK命令对应用进行解锁。

若对某应用连续三次解锁失败，教育卡将永久锁定该应用，并回送状态字“9303”。

APPLICATION UNBLOCK命令的定义和描述见附录C。

7.19.4 PIN 码解锁与重装

终端发出PIN UNBLOCK/RELOAD PIN命令对PIN码解锁或重置。

若PIN UNBLOCK/RELOAD PIN命令连续三次执行失败，教育卡将永久锁定，并回送状态字“9303”。

PIN UNBLOCK/RELOAD PIN命令的定义和描述见附录C。

7.19.5 修改 PIN 码

当教育卡接到CHANGE PIN命令时，将检查PIN尝试计数器，进行以下处理：

a) 若 PIN 尝试计数器值为 0，回送状态字“6983”；

b) 将命令中的“当前 PIN”和教育卡上存放的 PIN 比较；

c) 若二者相同，将教育卡上的 PIN 改为命令中的新 PIN，将 PIN 尝试计数器置为 PIN 重试的最大次数；

d) 若二者不同，将 PIN 尝试计数器减 1，回送状态字“63Cx”，x 是 PIN 尝试计数器的新值。

7.20 防拔

卡片在交易处理的任何情况下，应保持数据的完整性。在每次更新数据前对数据进行备份，并且在重新加电后自动地触发恢复机制。

8 教育卡卡面规范信息

教育卡卡面规范信息的要求见附录F。

9 教育卡应用安全要求

9.1 总体要求

教育卡应用安全的总体要求如下：

a) 教育卡内存储与应用相关的对称密钥和非对称密钥。密钥管理应符合国家密码主管部门的管理要求；
b) 教育卡采用公钥鉴别机制实现对卡片和持卡人的身份鉴别；
c) 教育卡使用国产密码算法实现对数据的完整性和机密性保护；
d) 教育卡COS应具有鉴别与核实、数据加密与解密、文件访问控制的安全机制，并写入国家密码主管部门批准的安全芯片的ROM中；
e) 教育卡内应建立安全域，保护密码算法代码模块、密钥和卡内应用的安全。

9.2 加密机制

9.2.1 对称加密机制

9.2.1.1 加密解密

采用CBC模式的16字节分组加密算法以及MAC过程密钥K_S，对任意长度的报文MSG计算密文。计算步骤如下：

步骤1：填充并分块

a) 在MSG的右端强制加上1个‘80’字节，然后再在右端加上最少的‘00’字节，使得结果报文的长度是16字节的整数倍；
b) 然后，将结果报文拆分为16字节的块X_1，X_2，…… X_K。

步骤2：加密过程密钥

加密过程密钥K_S长度为16字节。

步骤3：密文计算

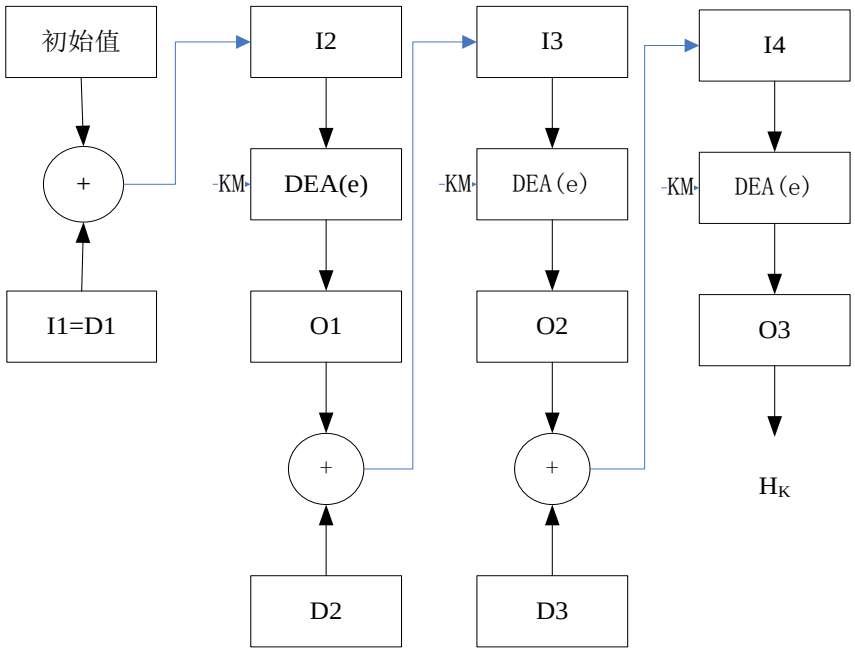
用加密过程密钥以CBC模式的分组加密处理16字节块X_1, X_2, ... , X_K：

Hk := ALG(K)[Xi⊕Hi-1]，这里k = 1, 2, ... , K。

针对安全报文MAC、交易MAC、应用密文，H0的初始值 H0 :=（‘00’||‘00’||‘00’||‘00’||‘00’||‘00’|| ‘00’|| ‘00’||‘00’||‘00’|| ‘00’|| ‘00’||‘00’||‘00’|| ‘00’）。

Hk的计算方法如图5所示。

步骤4：最终密文生成。



说明：

I = 输入　　D = X = 数据块
DEA(e)= 数据加密算法（加密模式）　　KM = MAC过程密钥
O = 输出　　+ = 异或

图5　使用 SM4 算法计算 H_K 的算法

9.2.1.2　过程密钥产生

对于联机圈存与联机消费应用流程中需要计算MAC、AC与ARPC时使用的过程密钥的产生方法如下：

步骤1：卡片（或发卡方）决定是使用MAC密钥还是数据加密密钥来进行所选择的算法处理；

步骤2：将当前的ATC在其左边用十六进制数字‘0’填充到8个字节作为数据源A，将当前的ATC异或十六进制值FFFF后在其左边用十六进制数字‘0’填充到8个字节作为数据源B，将数据源A和数据源B串连，用选定的密钥对该数据作如图6所示的运算产生过程密钥。

Z:=ALG(Key)[[‘00’ || ‘00’ || ‘00’ || ‘00’ || ‘00’ || ‘00’ ||ATC|| ‘00’ || ‘00’ || ‘00’ || ‘00’ || ‘00’ ||(ATC⊕‘FFFF’)]

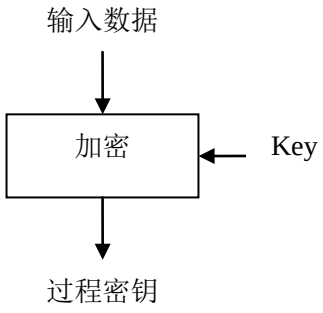


图6　过程密钥产生流程

对于文件读写以及加解密的过程密钥的计算算法为：输入数据为16字节随机数，对输入数据做加密运算来产生过程密钥，如图6所示。

9.2.1.3 子密钥分散

子密钥分散使用一个16字节的发卡方主密钥IMK分散得出用于密文生成、发卡方认证和安全报文的子密钥。

以主账号和主账号序列号（若主账号序列号不存在，则用一个字节‘00’代替）的最右16个数字及其衍生数据作为输入数据，以发卡方主密钥IMK作为密钥，生成16字节的教育卡子密钥MK。

步骤1：将主账号和主账号序列号连接生成为16字节输入数据；

步骤 2：计算：Z=ALG(IMK)[X]。Z 即子密钥 MK。

子密钥分散流程如图7所示。

发卡行主机安全模块

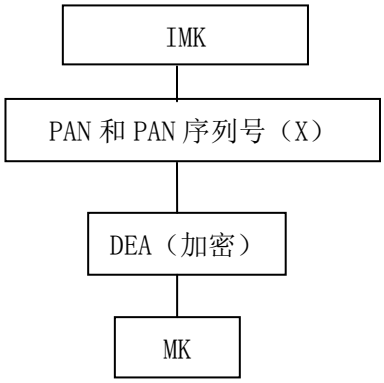


图7 子密钥分散流程

9.2.2 非对称加密机制

9.2.2.1 密码算法

非对称密码算法使用SM2密码算法，算法规范见GM/T 0003-2012。

SM2签名方案使用如下三种函数：

a) 签名函数 Sign(S_K)[M]，该函数输出两个相同长度的数字 r 和 s；

b) 验证函数 Verify(P_K)[M, Sign(S_K)[M]]，该函数输出 True 或 False，表示验证正确或失败；

c) 哈希算法 H[i]，将任意长度的报文映射为一个 32 字节的哈希值。

9.2.2.2 数字签名产生

对任意长度的数据组成的报文MSG计算签名S的过程如下：

a) 计算 ZA=SM3(ENTLA || IDA || a || b || xG ||yG || xA || yA)。其中 IDA 固定设置为 16 字节的数据 0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38, 0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38；ENTLA 值为两个字节数据 0x00, 0x80；

b) 计算报文 MSG 的 32 字节的 HASH 值 h= SM3 [ZA||MSG]；

c) 计算 Sign(SK)[h]，得到两个数字 r 和 s；

d) 数字签名 S= r||s，即将数字 r 和 s 串联而成。

9.2.2.3 数字签名验证

对任意长数据组成的报文MSG验证签名S的过程如下：

a) 计算 Z_A=SM3($ENTL_A$ || ID_A || a || b || x_G ||y_G || x_A || y_A)。其中 ID_A固定设置为 16 字节的数据 0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38, 0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38；$ENTL_A$值为两个字节数据 0x00, 0x80；
b) 计算报文 MSG 的 32 字节的 HASH 值 h= SM3[Z_A||MSG]；
c) Verify(P_K)[h, S]，若函数输出 True，签名验证正确，若输出 False，签名验证失败。

9.3 公钥鉴别

9.3.1 公钥鉴别要求

公钥鉴别分为卡片鉴别和身份鉴别两类。卡片鉴别是验证教育卡的合法性；身份鉴别是验证教育卡持卡人的合法性。

发卡方生成发卡方SM2密钥对（发卡方公钥P1与发卡行方私钥S1）；教育卡生成SM2密钥对（教育卡公钥Picc与教育卡私钥Sicc）；使用发卡方私钥S1对教育卡公钥Picc进行签名生成人员签名证书并存储在教育卡。

在教育卡使用过程中，使用发卡方公钥P1验证人员签名证书，实现卡片鉴别和身份鉴别。

9.3.2 公私钥对

9.3.2.1 发卡方公私钥对

发卡方公私钥对在生成后，将分配一个唯一的发卡方公钥索引。发卡方公钥及其索引存储在教育卡终端设备中。发卡方私钥由发卡方保管并保证其安全性。

终端设备应有足够空间存储发卡方公钥，以及该公钥所对应的注册应用提供商标识和发卡方公钥索引。

终端设备通过注册应用提供商标识和发卡方公钥索引定位发卡方公钥。

9.3.2.2 教育卡公私钥对

教育卡公私钥对由发卡方分配，或者由教育卡生成。教育卡签名私钥存储在教育卡的安全存贮区域，教育卡签名公钥使用发卡方私钥签名，产生的人员签名证书存储在卡片中。

在应用过程中，应通过注册应用标识和发卡方公钥索引定位发卡方公钥，并用发卡方公钥验证人员签名证书。人员签名公钥验证卡片的数字签名数据。验证数字签名数据时，应根据人员签名证书的“发卡方公钥签名算法标识”检查算法类型。

9.3.3 公钥鉴别数据

9.3.3.1 公钥鉴别处理使用的数据

公钥鉴别处理使用如下数据：

a) 发卡方公钥索引：指明应使用与该索引对应的发卡方公钥进行公钥鉴别处理；
b) 人员签名证书：由发卡方签发，并存储在教育卡中；
c) 教育卡签名私钥：存储在教育卡内。

9.3.3.2 教育卡应生成的数据

支持公钥鉴别的教育卡应生成下列数据：

a) 签名的动态应用数据：使用教育卡签名私钥对动态应用数据进行签名生成；
b) 每台终端应至少存储 2 个以上的发卡方公钥，并需确保与密钥相关的密钥信息能够和每一个密

钥相互关联。

9.3.4 密钥和证书

教育卡内存储有签名密钥对。签名私钥存储在专有的密钥文件中，签名公钥存储在人员签名证书中。

人员签名证书由发卡方私钥对表43中指定的数据计算生成。

为了完成公钥鉴别，应首先验证人员签名证书。表43详细说明了验证人员签名证书所需要的信息。RID可以从AID中获得，其他信息可以通过READ RECORD命令或READ BINARY命令获得。若缺少任意一项数据，将导致公钥鉴别失败。

表43 由发卡方签名的人员签名公钥数据（待签名数据）

字段名	长度（字节）	描述	格式
证书格式	1	值为‘14’	b
应用主账号	10	主账号（在右边补上十六进制数‘F’）	cn 20
证书失效日期	2	MMYY，在此日期后，这张证书无效	n4
证书序列号	4	由发卡方分配给这张证书的唯一的二进制数	b
签名算法标识	1	标识人员签名证书对应的数字签名算法	b
加密算法标识	1	标识人员签名证书对应的加密算法，保留项。	b
签名公钥参数标识	1	用于标识椭圆曲线参数，同时确定 N_{IC}。见附录 G.4	b
签名公钥长度	1	标识人员签名公钥的字节长度	b
签名公钥	N_{IC}	签名算法标识对应于 SM2，该信息项代表椭圆曲线上的一个点	b

公钥鉴别中的公钥认证所需的数据对象见表44。

表44 公钥鉴别中的公钥认证所需的数据对象

标签	长度（字节）	值	格式
-	5	注册的应用提供商标识	b
8F	1	发卡方公钥索引	b
3FA5	$N_I+N_{IC}+20$	人员签名证书，格式见表 45	b

9.3.5 发卡方公钥的获取

终端使用发卡方公钥索引和应用提供商标识，能取得存储在终端的发卡方公钥相关信息。

9.3.6 人员签名证书格式及验证

人员签名证书格式如表45所示。

表45 发卡方使用 SM2 签名的人员签名证书的格式

字段名	长度（字节）	描述	格式
证书格式	1	十六进制，值为‘14’	b
应用主账号	10	主账号	cn 20
教育卡关键信息 Hash 值	32	关键信息见表 46	b
证书失效日期	2	MMYY，在此日期后，这张证书无效	n4

证书序列号	4	由发卡方分配给这张证书的唯一的二进制数	b
签名算法标识	1	标识人员签名公钥对应的数字签名算法	b
加密算法标识	1	标识人员签名公钥对应的加密算法，保留项	b

表45 （续）

字段名	长度（字节）	描述	格式
签名公钥参数标识	1	用于标识椭圆曲线参数，同时确定 N_{IC}	b
签名公钥长度	1	标识人员签名公钥的字节长度	b
签名公钥	N_{IC}	若签名算法标识对应于 SM2，该字段是椭圆曲线上的一个点	b
数字签名	N_I	发卡方对表 43 数据计算的 SM2 签名 r||s	b

人员签名证书验证的步骤如下：

步骤1：获取并解析如表45所示的人员签名证书数据；若失败，则签名证书验证失败；

步骤2：检查证书格式。若它不是“14”，那么签名证书验证失败；

步骤3：比较证书中的应用主账号和从教育卡读出的应用主账号是否相同。若不同，那么签名证书验证失败；

步骤4:检验证书失效日期表明的日期是否等于或迟于当前日期。若证书失效日期在当前日期之前，那么证书已过期，签名证书验证失败；

步骤5：准备表45中的前9个数据元。检查发卡方（签名）公钥算法标识是否为“04”（SM2算法）。若不是，那么签名证书验证失败；

步骤6：验证教育卡关键信息Hash值是否正确（Hash值格式见表46）；

步骤7：使用发卡方公钥和相应的发卡方签名算法使用（见9.2.2.3）中指明的验证函数对表45中准备的数据元数字签名进行验证。若验证签名失败，那么签名证书验证失败；

步骤8：若以上所有的检验都通过，继续按下面章节的描述执行实际的公钥鉴别。

表46 教育卡关键信息 Hash 值明文格式

字段名	长度（字节）	描述	格式
发卡机构代码	5	十六进制	b
卡类型标识	1	‘1’：学生卡；‘2’：教师卡；‘3’：毕业生卡；‘4’：电子毕业证；‘5’：电子结业证；‘6’：电子学位证；；‘7’：电子校徽；‘9’：其他	cn 2
教育电子身份号	10	十六进制	b
学籍号	19	学籍的数字标识	cn 38

9.3.7 公钥鉴别过程

9.3.7.1 数字签名的生成

数字签名生成的步骤如下：

步骤1：终端发出PERSONAL AUTHENTICATE命令或CARD AUTHENTICATE命令，命令中包含由动态数据对象列表指定的数据元；

步骤2：教育卡使用教育卡签名私钥对表47中指明的数据计算签名，得到签名动态应用数据。

表47 公钥鉴别需签名的动态应用数据（待签名数据）

字段名	长度（字节）	描述	格式
签名的数据格式	1	值为‘15’，表示用 SM2 签名	b

表47 （续）

字段名	长度（字节）	描述	格式
数字签名数据长度	1	标识教育卡动态数据的字节长度 L_{DD}，包括教育卡动态数据与终端动态数据	b
教育卡动态数据	L_{DD}	由教育卡生成和/或存储在教育卡上的签名数据	-
终端动态数据	8	由动态数据对象列表指定的数据元连接而成	-

教育卡数字签名由教育卡生成的4字节随机数、ESN或教育卡卡片序列号组成。

除了表47和表48中指明的数据，公钥鉴别所需的数据对象在表44中说明。

表48 生成和检验数字签名所需要的其他数据对象

标签	长度（字节）	值	格式
3FA9	$N_{IC}+L_{DD}+2$	SM2 签名动态应用数据，格式见表 49 与表 50	b
3FA2	变长	动态数据对象列表指定的数据元	b

9.3.7.2 数字签名的验证

终端获取的签名动态应用数据的格式如表49和表50所示,包括明文数据及数字签名。终端使用教育卡的公钥验证动态应用数据的签名。若数字签名验证成功,表51中的教育卡动态数据中所包含的教育卡动态数字应被存储在标签“9F4C”中。

表49 教育卡使用 SM2 签名的身份鉴别动态应用数据的格式

字段名	长度（字节）	描述	格式
签名的数据格式	1	十六进制，值为‘15’	b
教育卡返回的动态数据长度	1	标识教育卡返回的动态数据的字节长度 L_{DD}	b
教育卡返回的动态数据	L_{DD}	由教育卡生成和/或存储在教育卡上的动态数据，具体见表 51	-
数字签名	N_{IC}	教育卡对表 51 中数据计算的 SM2 签名 r||s	b

表50 教育卡使用 SM2 签名的卡片鉴别签名应用数据的格式

字段名	长度（字节）	描述	格式
签名的数据格式	1	十六进制，值为‘16’	b
教育卡返回的签名数据长度	1	标识教育卡返回的动态数据的字节长度 L_{DD}	b
教育卡返回的签名数据	L_{DD}	由教育卡生成和/或存储在教育卡上的动态数据，具体见表 51	-
数字签名	N_{IC}	教育卡对表 51 中数据计算的 SM2 签名 r||s	b

数字签名验证步骤如下：

步骤1：获取签名动态应用数据，并进行解析；

步骤2：检查“签名的数据格式”信息。对于身份鉴别，若不是“15”，身份鉴别失败；对于卡片鉴别，若不是“16”，卡片鉴别失败；

步骤3：准备表49或表50中的相关数据元（即从签名数据格式直到教育卡动态数据）及动态数据对象列表中指定的数据元（即表51数据用于验证签名）；

步骤4：使用人员签名公钥对表49或表50的数字签名进行验证。若签名验证失败，公钥鉴别失败；

步骤5：若以上所有的步骤成功，公钥鉴别成功。终端获取表51中教育卡动态数据所包含的教育卡动态数字后，将其存储在标签“9F4C”中。

表51　教育卡返回的签名数据的内容

长度（字节）	值	格式
4	卡片随机数	b
32	应用数据哈希值	b

身份鉴别的应用数据哈希值由ZA、教育卡签名数据长度、卡片伪随机数、ESN、动态数据对象列表组成。

卡片鉴别的应用数据哈希值由ZA、教育卡签名数据长度、卡片伪随机数、教育卡卡片序列号、动态数据对象列表组成。

ESN和教育卡卡片序列号可以通过命令方式从卡片获取。

9.4　安全报文

9.4.1　安全报文要求

安全报文分为MAC安全报文、加密安全报文两种。MAC安全报文是在报文后附上4字节MAC；加密报文是将报文加密后，在密文后附上4字节的密文MAC。

9.4.2　MAC 安全报文

9.4.2.1　MAC 过程密钥生成

MAC过程密钥的生成步骤如下：

步骤1：通过取随机数命令获取8字节随机数；

步骤2：使用附录D.4规定的过程密钥计算方法，生成MAC过程密钥。

9.4.2.2　MAC 的计算

MAC是通过使用MAC过程密钥，对所要保护的报文进行计算得到，计算方法见附录D。

要保护的报文应按照教育卡应用系统的专有规范来构建。

9.4.3　加密安全报文

9.4.3.1　数据加密密钥的生成

数据加密密钥是按9.2.1.2规定的计算方法生成。

9.4.3.2　数据加密计算

在报文数据前添加1字节的报文长度数据作为待加密的数据。将待加密数据按9.2.1.1进行填充、分块，加密生成密文。

9.4.3.3 密文 MAC 的计算

按9.4.2的要求，生成密文MAC。

9.5 卡片安全

9.5.1 卡片安全要求

卡片安全要求如下：

a) 教育卡的每一个应用均应放在一个单独的 ADF 中；
b) 用于一种特定功能的加密/解密密钥不能被任何其他功能所使用，包括保存在教育卡中的密钥和用来产生、派生、传输这些密钥的密钥；
c) 教育卡 COS 使用合适的安全机制，在卡片内部为访问数据文件、命令执行等提供安全性保障。

9.5.2 安全域

COS建立安全域，以控制对所有数据和可执行资源（即数据文件、记录、命令和加密密钥与算法）的访问。

建立安全域是通过执行SELECT命令实现。SELECT命令用于建立描述安全域的相关信息，并且定义了指定数据和可执行资源可以被访问的范围。

处理SELECT命令使得应用管理数据可以被访问。应用管理数据指定了能够被后续指令访问的所有数据文件，记录以及可执行资源。

应用管理数据决定了应用可以访问的文件和可执行资源。文件和记录编号则由该命令在应用文件定位器中提供。

使用SELECT命令建立安全域，发卡方可以限制在卡应用期间被存取的资源，包括决定该资源是被包含在应用管理数据和应用文件定位之内还是被排除在外。

a) 不被应用管理数据和应用文件定位引用的数据文件不能够被访问；
b) 不被应用管理数据和应用文件定位引用的命令或者加密算法，不能够在当前安全域内被使用。

应用管理数据的初始化状态仅包含了处理该应用交易的过程中可以被访问的那些数据文件。初始的应用管理数据在选择应用时建立，并且在个人化时被定义。

9.5.3 EF 访问条件

对于EF的访问，其前提条件是至少执行一次SELECT命令并且安全域已经建立。

一旦安全域建立，并且后续读取数据（如：READ RECORD命令）或者更新数据（如：UPDATE RECORD命令）命令被发送到一个EF的时候，EF的访问控制（由文件控制信息的文件控制参数定义）被强制使用。

使用安全通信或VERIFY命令（或者包含二者）作为访问条件的文件，只有在访问条件都满足以后被请求的访问才能继续执行。

EF的访问条件应用于所有命令。

9.5.4 文件控制信息的安全

9.5.4.1 文件控制信息的构成

FCI在教育卡个人化期间建立。FCI包含了文件管理数据。文件管理数据可能包含应用管理数据。

9.5.4.2 应用管理数据

应用管理数据在教育卡个人化期间建立。应用管理数据保存在应用定义文件的文件管理数据中。

应用管理数据描述的安全域定义以下内容：

a) 在应用范围内可以被存取的资源，AEF 和内部基本文件（例如，个人识别码 PIN、密钥、参数）；

b) 可在应用的上下文范围内被执行的命令；

c) 命令与资源之间的关系。

安全域由应用管理数据说明的相关资源定义。没有被包含在应用管理数据内的资源不能被应用使用。

教育卡有以下两类资源被定义：

a) 数据资源；

b) 可执行代码资源。

9.5.4.3 数据资源

9.5.4.3.1 数据标识

数据资源是指存储在文件内的数据元。数据资源由教育卡内部的唯一标识符所识别。文件由教育卡内部唯一的文件标识符所标识。不包含在文件内的数据元则由一个唯一数据标识所标识。运行应用所需的任何数据资源应在应用管理数据内标识。

对于包含了数据元的文件，SFI与文件标识之间的关系被存储在应用管理数据内进行维护。

对于未被包含在文件内的数据对象，数据对象标签与唯一数据标识之间的关系被存储在应用管理数据内进行维护。

9.5.4.3.2 密钥标识

密钥不能从外部被引用。对保存在文件内的密钥，应用管理数据维护有在执行应用管理数据定义的命令，或执行加密算法时定位密钥所对应的文件标识和指向密钥的引用。

对未保存在文件内的密钥，应用管理数据维护有在执行应用管理数据定义的命令，或执行加密算法时定位密钥所对应的教育卡内部的唯一密钥标识。

9.5.4.3.3 PIN/口令标识

PIN和口令只能通过应用管理数据和安全通信共同定义的命令被引用。

对于保存在文件内的PIN或口令，应用管理数据维护了在执行应用管理数据定义的命令，或加密算法时定位PIN/口令所应的文件标识和指向PIN/口令的引用。

对于未保存在文件内的PIN/口令，应用管理数据维护了在执行应用管理数据定义的命令，或加密算法时定位PIN/口令所应的教育卡内部的唯一PIN/口令标识。

9.5.4.4 可执行代码资源

9.5.4.4.1 命令标识

命令资源的内容包括CLA和INS字节，COS用他们来查找命令的位置。

9.5.4.4.2 算法标识

算法资源建立了为应用而定义的算法标识，用来定位可执行代码的实际算法。

9.6 密钥管理

9.6.1 非对称密钥管理

9.6.1.1 发卡方公私钥对

发卡方公私钥对的管理要求如下：

a) 公私钥对采用国家密码主管部门批准使用的密码设备产生；
b) 私钥存储在密码设备中，不允许明文导出；
c) 公钥导出后，由国家密码主管部门管理的国家根证书签发生成发卡方证书，对外发布；
d) 发卡方私钥用于生成人员签名证书，发卡方公钥用于验证人员签名证书。

9.6.1.2 教育卡公私钥对

教育卡公私钥对的管理要求如下：

a) 公私钥对在教育卡内产生，或采用国家密码主管部门批准使用的密码设备产生；
b) 私钥存储在教育卡中，不允许明文导出；
c) 公钥导出后，由发卡方私钥签发生成人员签名证书，对外发布；
d) 教育卡私钥用于生成签名动态应用数据，教育卡公钥用于签名动态应用数据的验证。

9.6.2 对称密钥管理

9.6.2.1 发卡方对称密钥

9.6.2.1.1 对称密钥种类

对称密钥种类见表52。

表52 对称密钥的种类

密钥类型	用途	长度（字节）
应用密文主密钥	产生教育卡应用密文子密钥，用于应用密文的产生和验证	16
安全报文认证主密钥	产生教育卡MAC子密钥，用于安全报文鉴别码的产生和验证	16
联机支出（OPK）主密钥	产生教育卡联机支出子密钥，用于联机支出密文计算	16
联机导入(OLK)主密钥	产生教育卡联机导入子密钥，用于联机导入密文的计算	16
PIN解锁主密钥	产生教育卡PIN解锁子密钥，用于脱机PIN解锁	16
应用锁定主密钥	产生教育卡应用锁定子密钥，用于应用锁定	16
应用解锁主密钥	产生教育卡应用解锁子密钥，用于应用解锁	16
文件读外部认证主密钥	控制文件读鉴别的外部认证密钥	16
文件写外部认证主密钥	控制文件写鉴别的外部认证密钥	16

9.6.2.1.2 密钥管理

在发卡方对称密钥的生命周期内，应按以下要求进行管理：

a) 密钥生成，应使用国家密码主管部门批准的密码设备生成各类密钥；
b) 密钥存储，应安全存储在密码设备中；
c) 密钥分发，应安全地将密钥分发到终端设备、发卡密码设备或下级密钥管理系统；
d) 密钥备份，对系统中使用的密钥应提供备份机制。备份数据应加密存储；
e) 密钥销毁，应按国家密码主管部门的要求，对系统中不再使用的密钥进行销毁；
f) 密钥审计，应定期对密钥的生成、分发、销毁等操作进行审计。

9.6.2.2 教育卡对称密钥

9.6.2.2.1 对称密钥种类

教育卡内存储的对称密钥种类见表53。

表53 教育卡存储的对称密钥种类

密钥类型	用途	长度（字节）
应用密文密钥	用于应用密文的产生和验证	16
安全报文认证密钥	用于安全报文鉴别码的产生和验证	16
联机支出（OPK）密钥	用于联机支出密文计算	16
联机导入(OLK)密钥	用于联机导入密文的计算	16
PIN解锁密钥	用于脱机PIN解锁	16
应用锁定密钥	用于应用锁定	16
应用解锁密钥	用于应用解锁	16
文件读外部认证密钥	控制文件读鉴别的外部认证密钥	16
文件写外部认证密钥	控制文件写鉴别的外部认证密钥	16

9.6.2.2.2 密钥管理

在教育卡对称密钥的生命周期内，应按以下要求进行管理：

a) 密钥生成，由发卡方主密钥分散生成；

b) 密钥存储，应安全存储在教育卡内，不允许明文导出。

9.7 密码算法

9.7.1 对称密码算法

教育卡使用的对称密码算法为SM4算法。算法规范见GM/T 0002-2012。

9.7.2 非对称密码算法

教育卡使用的非对称密码算法为SM2算法。算法规范见GM/T 0003-2012，GM/T 0009-2012。

9.7.3 哈希算法

教育卡使用的哈希算法为SM3算法。算法规范见GM/T 0004-2012。

10 教育卡应用接口

教育卡应用接口包含C/S和B/S两类应用接口，应用接口函数规范见附录H、附录I。

附 录 A
（规范性附录）
教育应用文件定义

A.1 教育应用文件的AID和FID信息

教育应用文件结构中的DDF和ADF对应的AID、FID的信息定义见表A.1

表A.1 AID 和 FID 信息

序号	应用	AID	FID
1	教育卡 DDF	D156000044000000	3F00
2	公共应用（ADF00）	B9ABB9B2D3A6D3C3	ADF0
3	法定身份证件网上应用（ADF01）	B7A8B6A8C9EDB7DDD6A4BCFED3A6D3C3	ADF1
4	学校应用（ADF02）	D1A7D0A3D3A6D3C3	ADF2
5	机构应用（ADF03）	BBFAB9B9D3A6D3C3	ADF3
6	PKI 应用（ADF04）	504B49D3A6D3C3	ADF4
7	教育管理应用（ADF05）	BDCCD3FDB9DCC0EDD3A6D3C3	ADF5
8	行业扩展应用（ADF06）	C0A9D5B9D3A6D3C3	ADF6
9	教育电子证件应用（ADF08）	D0BEC6ACB9DCC0EDD3A6D3C3	ADF8
10	芯片管理应用（ADF09）	B5E7D7D3CEC4C6BED3A6D3C3	ADF9
11	省级教育管理应用（ADF10）	CAA1BCB6BDCCD3FDB9DCC0EDD3A6D3C3	ADFA
12	市级教育管理应用（ADF11）	CAD0BCB6BDCCD3FDB9DCC0EDD3A6D3C3	ADFB
13	卡发行单位教育管理应用（ADF12）	BFA8B7A2D0D0B5A5CEBBD3A6D3C3	ADFC
14	卡应用单位教育管理应用（ADF13）	BFA8D3A6D3C3B5A5CEBBD3A6D3C3	ADFD

A.2 公共应用文件

A.2.1 教育卡发行信息文件

教育卡发行信息文件包含发卡方代码、应用类型标识、应用版本等信息，信息定义见表A.2。

表A.2　教育卡发行信息文件

文件路径		ADF0/EF01
文件类型		二进制文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F01	5	发卡方代码
3F02	5	应用类型标识
3FB2	1	应用版本
3F03	1	卡类型标识
5A	10	应用序列号（卡号）
3FB3	4	应用启用日期
3FB4	4	应用有效日期
BF0C	2	发卡方自定义 FCI 数据

A.2.2　个人基本信息文件

个人基本信息文件包含持卡人姓名、身份证件类型与号码、教育电子身份号等信息，信息定义见表A.3。

表A.3　个人基本信息文件

文件路径		ADF0/EF02
文件类型		二进制文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3FB7	var.最大 60	姓名
3F04	var.最大 60	姓名拼音
3FB5	1	身份证件类型
3FB6	20	身份证件号码
3F05	19	学籍号
3F06	10	教育电子身份号
3F07	4	出生日期
3F08	1	性别码
3F09	2	民族码
3F10	3	籍贯码

表A.3 （续）

标签	长度（字节）	数据项
3F11	3	国别码
3F12	2	港澳台侨外码
3F13	2	户口性质

A.2.3 照片信息文件

照片信息文件存放持卡人的照片信息，信息定义见表A.4。

表A.4 照片信息文件

文件路径		ADF0/EF03
文件类型		二进制文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F14	2	照片数据长度
3F15	var.最大 4096	照片数据

A.2.4 生物特征信息文件

生物特征信息文件存放持卡人的生物特征识别信息，信息定义见表A.5。

表A.5 持卡人生物特征信息文件

文件路径		ADF0/EF03
文件类型		二进制文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F16	1	生物特征码
3F17	1	算法标识
3F18	1	生物特征编号
3F19	2	生物信息长度
3F20	var.最大 1024	生物信息值

A.3 法定身份证件网上应用文件

A.3.1 居民身份认证网上副本文件

居民身份证网上副本文件存储持卡人的居民身份证网上副本信息，信息定义见表A.6。

表A.6　居民身份证网上副本文件

文件路径		ADF1/EF01
文件类型		二进制文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3FB8	300	居民身份认证网上副本信息

A.4　学校应用文件

A.4.1　工作信息文件

工作信息文件包含持卡人的工作单位名称、职工号、职务类别等信息，信息定义见表A.7。

表A.7　工作信息文件

文件路径		ADF2/EF01
文件类型		二进制文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F21	1	教职员工类别代码
3F22	12	职工号
3F23	10	学校编码
3F24	var.最大 60	学校名称
3F25	var.最大 30	二级机构名称
3F26	var.最大 20	三级机构名称
3F27	2	文化程度码
3F28	2	编制类别码
3F29	4	现从事专业号
3F30	1	现职务类别码
3F31	3	现任职资格名称码
3F32	3	从教年月
3F33	3	最高学位码

A.4.2　学籍信息文件

学籍信息文件包含持卡人的所在学校名称、专业、学制等学籍信息，信息定义见表A.8。

表A.8　学籍信息文件

文件路径		ADF2/EF02
文件类型		二进制文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F34	9	组织机构代码
3F23	10	单位/学校代码
3F24	var.最大 60	单位/学校全名
3F25	var.最大 30	二级机构名
3F26	var.最大 20	三级机构名
3F35	var.最大 30	专业/学科名
3F36	4	年级
3F37	4	班号
3F38	10	学号
3F39	2	培养方式码
3F40	1	学制
3F41	3	入学年月
3F42	2	入学方式
3F43	1	学生当前状态

A.4.3　学籍注册信息文件

学籍注册信息文件包含持卡人的注册状态、注册日期等信息，信息定义见表A.9。

表A.9　学籍注册信息文件

文件路径		ADF2/EF03
文件类型		循环记录文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F44	1	注册状态码
3F45	3	注册学期
3F46	4	注册有效期
3F47	4	注册日期

A.4.4　体质健康信息文件

体质健康信息文件存储持卡人的体质健康信息，信息定义见表A.10。

表A.10　体质健康信息文件

文件路径		ADF2/EF04
文件类型		二进制文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F61	var.最大 20	指标名称
3F62	4	指标数据
3F63	4	检测时间

A.4.5　学生助学贷款信息文件

学生助学贷款信息文件存储学生的助学贷款与还款信息，信息定义见表A.11。

表A.11　学生助学贷款信息文件

文件路径		ADF2/EF05
文件类型		循环记录文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F64	1	贷款类别
3F65	4	贷款总金额
3F66	4	贷款期限
3F67	2	申请贷款起始年度
3F68	2	申请贷款截止年度
3F69	var.最大 60	贷款银行名称
3F70	4	贷款合同日期
3F71	20	贷款合同编号
3F72	4	还款截止日期
3F73	1	还款计划
3F74	4	还款总金额

A.4.6　营养餐资格信息文件

营养餐资格信息文件包括营养餐资格标识、开始日期、结束日期等信息，信息定义见表A.12。

表A.12　营养餐资格信息文件

文件路径		ADF2/EF06
文件类型		二进制文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F75	1	资格标志
3F48	4	开始日期
3F49	4	结束日期
3F76	2	总次数
3F77	4	餐类模式

A.4.7　营养餐领餐信息文件

营养餐领餐信息文件存储最近的22条领用营养餐的流水记录信息，信息定义见表A.13。

表A.13　营养餐领餐信息文件

文件路径		ADF2/EF07
文件类型		循环记录文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F78	2	用餐流水号
3F79	7	最后领用时间

A.5　机构应用文件

A.5.1　毕业/结业证书信息文件

毕业/结业证书信息文件包含证书名称、证书编号、专业、学制等信息，信息定义见表A.14。

表A.14　毕业/结业证书信息文件

文件路径		ADF3/EF01
文件类型		循环记录文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F51	var.最大 30	证书名称
3F52	8	证书类别
3F48	8	学习起始日期

表A.14 （续）

标签	长度（字节）	数据项
3F49	8	学习截止日期
3F35	var.最大30	专业名称
3F40	1	学制
3F53	18	证书编号
3F54	4	证书颁发日期
3F55	var.最大60	发证机构

A.5.2 学位证书信息文件

学位证书信息文件包含证书名称、证书编号、学位名称、专业名称等信息，信息定义见表A.15。

表A.15 学位证书信息文件

文件路径		ADF3/EF02
文件类型		循环记录文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F51	var.最大30	证书名称
3F56	var.最大30	学位名称
3F35	var.最大30	专业名称
3F53	18	证书编号
3F54	4	证书颁发日期
3F55	var.最大60	发证机构

A.5.3 资格水平信息文件

资格水平信息文件包含证书名称、证书编号、专业/资格名称、专业水平等国家认可的专业资格信息和岗位证书信息，信息定义见表A.16。

表A.16 资格水平信息文件

文件路径		ADF3/EF03
文件类型		循环记录文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F51	var.最大30	证书名称

表A.16 （续）

标签	长度（字节）	数据项
3F53	18	证书编号
3F35	var.最大 30	学科/专业名称
3F57	var.最大 20	级别/成绩
3F54	4	证书颁发日期
3F55	var.最大 60	发证机构
3F58	17	证书有效期
3F47	4	注册日期
3F59	var.最大 40	注册机构

A.5.4 考务基本信息文件

考务基本信息文件包含准考证号、考场地址等信息，信息定义见表A.17。

表A.17 考务基本信息文件

文件路径		ADF3/EF04
文件类型		循环记录文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F81	18	准考证号
3F82	12	考区
3F83	12	考点
3F84	12	考场
3F85	8	考室
3F86	3	座位
3F87	1	身份认证方式
3F48	4	开始日期
3F49	4	结束日期
3F88	var.最大 60	考试组织机构
3F80	var.最大 60	考试名称

A.5.5 学生首次就业信息文件

学生首次就业信息文件包含首次就业日期、就业单位名称等信息，信息定义见表A.87。

表A.18　学生首次就业信息文件

文件路径		ADF3/EF05
文件类型		二进制文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F89	13	报到证编号
3F8A	4	首次就业日期
3F8B	var.最大60	就业单位名称

A.5.6　教育经历信息文件

教育经历信息文件包含学校名称、开始日期、结束日期、学历代码等信息，信息定义见表A.19。

表A.19　教育经历信息文件

文件路径		ADF3/EF06
文件类型		循环记录文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F48	8	开始日期
3F49	8	结束日期
3F24	var.最大60	学校名称
3F35	var.最大30	专业名称
3F50	2	学历代码

A.6　PKI应用文件

A.6.1　教育卡发卡中心证书文件

教育卡发卡中心证书文件存储教育卡发卡中心的签名证书，信息定义见表A.20。

表A.20　教育卡发卡中心证书文件

文件路径		ADF4/EF01
文件类型		二进制文件
文件写控制		保护
文件读控制		自由
标签	长度（字节）	数据项
3FA5	N_{CA}	教育卡发卡中心的签名证书

A.6.2 人员签名证书文件

人员签名证书文件存储持卡人的人员签名证书，信息定义见表A.21。

表A.21 人员签名证书文件

文件路径		ADF4/EF04
文件类型		二进制文件
文件写控制		保护
文件读控制		自由
标签	长度（字节）	数据项
3FA8	N_{CA}	人员签名证书

A.6.3 签名密钥文件

签名密钥文件存储人员签名证书所对应的签名私钥，信息定义见表A.22。

表A.22 签名密钥文件

文件路径		ADF4/EF2
文件类型		私钥文件
文件写控制		保护
文件读控制		禁止
标签	长度（字节）	数据元
3FA6	N_{IC}	签名私钥

A.6.4 人员加密证书文件

人员加密证书文件存储持卡人的人员加密证书，信息定义见表A.23。

表A.23 人员加密证书文件

文件路径		ADF4/EF05
文件类型		二进制文件
文件写控制		保护
文件读控制		自由
标签	长度（字节）	数据项
3FA9	N_{CA}	人员加密证书

A.6.5 加密密钥文件

加密密钥文件存储人员加密证书所对应的加密私钥，信息定义见表A.24。

表A.24 加密密钥文件

文件路径	ADF4/EF03
文件类型	私钥文件

表 A.24 （续）

文件路径		ADF4/EF03
文件写控制		保护
文件读控制		禁止
标签	长度（字节）	数据项
3FA7	N_{IC}	加密私钥

A.7 行业扩展应用文件

A.7.1 交通票务优惠信息文件

交通票务优惠信息文件存储学生搭乘交通工具（火车、汽车、飞机等）的票务优惠信息，信息定义见表A.25。

表A.25 交通票务优惠信息文件

文件路径		ADF6/EF01
文件类型		循环记录文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F91	1	交通工具类型
3F92	12	起点
3F93	12	终点
3F48	4	开始日期
3F49	4	结束日期

A.7.2 交通票务使用信息文件

交通票务使用信息文件记录学生优惠购买交通票的信息，见表A.26。

表A.26 交通票务使用信息文件

文件路径		ADF6/EF02
文件类型		循环记录文件
文件写控制		保护
文件读控制		认证
标签	长度（字节）	数据项
3F94	4	最近使用日期
3F95	1	最近使用交通工具类型
3F96	1	总使用次数

A.8 教育电子证件应用文件

A.8.1 电子毕业/结业证信息文件

电子毕业/结业证信息文件存储电子毕业/结业证的格式化信息，信息定义见表A.27。

表A.27 电子毕业/结业证信息文件

文件路径		ADF8/EF01
文件类型		二进制文件
文件写控制		不可改写
文件读控制		认证
标签	长度（字节）	数据项
3FC0	2048	毕业/结业证书信息

A.8.2 电子学位证信息文件

电子学位证信息文件存储电子学位证的格式化信息，信息定义见表A.28。

表A.28 电子学位证信息文件

文件路径		ADF8/EF02
文件类型		二进制文件
文件写控制		不可改写
文件读控制		认证
标签	长度（字节）	数据项
3FC1	2048	学位证书信息

A.8.3 电子毕业/结业证版式文件

电子毕业/结业证版式文件存储电子毕业/结业证对应的版式文件信息，信息定义见表A.29。

表A.29 电子毕业/结业证版式文件

文件路径		ADF8/EF03
文件类型		二进制文件
文件写控制		不可改写
文件读控制		认证
标签	长度（字节）	数据项
3FC2	N_{PDF}	毕业/结业证书的版式文件

A.8.4 电子学位证版式文件

电子学位证版式文件存储电子学位证对应的版式文件信息，信息定义见表A.30。

表A.30　电子学位证版式文件

文件路径		ADF8/EF04
文件类型		二进制文件
文件写控制		不可改写
文件读控制		认证
标签	长度（字节）	数据项
3FC3	N_{PDF}	学位证书的版式文件

A.9　芯片管理应用文件

A.9.1　芯片验证身份认证码密钥文件

芯片验证身份认证码密钥文件存储芯片验证身份认证码证书文件对应的签名私钥，信息定义见表A.31。

表A.31　芯片验证身份认证码密钥文件

文件路径		ADF9/EF01
文件类型		私钥文件
文件写控制		保护
文件读控制		禁止
标签	长度（字节）	数据项
3FF1	N_{IC}	签名私钥

A.9.2　芯片验证身份认证码证书文件

芯片验证身份认证码证书文件存储用于识别芯片合法性的签名证书，见表A.32。

表A.32　芯片验证身份认证码证书文件

文件路径		ADF9/EF02
文件类型		二进制文件
文件写控制		保护
文件读控制		自由
标签	长度（字节）	数据项
3FF2	N_{CA}	签名证书

附 录 B
（规范性附录）
教育卡存储的数据元

B.1 数据元格式定义说明

数据元格式定义包括标签（T）、格式（F）和长度（L），定义说明如下：

a) 标签（T）定义了数据元的唯一标识，长度为 2 个字节。

b) 格式（F）定义了数据元的数据类型，支持的类型如下：

—— n（数字型）；

—— cn（压缩数字型）；

—— b（二进制）；

—— an（字母数字）；

—— ans（特殊字母数字）。

c) 长度（L）定义了数据元的最大字节数。当数据元定义的长度超过数据实际长度时，填充规则如下：

—— 格式 n 的数据元右对齐，左补 0；

—— 格式 cn 的数据元左对齐，右补 F；

—— 格式 an 的数据元左对齐，右补 0；

—— 格式 ans 的数据元左对齐，右补 0。

数据元采用采用大端模式进行传输。

B.2 数据元定义

教育卡存储的数据元定义见表B.1。

表B.1 教育卡数据元定义

数据元名称	数据元定义	数据元描述
发卡方代码	T：3F01 F：cn L：5	由教育卡服务中心定义
应用类型标识	T：3F03 F：b L：1	由国家 IC 卡注册中心赋予
卡类型标识	T：3F03 F：b L：1	由教育卡发卡方定义 1：学生卡；2 教师卡：3：毕业生卡；4：电子毕业证；5：电子结业证；6：电子学位证；7：电子校徽；9：其他
持卡人姓名拼音	T：3F04 F：an L：var.最大 60	姓名全称的汉语拼音

表B.1 （续）

数据元名称	数据元定义	数据元描述
学籍号	T：3F05 F：an L：19	国家教育主管部门统一编制
教育电子身份号	T：3F06 F：an L：10	国家教育主管部门统一生成
出生日期	T：3F07 F：cn L：4	
性别码	T：3F08 F：b L：1	见 JY/T 1001—2012
民族码	T：3F09 F：b L：2	见 JY/T 1002—2012
籍贯码	T：3F10 F：cn L：3	见 GB/T2260-2007
国别码	T：3F11 F：an L：3	见 JY/T 1002—2012
港澳台侨外码	T：3F12 F：an L：2	见 JY/T 1001—2012
户口性质	T：3F13 F：an L：2	见 JY/T 1001—2012
照片数据长度	T：3F14 F：b L：2	照片数据实际长度，长度为 0 表示未提供照片
照片数据	T：3F15 F：b L：var.最大 4096	照片采用 JPG 格式 照片分辨率：358×441 像素
生物特征码	T：3F16 F：b L：1	0：指纹；1：虹膜；2：面相；3：掌纹；9：其他
算法标识	T：3F17 F：b L：1	具体采用的算法编号

表B.1 （续）

数据元名称	数据元定义	数据元描述
生物特征编号	T：3F18 F：b L：1	例如指纹的手指编号
生物特征值长度	T：3F19 F：b L：2	
生物特征值	T：3F20 F：b L：1024	不定长，根据生物特征算法确定特征值
教职员工类别代码	T：3F21 F：an L：1	
职工号	T：3F22 F：an L：12	
学校编号	T：3F23 F：an L：10	国家教育主管部门自定义的学校编码
学校名称	T：3F24 F：an L：var.最大 60	与公章一致的标准名称
二级机构名称	T：3F25 F：an L：var.最大 30	二级机构的名称，如学院名称
三级机构名称	T：3F26 F：an L：var.最大 20	二级机构下属三级机构的名称，如系名称
文化程度码	T：3F27 F：cn L：2	见 JY/T 1001—2012
编制类型码	T：3F28 F：cn L：2	见 JY/T 1001—2012
现从事专业号	T：3F29 F：cn L：4	见 JY/T 1001-2012
职务类别号	T：3F30 F：cn L：1	见 JY/T 1001-2012

表B.1 （续）

数据元名称	数据元定义	数据元描述
现任职资格名称码	T：3F31 F：cn L：3	见 JY/T 1001-2012
从教年月	T：3F32 F：cn L：3	持卡人进入所在机构的时间
最高学位码	T：3F33 F：cn L：3	见 JY/T 1001-2012
组织机构代码	T：3F34 F：an L：9	学校或单位所对应的组织机构代码
专业/学科名称	T：3F35 F：an L：var.最大 30	见 JY/T 1001-2012
年级	T：3F36 F：cn L：4	持卡人所在年级
班号	T：3F37 F：cn L：4	持卡人所属班级
学号	T：3F38 F：an L：10	由学校生成
培养方式法	T：3F39 F：cn L：2	见 JY/T 1001-2012
学制	T：3F40 F：an L：1	单位：年
入学年月	T：3F41 F：cn L：3	格式：CCYYMM
入学方式	T：3F42 F：cn L：2	见 JY/T 1001-2012

表B.1 （续）

数据元名称	数据元定义	数据元描述
注册状态码	T：3F44 F：an L：1	见 JY/T 1001-2012
注册学期	T：3F45 F：cn L：3	年度+学期 年度格式：YYYY 学期： 1 秋季学期；2 春季学期；3 夏季学期
注册有效期	T：3F46 F：cn L：4	格式：YYYYMMDD
注册日期	T：3F47 F：cn L：4	
开始日期	T：3F48 F：cn L：4	攻读本学历/学习/营养餐开始日期
结束日期	T：3F49 F：cn L：4	攻读本学历/学习/营养餐截止日期
学历代码	T：3F50 F：an L：2	见 JY/T 1001-2012
证书名称	T：3F51 F：an L：var.最大 30	与证书名称一致
证书类别	T：3F52 F：an L：8	证书类别名称，如：小学、中学、中专、大专、本科、硕士研究生、博士研究生等
证书编号	T：3F53 F：an L：18	发证机构对证书的统一编号
证书颁发日期	T：3F54 F：cn L：4	以证书签发日期为准，格式：YYYYMMDD

表B.1 （续）

数据元名称	数据元定义	数据元描述
发证机构	T：3F55 F：an L：var.最大 60	与证书当中授予单位名称一致
学位名称	T：3F56 F：an L：var.最大 30	
级别/成绩	T：3F57 F：an L：var.最大 20	资质级别名称或成绩，与证书一致
证书有效期	T：3F58 F：an L：17	格式：YYYYMMDD-YYYYMMDD
注册机构	T：3F59 F：an L：var.最大 40	学校或单位名称
资格种类	T：3F60 F：an L：2	见 JY/T 1003-2012 定义的教师资格种类码
指标名称	T：3F61 F：cn L：var.最大 20	
指标数据	T：3F62 F：cn L：4	
检测日期	T：3F63 F：cn L：4	格式 YYYYMMDD
贷款类别	T：3F64 F：b L：1	1：学费贷款、2：生活贷款、3：二者皆有
贷款总金额	T：3F65 F：b L：4	学生贷款的金额
贷款期限	T：3F66 F：cn L：4	学生还款年限，应在该年限内付清贷款

表B.1 （续）

数据元名称	数据元定义	数据元描述
申请贷款起始年度	T：3F67 F：cn L：2	格式：YYYY
申请贷款截止年度	T：3F68 F：cn L：2	格式：YYYY
贷款银行名称	T：3F69 F：an L：var.最大 60	
贷款合同日期	T：3F70 F：cn L：4	格式：YYYYMMDD
贷款合同编号	T：3F71 F：an L：20	
贷款截止日期	T：3F72 F：cn L：4	格式：YYYYMMDD
还款计划	T：3F73 F：b L：1	0：毕业前一次性归还 1：毕业后一次性归还 2：毕业后逐月归还，分 n 年还清 9：其他（请描述）
还款总金额	T：3F74 F：b L：4	
资格标志	T：3F75 F：cn L：1	0-无资格 1-有资格 2-暂时停止
总次数	T：3F76 F：an L：2	学生可以领取营养餐的总次数
餐类模式	T：3F77 F：an L：4	00000001：早餐 00000010：课间餐 00000100：中餐 00001000：晚餐 00010000：加餐

表B.1 （续）

数据元名称	数据元定义	数据元描述
用餐流水号	T：3F78 F：an L：2	学生当日已领取营养餐的次数
最后领用时间	T：3F79 F：cn L：7	格式：YYYYMMDDHHMMSS
考试名称	T：3F80 F：an L：var.最大 30	普通高校、成人高考、自学、中考等
准考证号	T：3F81 F：cn L：18	最长 16 位数字或字母
考区	T：3F82 F：an L：12	
考点	T：3F83 F：an L：12	
考场	T：3F84 F：an L：12	
考室	T：3F86 F：an L：8	
座位：	T：3F86 F：an L：3	
身份认证方式	T：3F87 F：b L：1	0：教育卡，1：身份证，2：生物特征，3：身份证+生物特征，4：照片，9：其他
考试组织机构	T：3F88 F：cn L：var.最大 30	
报到证编号	T：3F89 F：an L：13	

表B.1 （续）

数据元名称	数据元定义	数据元描述
首次就业日期	T：3F8A F：cn L：4	格式：YYYYMMDD
就业单位名称	T：3F8B F：an L：var.最大 60	
交通工具类型	T：3F91 F：b L：1	0：火车；1：汽车；2：飞机；3：轮船；4：其他
起点	T：3F92 F：an L：var.最大 20	城市名、站点名或范围名
终点	T：3F93 F：an L：var.最大 20	城市名、站点名或范围名
最近使用日期	T：3F94 F：cn L：4	格式：YYYYMMDD
最近使用交通工具	T：3F95 F：an L：1	0：火车；1：汽车；2：飞机；3：轮船；4：其他
总使用次数	T：3F96 F：an L：1	
交易类型授权码	T：3F98 F：b L： 1	01：联机圈存 02：联机消费 其他：RFU
应用标识符（AID）	T：4F F：b L：5－16	按 GB/T 16649.5-2002 规定标识应用。由注册的应用提供商标识和扩展的专用应用标识符组成
应用标签	T：50 F：an L：1－16	和 AID 相关的便于记忆的数据。 用于应用选择。存在于 ADF 的 FCI 中（可选）和 ADF 目录入口中（必备）
应用首选名称	T：3F99 F：an L：1－16	和 AID 相关的便于记忆的数据。若终端支持在发卡方代码表索引数据中指定的字符类型，终端在应用选择过程中显示应用首选名称

表B.1 （续）

数据元名称	数据元定义	数据元描述
应用优先指示器	T：87 F：b L：1	若卡片中有多个应用，指出同一目录中的应用的优先级 位 8 1：没有持卡人确认应用不能选择 0：没有持卡人确认应用可以选择 位 7-5：RFU（000） 位 4-1： 0000：不指定优先级 xxxx：应用显示和选择的顺序，从 1-15.1 的优先级最高
应用模板	T：61 F：b L：var. 最大 252	按 GB/T 16649.5-2002 的规定，包含和应用目录入口相关的 1 个或多个数据对象
应用处理计数器	T：3FA1 F：b L：2.	初始值为 0，执行一次交易加 1
CA 公钥索引 （PKI）	T： 8F F： b L： 1	在身份鉴别过程中，用来标识 CA 公钥
专用文件（DF）名称	T： 84 F： b L： 5－16	按 GB/T 16649.4-2010 规定的，DF 的名字
目录自定义模板	T： 73 F： var. L： var. 最大 252	按 GB/T 16649.5-2002，目录中发卡方自定义部分
动态数据认证数据对象列表（DDOL）	T： 3FA2 F： b L： var. 最大 252	在身份鉴别命令中需要终端送到卡片中的数据列表，包括数据对象的标签和长度
文件控制信息（FCI）专用模板	T： A5 F： var. L： var.	按 GB/T 16649.4-2010，标识 FCI 模板中，专用于 JR/T 0025-2013 的数据对象
文件控制信息（FCI）模板	T： 6F F： var. L： var.最大 252	按 GB/T 16649.4-2010，标识 FCI 模板
教育卡动态数据 .	T： － F： － L： var	教育卡生成或保存的动态数据。在签名的动态应用数据中传送给终端。终端用来证明身份鉴别执行了

表B.1 （续）

数据元名称	数据元定义	数据元描述
IC 动态数	T： 3FA3 F： b L： 2－8	身份鉴别处理过程中，卡片生成的随时间变化不同的随机数。包括在签名动态数据中送到终端，由终端恢复
教育卡私钥	T： － F： b L： N_{IC}	教育卡公私钥对中的私钥部分。用于脱机动态数据认证。有两种格式：模/私钥指数形式和中国余数定理（CRT）形式
教育卡公钥证书	T： 3FA5 F： b L： N_I	发卡方认证过的教育卡公钥
人员签名证书	T： 3FA8 F： b L： N_{CA}	
安全报文鉴别密钥	T： － F： b L： 16	专有数据。双长度安全报文鉴别密钥，16 字节。当发卡方脚本需要安全报文时用来计算 MAC
短文件标识符	T： 88 F： b L： 1	命令中用于标识文件。字节中高三位为 0
签名的动态应用数据	T： 3FA9 F： b L： N_{IC}	卡片生成的动态数据签名。在身份鉴别过程中由终端验证
国家教育管理应用保留信息 1	T： 3FAA F： b L：2048	
国家教育管理应用保留信息 2	T： 3FAB F： b L：2048	
算法支持指示器	T：3FB1 F；b L：1	01：国密算法 02：国际算法
应用版本号	T：3FB2 F：b L：1	
卡号	T：5A F：cn L：10	由统一的教育卡发卡系统产生、全国唯一、长度为十字节

表B.1 （续）

数据元名称	数据元定义	数据元描述
应用启用日期	T：3FB3 F：cn L：4	卡片中应用启用日期 YYYYMMDD
应用失效日期	T：3FB4 F：cn L：4	卡片中应用的失效日期 YYYYMMDD
发卡方自定义数据	T：BF0C F：b L：2	发卡方自定义
身份证件类型	T：3FB5 F：an L：1	见 JY/T 1002-2012 定义的 SFZJLX 身份证件类型代码
身份证件号码	T：3FB6 F：an L：20	
姓名	T：3FB7 F：an L：var.最大 60	姓名全称的汉字，应支持 GB 18030-2005 汉字强制部分
居民身份证网上副本	T：3FB8 F：b L：var.最大 300	公安部门生成的居民身份证网上副本

附 录 C
（规范性附录）
命令规范

C.1 选择命令（SELECT）

C.1.1 定义和范围

SELECT命令通过文件名或AID来选择教育卡中的ADF，通过文件标识符来选择ADF中的AEF。
响应报文应由回送的FCI组成。

C.1.2 命令报文

SELECT命令报文代码见表C.1。

表C.1 SELECT 命令报文

代码	值
CLA	‘00’
INS	‘A4’
P1	04：使用ADF的AID进行选择 02：用文件标识符在当前ADF下选择EF（数据域=EF的文件标识符）
P2	‘00：第一个或唯一一个文件 02：下一个文件
Lc	‘05’-‘10’ 02：使用文件标识符时
Data	见C.1.3
Le	‘00’

C.1.3 命令报文数据域

命令报文数据域应包括所选择的ADF的AID或者2个字节的文件标识符。
支持部分DF名称选择DF，若有两个或以上DF部分名称相同，则选择第一个符合的DF。部分DF名称应为完整DF名的前N（5≤N≤16）个字节，否则返回应答“6700”。

C.1.4 响应报文数据域

响应报文数据域应包括所选择的ADF的FCI。
表C.2定义了成功选择后回送的FCI。

表C.2 成功选择 ADF 的响应报文（FCI）

标签	值	
‘6F’	FCI 信息	
	‘84’	DF 名

C.1.5 响应报文的状态字

教育卡支持部分名称选择，应遵守如下规则：

当一个DF成功选中后，终端重复发出SELECT命令，且P2设置为选择下一个文件的选项及使用相同的部分DF名时，卡片应该选中与部分DF名称匹配的不同的DF文件（若这样的DF存在）。在没有应用层命令干扰的情况下重复发出相同的SELECT命令，卡片应该可以找到所有满足条件的DF文件，且每个文件不会被找到两次。当所有满足条件的DF都被选择后，再发出同样的SELECT命令，应该得到没有文件被选择的结果，卡片应响应SW1SW2=“6A82”（文件未找到）。

SELECT命令执行返回的状态字见表C.3。

表C.3 SELECT 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
67	00	长度错误
6A	82	文件未找到
6A	86	参数 P1,P2 不正确
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误
6A	81	应用临时锁定
93	03	应用永久锁定

C.2 身份鉴别命令（PERSONAL AUTHENTICATE）

C.2.1 定义和范围

PERSONAL AUTHENTICATE命令使用收到的随机数、数据和卡片中储存的签名私钥计算“签名动态应用数据”。

C.2.2 命令报文

PERSONAL AUTHENTICATE命令报文代码见表C.4。

表C.4 PERSONAL AUTHENTICATE 命令报文代码

代码	值
CLA	00
INS	88
P1	00
P2	00
Lc	验证数据的长度
Data	见 C.2.3
Le	00

C.2.3 命令报文数据域

PERSONAL AUTHENTICATE命令报文数据域见表C.5。

表C.5 PERSONAL AUTHENTICATE 命令报文数据域

说明	长度（字节）
验证数据	8

C.2.4 响应报文数据域

响应报文数据域包括签名动态应用数据。签名动态应用数据定义见9.3.7.1。

C.2.5 响应报文的状态字

PERSONAL AUTHENTICATE命令执行返回的状态字见表C.6。

表C.6 PERSONAL AUTHENTICATE 执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
67	00	长度错误
69	85	使用条件不满足
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误

C.3 卡片鉴别命令（CARD AUTHENTICATE）

C.3.1 定义和范围

CARD AUTHENTICATE命令使用收到的随机数、数据和卡片中的签名私钥计算“签名动态应用数据”。

C.3.2 命令报文

CARD AUTHENTICATE命令报文代码见表C.7。

表C.7 CARD AUTHENTICATE 命令代码

代码	值
CLA	00
INS	89
P1	00
P2	00
Lc	验证数据的长度
Data	见 C.3.3
Le	00

C.3.3 命令报文数据域

CARD AUTHENTICATE命令报文数据域见表C.8。

表C.8　CARD AUTHENTICATE 命令报文数据域

说明	长度（字节）
验证数据	8

C.3.4　响应报文数据域

响应报文数据域包括签名动态应用数据。签名动态应用数据定义见9.3.7.1。

C.3.5　响应报文的状态字

CARD AUTHENTICATE命令执行返回的状态字见表C.9。

表C.9　CARD AUTHENTICATE 执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
67	00	长度错误
69	85	使用条件不满足
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误

C.4　取随机数命令（GET CHALLENGE）

C.4.1　定义和范围

GET CHALLENGE命令请求一个随机数。
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，该随机数将立即失效。

C.4.2　命令报文

GET CHALLENGE命令报文代码见表C.10。

表C.10　GET CHALLENGE 命令报文代码

代码	值
CLA	00
INS	84
P1	00
P2	00
Lc	不存在
Data	不存在
Le	04/08/10

C.4.3　命令报文数据域

命令报文数据域不存在。

C.4.4　响应报文数据域

响应报文数据域包括随机数，长度为Le字节。

C.4.5 响应报文的状态码

GET CHALLENGE命令执行返回的状态字见表C.11。

表C.11 GET CHALLENGE 执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
6A	81	不支持此功能
67	00	长度错误
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误

C.5 交易认证命令（TRANS AUTHENTICATE）

C.5.1 定义和范围

TRANS AUTHENTICATE命令要求教育卡验证ARPC或交易授权码。

C.5.2 命令报文

TRANS AUTHENTICATE报文代码见表C.12。

表C.12 TRANS AUTHENTICATE 命令报文代码

代码	值
CLA	00
INS	82
P1	00
P2	00
Lc	09
Data	见 C.5.3
Le	不存在

C.5.3 命令报文数据域

TRANS AUTHENTICATE命令的数据域见表C.13。

表C.13 TRANS AUTHENTICATE 命令报文数据域

说明	长度（字节）
ARPC	8
交易类型授权码	1

C.5.4 响应报文数据域

响应报文中没有数据域。

C.5.5 响应报文的状态码

TRANS AUTHENTICATE命令执行返回的状态字见表C.14。

表C.14 TRANS AUTHENTICATE 执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
69	82	安全条件不满足
63	00	交易认证校验失败
67	00	长度错误
69	01	命令不接受（无效状态）
69	85	使用条件不满足
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误

C.6 添加记录命令（APPEND RECORD）

C.6.1 定义和范围

APPEND RECORD命令用于在定长、变长或循环记录文件结尾添加记录。

卡片接收到APPEND RECORD命令后，将进行如下处理：

a) 判断新增记录长度是否超过文件记录最大长度限制，若超过，卡片回送状态字 6A80；

b) 判断文件剩余空间是否足够，若空间不足，卡片回送状态字 6A84。

通过以上判断,卡片将根据命令数据域的记录数据长度,分配记录空间,将新的记录数据写入文件。

命令成功执行后，设置记录指针指向所添加的记录。

C.6.2 命令报文

APPEND RECORD命令报文代码见表C.15。

表C.15 APPEND RECORD 命令报文代码

代码	值
CLA	04
INS	E2
P1	00
P2	见表 C.16
Lc	数据域的长度
Data	见 C.6.3
Le	不存在

参数P2的定义见表C.16。

表C.16 APPEND RECORD 命令报文中引用控制参数 P2 定义

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	—	—	—	RFU
X	X	X	X	X	—	—	—	SFI
1	1	1	1	1	—	—	—	RFU
—	—	—	—	—	X	X	X	RFU
其他值								RFU

C.6.3 命令报文数据域

命令报文数据域由写入的记录数据组成。若更新的文件为变长记录文件，则数据域需要按照TLV格式填写。

若为线路保护，则由写入的记录数据附上4字节MAC组成。

若为线路加密保护，则由被加过密的记录数据附上4字节MAC码组成。

C.6.4 响应报文数据域

响应报文数据域不存在。

C.6.5 响应报文的状态码

APPEND RECORD命令执行返回的状态字见表C.17。

表C.17 APPEND RECORD 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
65	81	内存失败（修改失败）
67	00	长度错误（Lc 域为空）
69	81	命令与文件结构不相容
69	82	不满足安全状态
69	87	安全报文数据项丢失（需要线路保护更新而采用明文更新方式时）
69	88	安全报文数据项不正确
6A	81	不支持此功能
6A	82	未找到文件
6A	83	未找到记录
6A	84	文件中存储空间不够
6A	85	使用条件不满足
6A	86	参数 P1 P2 不正确
6E	00	无效的 CLA
94	03	应用永久锁定

C.7 更新记录命令（UPDATE RECORD）

C.7.1 定义和范围

UPDATE RECORD命令用于更新记录信息。

卡片在收到UPDATE RECORD命令后，将进行以下处理：

a) 根据P2指定的SFI选取相应的EF文件。若文件不存在，卡片回送状态码“6A82”；

b) 检查文件的使用条件，若不满足条件，则回送状态码“6982”；

c) 指定的记录号不存在时，卡片回送状态码“6A83”。

命令执行成功后，将更新文件中指定的记录内容。

C.7.2 命令报文

UPDATE RECORD 命令报文代码见表C.18。

表C.18 UPDATE RECORD 命令报文代码

代码	值
CLA	04
INS	DC
P1	记录号
P2	引用控制参数，见表C.19
Lc	数据域的长度
Data	见C.7.3
Le	不存在

P1为记录号，若该文件有N条记录，则记录号可以是1~N。

Lc表示要写入的字节数。若为线路保护，Lc为写入数据的长度+4字节；若为加密线路保护，Lc为加密后数据的长度+4字节。

参数P2定义见表C.19。

表C.19 UPDATE RECORD 命令报文中引用控制参数P2定义

b7	b6	b5	b4	b3	b2	b1	b0	含义
x	X	X	x	x				SFI
					1	0	0	更新P1指定记录

C.7.3 命令报文数据域

命令报文数据域包含记录内容或安全报文。

命令报文数据域由写入的记录数据组成。若更新的文件为变长记录文件，则数据域应按照TLV格式填写。

若为线路保护，由写入的记录数据附上4字节MAC组成。

若为线路加密保护，由被加过密的记录数据附上4字节MAC码组成。

当CLA为04时，命令报文数据域为4字节MAC值。若该MAC值错误，则回送状态码“6988”。若MAC错误的次数达到该维护密钥的重试次数，则应用永久锁定，并回送状态码“9303”。

C.7.4 响应报文数据域

响应报文数据域不存在。

C.7.5 响应报文的状态码

UPDATE RECORD 命令执行返回的状态字见表 C.20。

表C.20 UPDATE RECORD 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
65	81	内存失败（修改失败）
67	00	长度错误（Lc 域为空）
69	81	命令与文件结构不相容
69	82	不满足安全状态
69	87	安全报文数据项丢失（需要线路保护更新而采用明文更新方式时）
69	88	安全报文数据项不正确
6A	80	数据域不正确
6A	81	不支持此功能
6A	82	未找到文件
6A	83	未找到记录
6A	84	文件中存储空间不够
6E	00	无效的 CLA
93	03	应用永久锁定

C.8 读记录命令（READ RECORD）

C.8.1 定义和范围

READ RECORD命令从一个变长记录文件或循环记录文件中读取一条文件记录。
响应报文包含这条被读出的记录。

C.8.2 命令报文

READ RECORD命令报文代码见表C.21。

表C.21 READ RECORD 命令报文代码

代码	值
CLA	00
INS	B2
P1	记录号
P2	引用控制参数，见表 C.22
Lc	不存在
Data	不存在
Le	00

引用控制参数P2的定义见表C.22。

表C.22 READ RECORD 命令引用控制参数 P2

b7	b6	b5	b4	b3	b2	b1	b0	含义
x	x	x	x	x				SFI
					1	0	0	读 P1 指定记录

C.8.3 命令报文数据域

命令报文中没有数据域。

C.8.4 响应报文数据域

READ RECORD命令执行成功后，响应报文的数据域包含读出的记录数据。

C.8.5 响应报文的状态字

READ RECORD命令执行返回的状态字见表C.23。

表C.23 READ RECORD 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
69	81	命令与文件结构不相容
69	82	安全条件不满足
67	00	长度错误
6A	82	文件未找到
6A	83	记录未找到
6A	86	参数 P1/P2 不正确
69	85	使用条件不满足
6C	XX	长度错误（Le 错误，xx 为实际长度）
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误
93	03	应用永久锁定

C.9 PIN码校验命令（VERIFY PIN）

C.9.1 定义和范围

VERIFY PIN命令用于校验PIN码的正确性。

C.9.2 命令报文

VERIFY PIN命令报文代码见表C.24。

表C.24 VERFIY PIN 命令报文代码

代码	值
CLA	00

表C.24 （续）

代码	值
INS	20
P1	00
P2	00
Lc	00 或 02~08
Data	见 C.9.3
Le	不存在

C.9.3 命令报文数据域

命令报文数据域由持卡者输入的PIN码组成。

C.9.4 响应报文数据域

响应报文数据域不存在。

C.9.5 响应报文的状态字

当前的应用选择中，命令数据域中外部输入的PIN码与卡中存放的PIN码校验失败时，教育卡将回送SW1 SW2=“63Cx”，其中x表示个人识别码允许重试的次数；当卡SW2=SW1 SW2=“63C0”时，表示不能允许继续校验PIN码。此时再使用VERIFY PIN命令时，将回送失败状态字SW1 SW2=“6983”。

VERIFY PIN命令执行返回的状态字见表C.25。

表C.25 VERIFYPIN 执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
63	Cx	校验失败，x 表示允许重试的次数
64	00	标志状态位没变
69	83	教育卡（个人识别码）锁定
69	84	引用数据无效
6A	86	P1 和 P2 错误
6A	88	未找到引用数据
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误
93	03	应用已被永久锁定

C.10 PIN码修改命令（CHANGE PIN）

C.10.1 定义和范围

CHANGE PIN命令将修改当前PIN码。

CHANGE PIN命令执行成功后，PIN尝试计数器复位至PIN尝试次数的上限。

此命令中的PIN码以明文方式传送。

C.10.2 命令报文

CHANGE PIN命令报文见表C.26。

表C.26 CHANGE PIN 命令报文

代码	值
CLA	80
INS	5E
P1	01
P2	00
L_c	11~19
Data	当前 PIN‖FF‖新的 PIN
L_e	不用

C.10.3 命令报文数据域

命令报文数据域由旧的口令密钥、填充的1字节的FF及新的口令密钥三部分组成 。

若当前没有用PIN或更改后不再使用PIN，则命令数据中的“当前PIN”或“新的PIN”可以不存在，即命令数据域以FF开头或FF结尾。有效的PIN至少为4位数字（2字节）。

C.10.4 响应报文数据域

响应报文数据域不存在。

C.10.5 响应报文的状态码

CHANGE PIN命令执行返回的状态字见表C.27。

表C.27 CHANGE PIN 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
63	Cx	验证失败，还剩下 X 次尝试机会
67	00	Lc 错误
65	81	内存错误
69	83	验证方法锁定
69	85	使用条件不满足
6A	80	数据域参数不正确
6A	86	P1 和 P2 参数不正确
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误
93	03	应用已被永久锁定

C.11 PIN码解锁与重装命令（PIN UNBLOCK/RELOAD PIN）

C.11.1 定义和范围

PIN UNBLOCK/RELOAD PIN命令为发卡方重置PIN码错误计数器的值为应用设定的最大次数，或者更改PIN码。

命令中PIN码的传递采用加密方式。

命令使用解锁口令密钥进行加密及MAC计算。

C.11.2 命令报文

PIN UNBLOCK/RELOAD PIN命令报文代码见表C.28。

表C.28 PIN UNBLOCK/RELOADPIN 命令报文

代码	值
CLA	84
INS	24
P1	00
P2	00：解锁 PIN（仅重置尝试计数器，并不更改 PIN） 01：更改 PIN（重置尝试计数器并以新 PIN 取代原 PIN）
Lc	数据域字节数
Data	见 C.11.3
Le	不存在

C.11.3 命令报文数据域

PIN UNBLOCK/RELOAD PIN命令报文数据域定义，见表C.29。

表C.29 PIN UNBLOCK/RELOAD PIN 命令报文数据域定义

命令报文数据域	Lc 值	数据域内容
解锁 PIN	04	Lc 应包含 MAC 数据元长度
更改 PIN	14	Lc 应同时包括被加密的 PIN 数据元和 MAC 数据元的长度

当被加密的PIN码数据长度为零时，卡片应使卡片内部已存在的有效的PIN置为空的PIN。

若MAC值错误，则回送状态码“6988”；若MAC错误的次数达到解锁口令密钥的重试次数，则应用永久锁定，回送状态码“9303”。

C.11.4 响应报文数据域

响应报文数据域不存在。

C.11.5 响应报文的状态字

PIN UNBLOCK/RELAOD PIN命令执行返回的状态字见表C.30。

表C.30 PIN UNBLOCK/RELAOD PIN 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
67	00	Lc 错误

表C.30 （续）

SW1	SW2	说明
65	81	内存失败
69	82	不满足安全状态
69	84	引用数据无效（没有取随机数）
69	85	使用条件不满足（PIN 未锁定）
69	87	安全报文数据项丢失（需要线路保护更新而采用明文更新方式时）
69	88	安全报文数据项不正确
6A	86	P1 和 P2 错误
6A	88	未找到引用数据、 密钥未找到（解锁口令密钥不存在）
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误
93	03	应用被永久锁定

C.12 应用锁定命令（APPLICATION BLOCK）

C.12.1 定义和范围

APPLICATION BLOCK命令使当前选择的应用被临时锁定或永久锁定。

C.12.2 命令报文

APPLICATION BLOCK命令报文代码见表C.31。

表C.31 APPLICATION BLOCK 命令报文代码

代码	值
CLA	84
INS	1E
P1	00
P2	00 临时锁定，01 永久锁定
Lc	数据域字节长度
Data	见 C.12.3
Le	不存在

C.12.3 命令报文数据域

命令报文的数据域中包含了根据第10章中描述的安全报文格式代码的MAC数据。

C.12.4 响应报文数据域

响应报文中没有数据域。

C.12.5 响应报文的状态码

APPLICATION BLOCK命令执行返回的状态字见表C.32。

表C.32 APPLICATION BLOCK 执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
69	82	安全条件不满足
67	00	长度错误
69	01	命令不接受（无效状态）
69	85	使用条件不满足
69	88	安全报文数据项不正确
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误

C.13 应用解锁命令（APPLICATION UNBLOCK）

C.13.1 定义和范围

APPLICATION UNBLOCK命令用于恢复当前应用。

当APPLICATION UNBLOCK命令成功地完成后，由APPLICATION BLOCK命令产生的对应用命令响应的限制将被取消。

该指令数据域为4字节MAC值。若MAC值错误,则应用锁定指令会报安全报文数据项不正确的状态码，若MAC错误的次数超过了该维护密钥的重试次数，则锁定应用。

C.13.2 命令报文

APPLICATION UNBLOCK报文代码见表C.33。

表C.33 APPLICATION UNBLOCK 命令报文代码

代码	值
CLA	84
INS	18
P1	00
P2	00
Lc	数据域字节长度
Data	见 C.13.3
Le	不存在

C.13.3 命令报文数据域

命令报文的数据域中包含了安全报文格式代码的MAC数据。

C.13.4 响应报文数据域

响应报文中没有数据域。

C.13.5 响应报文的状态码

APPLICATION UNBLOCK命令执行返回的状态字见表C.34。

表C.34 APPLICATION UNBLOCK 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
69	82	安全条件不满足
67	00	长度错误
69	01	命令不接受（无效状态）
69	85	使用条件不满足
69	88	安全报文数据项不正确
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误
93	03	应用永久锁定

C.14 取应用交易计数器命令（GET ATC）

C.14.1 定义和范围

GET ATC 命令用于获取应用交易计数器的值。

C.14.2 命令报文

GET ATC命令报文代码见表C.35。

表C.35 GET ATC 命令报文代码

代码	值
CLA	80
INS	CA
P1	3F
P2	A1
Lc	不存在
Data	不存在
Le	02

C.14.3 命令报文数据域

GET ATC命令报文没有数据域。

C.14.4 响应报文数据域

响应报文的数据域中包含应用交易计数器的值。

C.14.5 响应报文的状态字

GET ATC命令执行返回的状态字见表C.36。

表C.36 GET ATC 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
67	00	长度错误
6A	88	不存在该数据元
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误

C.15 联机圈存命令（CREDIT FOR ONLINE LOAD）

C.15.1 定义和范围

CREDIT FOR ONLINE LOAD命令用于联机圈存交易。

C.15.2 命令报文

CREDIT FOR ONLINE LOAD命令报文代码见表C.37。

表C.37 CREDIT FOR ONLINE LOAD 命令报文代码

代码	值
CLA	80
INS	52
P1	00
P2	00
Lc	15
Data	见 C.15.3
Le	0A

C.15.3 命令报文数据域

CREDIT FOR ONLINE LOAD命令数据域格式见表C.38。

表C.38 CREDIT FOR ONLINE LOAD 命令报文数据域

说明	长度（字节）
交易金额	4
终端机编号	6
交易日期（主机）	4
交易时间（主机）	3
MAC	4

C.15.4 响应报文数据域

CREDIT FOR ONLINE LOAD命令执行成功的响应报文数据域见表C.39。命令执行未成功的，无数据域。

表C.39 CREDIT FOR ONLINE LOAD 命令响应报文数据域

说明	长度（字节）
ATC	2
AC	8

C.15.5 响应的报文状态码

CREDIT FOR ONLINE LOAD命令命令执行返回的状态字见表C.40。

表C.40 CREDIT FOR ONLINE LOAD 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
65	81	内存错误
67	00	长度错误
69	01	命令不接受（无效状态）
69	85	使用条件不满足
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误
93	02	MAC 无效

C.16 联机消费命令（DEBIT FOR ONLINE PURCHASE）

C.16.1 定义和范围

DEBIT FOR ONLINE PURCHASE命令用于联机消费交易。

C.16.2 命令报文

DEBIT FOR ONLINE PURCHASE命令报文代码见表C.41。

表C.41 DEBIT FOR ONLINE PURCHASE 命令报文代码

代码	值
CLA	80
INS	54
P1	01
P2	00
Lc	17
Data	见 C.16.3
Le	0A

C.16.3 命令报文数据域

DEBIT FOR ONLINE PURCHASE命令的数据域见表C.42。

表C.42 DEBIT FOR ONLINE PURCHASE 命令报文数据域

说明	长度（字节）
交易金额	4
终端机编号	6
终端交易序号	2
交易日期（主机）	4
交易时间（主机）	3
MAC	4

C.16.4 响应报文数据域

DEBIT FOR ONLINE PURCHASE响应报文数据域见表C.43。命令执行未成功的，无数据域。

表C.43 DEBIT FOR ONLINE PURCHASE 响应报文数据域

说明	长度（字节）
ATC	2
AC	8

C.16.5 响应的报文状态码

DEBIT FOR ONLINE PURCHASE命令执行返回的状态字见表C.44。

表C.44 DEBIT FOR ONLINE PURCHASE 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
65	81	内存错误
67	00	长度错误
69	01	命令不接受（无效状态）
69	85	使用条件不满足
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误
93	02	MAC 无效

C.17 取脱机交易应用密文命令（GET TRANSACTION PROVE）

C.17.1 定义和范围

GET TRANSACTION PROVE 命令提供了一种在交易处理过程中拔出并重插卡后卡片的恢复机制。

C.17.2 命令报文

GET TRANSACTION PROVE命令报文代码见表C.45。

表C.45 GET TRANSACTION PROVE 命令报文代码

代码	值
CLA	80
INS	CA
P1	00
P2	00
Lc	02
Data	见 C.17.3
Le	08

C.17.3 命令报文数据域

命令报文数据域由终端指定的交易ATC组成。

C.17.4 响应报文数据域

GET TRANSACTION PROVE命令响应报文数据域见表C.46。

表C.46 GET TRANSACTION PROVE 响应报文数据域

说明	长度（字节）
AC	8

C.17.5 响应报文的状态码

GET TRANSACTION PROVE命令执行返回的状态字见表C.47。

表C.47 GET TRANSACTION PROVE 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
67	00	长度错误
94	06	所需 TC 不可用
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误

C.18 修改二进制命令（UPDATE BINARY）

C.18.1 定义和范围

UPDATE BINARY命令用于更新二进制文件信息。

卡片在收到UPDATE BINARY命令后，将进行以下处理：

a) 根据 P1 指定的 SFI 选取相应的 EF 文件。若文件不存在，卡片回送状态码“6A82”；

b) 检查文件的使用条件，若不满足条件，则回送状态码“6985”；

c) 更新指定的二进制文件信息。

C.18.2 命令报文

UPDATE BINARY命令报文代码见表C.48。

表C.48 UPDATE BINARY 命令报文代码

代码	值
CLA	04
INS	D6
P1	引用控制参数，见表 C.49
P2	引用控制参数，见表 C.49
Lc	数据域的长度
Data	见 C.18.3
Le	不存在

参数P1、P2的定义如表C.49。

表C.49 UPDATE BINARY 命令报文中引用控制参数 P1、P2 定义

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
1	0	0	SFI					文件的偏移量
0	文件的偏移量							

C.18.3 命令报文数据域

若为明文，数据域为要写入的新数据；若为线路保护，数据域为写入的新数据+4字节MAC码（用该文件的安全报文密钥计算MAC）；若为线路加密保护，数据域为加密后的数据（用该文件的安全报文密钥加密）+4字节MAC码（用该文件的安全报文密钥计算MAC）。

当CLA为04时，命令报文数据域中包含4字节MAC值。若该MAC值错误，则回送状态码“6988”；若MAC错误的次数达到该维护密钥的重试次数，则应用永久锁定，并回送状态码“9303”。

C.18.4 响应报文数据域

UPDATE BINARY命令的响应报文数据域不存在。

C.18.5 响应报文的状态码

UPDATE BINARY命令执行返回的状态字见表C.50。

表C.50 UPDATE BINARY 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
65	81	内存失败（修改失败）
67	00	长度错误（Lc 域为空）
69	81	命令与文件结构不相容
69	82	不满足安全状态

表C.50 （续）

SW1	SW2	说明
69	87	安全报文数据项丢失（需要线路保护更新而采用明文更新方式时）
69	88	安全报文数据项不正确
6A	80	数据域不正确
6A	81	不支持此功能
6A	82	未找到文件
69	81	文件类型错误
6A	84	文件中存储空间不够
6B	00	参数错误(偏移地址超出了 EF)
93	03	应用永久锁定

C.19 读二进制文件命令（READ BINARY）

C.19.1 定义和范围

READ BINARY命令从一个二进制文件中读取一段数据。

C.19.2 命令报文

READ BINARY命令报文代码见表C.51。

表C.51 READ BINARY 命令报文

代码	值
CLA	00
INS	B0
P1	引用控制参数，见表 C.52
P2	引用控制参数，见表 C.52
Lc	不存在
Data	不存在
Le	00~FF

参数P1、P2的定义见表C.52。

表C.52 READ BINARY 命令引用控制参数

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
1	0	0	SFI					文件的偏移量
0	文件的偏移量							

若Le=0，偏移量+256小于等于文件实际长度时，读取从偏移量开始的256字节内容；偏移量+256大于文件实际长度时，读取从偏移量开始到文件结束的所有内容。

若Le≠0，偏移量+Le小于文件实际长度时，读取从偏移量开始的Le字节；偏移量+Le大于文件实际长度时，则送回警告状态6Cxx，xx为可读取的有效数据长度，请求将Le置为xx并重发该命令。

C.19.3 命令报文数据域

READ BINARY命令报文中没有数据域。

C.19.4 响应报文数据域

READ BINARY命令执行成功，响应报文的数据域包含读出的数据。

C.19.5 响应报文的状态字

READ BINARY命令执行返回的状态字见表C.53。

表C.53 READ BINARY 执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
69	81	不是二进制文件
69	82	读的条件不满足
69	86	不满足命令执行的条件（未选择任何 EF，而使用当前文件方式操作）
67	00	长度错误
6A	82	文件未找到
6A	86	参数 P1/P2 不正确
69	85	使用条件不满足
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误
6B	00	参数错误(偏移地址超出了 EF)
6C	XX	长度错误（Le 错误；XX 为实际长度）

C.20 外部认证命令（EXTERNAL AUTHENTICATE）

C.20.1 定义和范围

EXTERNAL AUTHENTICATE命令要求教育卡中的应用验证终端设备中保密模块的有效性，以使终端设备获得某种授权。

C.20.2 命令报文

EXTERNAL AUTHENTICATE命令报文代码见表C.54。

表C.54 EXTERNAL AUTHENTICATE 命令报文代码

代码	值
CLA	00
INS	82
P1	00
P2	外部认证密钥标识符（0-F）
Lc	10~11
Data	见 C.20.3

表C.54 （续）

代码	值
Le	不存在

C.20.3 命令报文数据域

命令报文数据域中包括以下数据：

a) 第 1 至第 8 字节为认证数据。认证数据是使用过程密钥对终端产生的随机数进行加密，加密方式见 9.2.1.1。过程密钥是使用终端产生的随机数对外部认证密钥进行分散生成，密钥分散方式见 9.2.1.3；
b) 第 9 至第 16 字节为终端产生的随机数；
c) 第 17 字节表示密钥版本，为可选数据。若不存在该字节，则表示使用该密钥标识第一条添加的外部认证密钥。

C.20.4 响应报文数据域

EXTERNAL AUTHENTICATE命令响应报文数据域不存在。

C.20.5 响应报文的状态字

EXTERNAL AUTHENTICATE命令执行返回的状态字见表C.55。

表C.55 EXTERNAL AUTHENTICATE 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
69	82	安全条件不满足
67	00	长度错误
6A	82	文件未找到
69	81	文件类型错误
6A	86	参数 P1/P2 不正确
69	85	使用条件不满足
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误
6B	00	参数错误(偏移地址超出了 EF)

C.21 获取教育卡认证码命令（READ AUTHCODE）

C.21.1 定义和范围

READ AUTHCODE命令用于从教育卡中取得国家教育主管部门为每张教育卡芯片生成的认证码。

C.21.2 命令报文

READ AUTHCODE命令报文代码见表C.56。

表C.56 READ AUTHCODE 命令报文代码

代码	值
CLA	80
INS	CA
P1	00
P2	00
Lc	无
Data	无
LE	10

C.21.3 命令报文数据域

READ AUTHCODE命令报文没有数据域。

C.21.4 响应报文数据域

响应报文的数据域为识别认证信息。

C.21.5 响应报文的状态字

READ AUTHCODE命令执行返回的状态字见表C.57。

表C.57 READ AUTHCODE 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
67	00	长度错误
6A	86	P1、P2 参数不正确
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误

C.22 导出会话密钥命令（EXPORT SESSION KEY）

C.22.1 定义和范围

EXPORT SESSION KEY命令用于生成对称会话密钥，保存到RAM中，并用加密公钥加密导出。

使用条件如下：

a) RAM 中有足够空间保存会话密钥；

b) 满足加密公钥的使用权限。

C.22.2 命令报文

EXPORT SESSION KEY 命令报文代码见表 C.58。

表C.58 EXPORT SESSION KEY 命令报文代码

代码	值
CLA	80
INS	D8
P1	02
P2	见表 C.59
Lc	加密导出：Lc=4； 明文导出：无
DATA	加密导出：见 C.22.3 明文导出：无
Le	会话密钥密文长度

P2参数说明见表C.59。

表C.59 EXPORT SESSION KEY 命令报文 P2 参数说明

b7	b6	b5	b4	b3	b2	b1	b0	说明
1								加密导出
0								明文导出
	0	1						SM2 算法
			-	-	x	x	x	密钥索引号

C.22.3 命令报文数据域

密文导出时，命令数据域包括用于对称密钥加密的公钥文件标识符数据元。
公钥文件标识符数据元格式见表C.60。

表C.60 EXPORT SESSION KEY 命令报文数据域

T	L	V
0xC0	0x02	公钥文件 FID，FID=0x0000 表示使用会话公钥

C.22.4 响应报文数据域

响应数据是会话密钥明文或密文，输出数据格式为大端序模式，见表 C.61、C.62。

表C.61 EXPORT SESSION KEY 命令明文导出响应数据

T	L	V
0xC1	XX（XX<80）	会话密钥明文

表C.62 EXPORT SESSION KEY 命令密文导出响应数据

T	L	V
0xC1	XX（XX<80）	会话密钥密文

C.22.5 响应报文状态字

EXPORT SESSION KEY命令执行返回的状态字见表C.63。

表C.63 EXPORT SESSION KEY 命令执行返回的状态字

SW1	SW2	说明
90	00	命令正确执行
65	81	内存访问错误
67	00	Lc 长度错
69	81	文件类型不匹配
69	82	不满足安全状态
69	85	使用条件不满足
6A	80	数据域错
6A	81	功能不支持
6A	82	文件未找到
6A	86	P1、P2 参数错
93	03	应用永久锁定

C.23 导入会话密钥命令（IMPORT SESSION KEY）

C.23.1 定义和范围

IMPORT SESSION KEY命令使用明文或密文导入对称会话密钥。该会话密钥保存在RAM中（最多同时保存5条会话密钥）。

C.23.2 命令报文

IMPORT SESSION KEY 命令报文代码见表 C.64。

表C.64 IMPORT SESSION KEY 命令报文代码

代码	值
CLA	80
INS	4A
P1	会话密钥算法类型，见表 C.65
P2	见表 C.66
Lc	P1！=FF，Lc 为会话密钥明文或密文长度 P1=ff，Lc 为 0
DATA	P1！=FF，见 C.23.3 P1=FF，数据域为空
Le	导入成功：1

P1 参数说明见表 C.65。

表C.65 IMPORT SESSION KEY 命令报文 P1 参数说明

b7	b6	b5	b4	b3	b2	b1	b0	说明
					x	x	x	会话密钥算法类型
					0	1	0	SM4 算法
			x	x				数据分块传输方式
			0	0				唯一块
			0	1				首块
			1	0				中间块
			1	1				尾块
1	1	1	1	1	1	1	1	删除指定会话密钥

P2 参数说明见表 C.66。

表C.66 IMPORT SESSION KEY 命令报文 P2 参数说明

b7	b6	b5	b4	b3	b2	b1	b0	说明
1								加密导入
0								明文导入
	0	1						SM2
			0					小端序模式
			1					大端序模式
					x	x	x	索引号 00：增加新密钥； 1~5：对应卡内密钥索引号+1；

C.23.3 命令报文数据域

数据域为SM2私钥文件标识符和会话密钥，格式采用TLV格式，如表C.67、C.68、C.69所示。

表C.67 IMPORT SESSION KEY 命令对应的私钥文件标识符数据元格式

T	L	V
C2	02	私钥文件 FID

表C.68 IMPORT SESSION KEY 命令对应的会话密钥明文数据元格式

T	L	V
C1	XX	会话密钥明文

表C.69 IMPORT SESSION KEY 命令会话密钥密文数据元格式

T	L	V
C1	82XXXX	会话密钥密文

C.23.4 响应数据域

导入会话密钥成功，返回该会话密钥在卡内的索引号（0-4）。

C.23.5 响应报文状态字

IMPORT SESSION KEY命令执行返回的状态字见表C.70。

表C.70 IMPORT SESSION KEY 命令执行返回的状态字

SW1	SW2	说明
90	00	命令正确执行
67	00	Lc 错误
6A	80	数据域的参数错误
6A	81	使用条件不满足
6A	86	P1 或者 P2 错误
6A	88	未找到引用数据
6D	00	指令不支持
6E	00	CLA 错误
93	03	应用被永久锁定

C.24 加密/解密命令（ENCRYPT/DECRYPT）

C.24.1 定义和范围

ENCRYPT/DECRYPT命令使用外部导入或内部保存的对称密钥对数据（满足分组长度的整数倍，卡内不做填充处理）进行加解密。使用条件如下：

a) 密钥来自密钥文件时，密钥文件要存在；
b) 每个指定的对称密钥文件中仅能保存一条密钥记录；
c) 使用内部密钥时，满足密钥的使用权限。

C.24.2 命令报文

ENCRYPT/DECRYPT 命令报文代码见表 C.71。

表C.71 ENCRYPT/DECRYPT 命令报文代码

代码	值
CLA	80
INS	FA
P1	00 唯一数据块，01 第一个数据块，02 中间数据块，03 末尾数据块
P2	P1=00,01：P2 见表 C.72；P1=02,03：P2=0；
Lc	输入数据长度
DATA	见 C.24.3
Le	返回的数据长度

P2 参数说明见表 C.72。

表C.72 ENCRYPT/DECRYPT 命令报文 P2 参数说明

b7	b6	b5	b4	b3	b2	b1	b0	说明
1								加密操作
0								解密操作
	0	0						加/解密密钥来自密钥文件
	1	0						使用已导入的会话密钥，若是初始数据块，则输入数据为 4 字节会话密钥 ID+待计算数据
				0	0	0		算法由密钥记录中的算法标识指定
							0	ECB 模式
							1	CBC 模式

C.24.3 命令报文数据域

命令报文数据域为待加密/解密数据。

C.24.4 响应数据域

响应数据域为加密/解密的计算结果。

C.24.5 响应报文状态字

ENCRYPT/DECRYPT 命令执行返回的状态字见表 C.73。

表C.73 ENCRYPT/DECRYPT 命令执行返回的状态字

SW1	SW2	说明
90	00	命令正确执行
67	00	Lc 长度错
69	81	文件类型不匹配
69	82	不满足安全状态
69	85	使用条件不满足
6A	80	数据域错
6A	81	功能不支持
6A	82	文件不存在
6A	86	P1、P2 参数错
6A	88	密钥不存在
93	03	应用永久锁定

C.25 哈希计算命令（DATA HASH）

C.25.1 定义和范围

DATA HASH命令采用SM3散列算法计算数据的哈希值。

C.25.2 命令报文

DATA HASH 命令报文代码见表 C.74。

表C.74 DATA HASH 命令报文代码

代码	值
CLA	80
INS	C4
P1	见表 C.75
P2	03：SM3，其他：RFU
Lc	01~FF
DATA	见 C.25.3
Le	00

P1 参数说明见表 C.75。

表C.75 DATA HASH 命令的 P1 参数说明

b7	b6	b5	b4	b3	b2	b1	b0	说明
0	0							数据来自卡外
0	1							数据来自卡内指定文件
1	0							数据来自卡外和卡内指定文件
1	1							数据为 4 字节会话密钥标识
		0	0	0	0	0	0	首块
		0	0	0	0	0	1	仅此一块
		0	0	0	0	1	0	中间块
		0	0	0	0	1	1	最后一块

C.25.3 命令报文数据域

若P1最高两位是00，则命令报文数据域是Hash计算输入数据块数据元（见表C.76）；若是01，则数据域是卡内数据文件标识符数据元（见表C.77）；若是10，则数据域是卡内数据文件标识符数据元和Hash计算输入数据块数据元。有卡外输入数据时，卡外输入数据在前，卡内数据在后计算Hash值。

表C.76 DATA HASH 命令对应的 Hash 计算输入数据块数据元格式

T	L	V
0xC1	XX	输入数据块，大端序模式

表C.77 DATA HASH 命令对应的卡内数据文件标识符数据元格式

T	L	V
0xC0	0x02	数据文件 FID

C.25.4 响应数据域

若P1的最低位是1，则响应报文是数据压缩的结果（非TLV格式，采用大端序模式）；否则无响应报文。

C.25.5 响应报文状态字

DATA HASH命令执行返回的状态字见表C.78。

表C.78 DATA HASH 命令执行返回的状态字

SW1	SW2	说明
90	00	命令正确执行
67	00	Lc 错误
6A	81	使用条件不满足
6A	86	P1 或者 P2 错误
6A	88	未找到引用数据
6D	00	指令不支持
6E	00	CLA 错误
93	03	应用被永久锁定

C.26 SM2 密钥对生成命令（SM2 GENERATE KEY PAIR）

C.26.1 定义和范围

SM2 GENERATE KEY PAIR命令用于产生SM2密钥对，同时将私钥和公钥分别存放在指定文件中。使用条件如下:

a) 满足公私钥文件的写权限;
b) 文件长度符合算法需要。

C.26.2 命令报文

SM2 GENERATE KEY PAIR 命令报文代码见表 C.79。

表C.79 SM2 GENERATE KEY PAIR 命令报文代码

代码	值
CLA	80
INS	40
P1	00
P2	00 SM2 签名密钥对；01 SM2 加密密钥对

表C.79 （续）

代码	值
Lc	08
DATA	见 C.26.3
Le	无或公钥模数据元长度+公钥指数数据元长度

C.26.3 命令报文数据域

数据域为公钥文件FID数据元和私钥文件FID数据元（见表C.80、C.81）。若公钥文件FID=0000，则不保存公钥文件，公钥通过响应报文返回。

表C.80 SM2 GENERATE KEY PAIR 命令对应的公钥文件标识符数据元格式

T	L	V
0xC0	0x02	公钥文件 FID，FID=0x0000 时使用临时公钥

表C.81 SM2 GENERATE KEY PAIR 命令对应的私钥文件标识符数据元格式

T	L	V
0xC2	0x02	私钥文件 FID

C.26.4 响应数据域

若公钥FID不等于0，则无响应数据；否则响应数据为返回公钥参数数据元（见表C.82）。

表C.82 SM2 GENERATE KEY PAIR 命令对应的 SM2 公钥数据元格式

T	L	V
0xCA	0x40	SM2 公钥参数数据（点坐标 X、Y）

C.26.5 响应报文状态字

SM2 GENERATE KEY PAIR命令执行返回的状态字见表C.83。

表C.83 SM2 GENERATE KEY PAIR 命令执行返回的状态字

SW1	SW2	说明
90	00	命令正确执行
65	81	内存访问错误
67	00	Lc 长度错
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持
6A	82	文件未找到
6A	86	P1、P2 参数错
6A	89	文件类型（密钥长度）和当前操作不匹配
93	03	应用永久锁定

C.27 SM2 公钥计算命令（SM2 PUBLIC KEY CAL）

C.27.1 定义和范围

SM2 PUBLIC KEY CAL命令使用SM2公钥进行加密/验签计算。若使用外部公钥计算，则应先使用IMPORT SM2 KEY指令将公钥导入到内部RAM中。使用条件如下:

a) 使用内部文件中公钥时，需要满足公钥使用权限；

b) 使用 RAM 中的公钥时，应事先导入公钥到 RAM。

C.27.2 命令报文

SM2 PUBLIC KEY CAL 命令报文代码见表 C.84。

表C.84 SM2 PUBLIC KEY CAL 命令报文代码

代码	值
CLA	80
INS	4C
P1	00
P2	00 SM2 公钥验签；01 SM2 公钥加密
Lc	见说明
DATA	见 C.27.3
Le	00

说明:

SM2验签操作：Lc=0x06+公钥文件路径长度+Hash值长度+签名长度。

SM2加密操作：Lc=0x06+公钥文件路径长度+待加密数据长度。

C.27.3 命令报文数据域

命令数据域为指定公钥文件绝对路径或标识符和计算数据块，格式采用 TLV 格式，如表 C.85、C.86、C.87 所示。

表C.85 SM2 PUBLIC KEY CAL 命令对应的公钥文件标识符数据元格式

T	L	V
0xC0	路径长度	公钥文件路径或 FID，该文件不能是内部公钥文件（FID 最高位为 1），FID=0x0000 时使用临时公钥

表C.86 SM2 PUBLIC KEY CAL 命令对应的 SM2 验签计算输入数据块数据元格式

T	L	V
0xC1	820060	Hash 值+数字签名

表C.87 SM2 PUBLIC KEY CAL 命令对应的 SM2 加密计算输入数据块数据元格式

T	L	V
0xC1	82XXXX	待加密数据块，“XXXX”表示数据字节长度（不得超过通信缓冲区长度-私钥长度×3）

C.27.4 响应报文数据域

SM2 PUBLIC KEY CAL 的响应报文数据域为公钥计算结果。

C.27.5 响应报文状态字

SM2 PUBLIC KEY CAL命令执行返回的状态字见表C.88。

表C.88 SM2 PUBLIC KEY CAL 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
67	00	Lc 长度错
69	81	文件类型不匹配
69	82	不满足安全状态
69	85	使用条件不满足 (密钥不完整)
6A	80	数据域错（Data 数据大于模数 n）
6A	81	功能不支持
6A	82	文件未找到
93	03	应用永久锁定

C.28 SM2 私钥计算命令(SM2 PRIVATE KEY CAL)

C.28.1 定义和范围

SM2 PRIVATE KEY CAL命令使用SM2私钥进行解密/签名计算。使用内部文件中私钥时，需要满足私钥使用权限。

C.28.2 命令报文

SM2 PRIVATE KEY CAL命令报文代码见表C.89。

表C.89 SM2 PRIVATE KEY CAL 命令报文代码

代码	值
CLA	80
INS	4E
P1	00
P2	00 SM2 签名操作；01 SM2 解密操作
Lc	见说明

表C.89 （续）

代码	值
DATA	见 C.28.3
Le	00

说明:

SM2签名操作：Lc=0x26+公钥文件路径长度。

SM2解密操作：Lc=0x06+公钥文件路径长度+待解密数据长度。

C.28.3 命令报文数据域

命令数据域为指定私钥文件绝对路径或标识符和计算数据块，格式采用TLV格式，见表C.90、C.91、C.92。

表C.90 SM2 PRIVATE KEY CALSM2 私钥计算）命令对应的私钥文件标识符数据元格式

T	L	V
0xC2	路径长度	私钥文件绝对路径或 FID，该文件不能是内部私钥文件（FID 最高位为 1）

表C.91 SM2 PRIVATE KEY CALSM2 私钥计算）命令对应的 SM2 签名计算输入数据块数据元格式

T	L	V
0xC1	0x820020	Hash 值

表C.92 SM2 PRIVATE KEY CALSM2 私钥计算）命令对应的 SM2 解密计算输入数据块数据元格式

T	L	V
0xC1	0x82XXXX	待解密数据块，“XXXX”表示数据字节长度（不得超过通信缓冲区长度）

C.28.4 响应数据域

SM2 PRIVATE KEY CAL 命令的响应报文数据域为私钥计算结果。

C.28.5 响应报文状态字

SM2 PRIVATE KEY CAL命令执行返回的状态字见表C.93。

表C.93 SM2 PRIVATE KEY CAL 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
61	XX	命令执行成功，有 XX 字节数据要返回
67	00	Lc 长度错
69	81	文件类型不匹配
69	82	不满足安全状态
69	85	使用条件不满足（密钥不完整）
6A	80	数据域错（Data 数据大于模数 n）
6A	81	功能不支持

续C.93 （续）

SW1	SW2	说明
6A	82	文件未找到
93	03	应用永久锁定

C.29 导入SM2 密钥命令（IMPORT SM2 KEY）

C.29.1 定义和范围

IMPORT SM2 KEY命令用于导入SM2公私钥到指定文件中，但该文件不能是内部公私钥文件（FID最高位为1），或导入临时公钥。应支持使用卡内对称会话密钥加密导入公私钥。若选择密文导入，则执行指令前需事先执行IMPORT SESSION KEY导入对称会话密钥。若CLA=0x84，则指令数据域中的MAC是使用卡指定卡内应用维护密钥计算而得，计算过程是先执行GET CHALLENGE命令获取8字节随机数，然后使用应用维护密钥加密随机数产生8字节过程密钥，最后使用过程密钥对命令报文计算MAC（注：PKI应用中MAC计算时的初始向量为此随机数）。CA应用中用指定的会话解密计算MAC，计算方法见9.4.2.2。

使用条件如下:

a) 公私钥文件存在;

b) 满足文件的写入权限。

C.29.2 命令报文

IMPORT SM2 KEY命令报文格式代码见表C.94。

表C.94 IMPORT SM2 KEY 命令报文格式

代码	值
CLA	80/84
INS	C2
P1	见表 C.95
P2	00 导入公钥；01 导入私钥
Lc	数据长度
DATA	见 C.29.3
Le	无

P1 参数说明见表 C.95。

表C.95 IMPORT SM2 KEY 命令的 P1 参数说明

b7	b6	b5	b4	b3	b2	b1	b0	说明
0								明文导入
1								密文导入
	0							小端序模式
	1							大端序模式

表C.95 （续）

b7	b6	b5	b4	b3	b2	b1	b0	说明
		×	×	×	×			会话密钥索引
							0	SM2 签名密钥对
							1	SM2 加密密钥对

C.29.3 命令报文数据域

命令报文数据域包含公钥或私钥文件FID以及公私钥参数见表C.96、C.97、C.98、C.99。若P1.b7=0，则公私钥参数是明文;若P1.b7=1,则公私钥参数值由事先导入的对称会话密钥加密导入,但Tag和Length字段是明文。MAC值是使用由应用维护密钥产生的过程密钥对命令报文计算生成。

表C.96 IMPORT SM2 KEY 命令对应的公钥文件 FID 数据元格式

T	L	V
0xC0	0x02	公钥文件 FID，FID=0x0000 时使用临时公钥

表C.97 IMPORT SM2 KEY 命令对应的私钥文件 FID 数据元格式

T	L	V
0xC2	0x02	私钥文件 FID

表C.98 IMPORT SM2 KEY 命令对应的公私钥参数明文数据元格式

T	L	V
0xCA	0x40	公钥
0xCB	0x20	私钥

表C.99 IMPORT SM2 KEY 命令对应的公私钥参数密文数据元格式

T	L	V
0xCA	密文长度（明文需要填充）	公钥密文（大端序模式）
0xCB	密文长度（明文需要填充）	私钥密文（大端序模式）

C.29.4 响应数据域

IMPORT SM2 KEY无响应报文数据域。

C.29.5 响应报文状态字

IMPORT SM2 KEY命令执行返回的状态字见表C.100。

表C.100 IMPORT SM2 KEY 命令报文执行返回的状态字

SW1	SW2	说明
90	00	命令正确执行

表C.100 （续）

SW1	SW2	说明
67	00	Lc 错误
69	87	MAC 缺失
69	88	MAC 错误
6A	80	数据域的参数错误
6A	81	使用条件不满足
6A	86	P1 或者 P2 错误
6A	88	未找到引用数据
6D	00	指令不支持
6E	00	CLA 错误
93	03	应用被永久锁定

C.30 导出公钥命令（EXPORT PUBLIC KEY）

C.30.1 定义和范围

EXPORT PUBLIC KEY命令导出指定公钥，应使用指定方法或指定私钥对该公钥进行保护。

使用条件如下：

a) 满足公钥文件的读权限；

b) 满足指定私钥文件的使用权限。

C.30.2 命令报文

EXPORT PUBLIC KEY命令报文代码见表C.101。

表C.101 EXPORT PUBLIC KEY 命令报文代码

代码	值
CLA	80
INS	C9
P1	数字签名算法，见表 C.102
P2	见表 C.103
Lc	数据域长度
DATA	见 C.30.3
Le	00 或返回数据实际长度

P1参数说明见表C.102。

表C.102 EXPORT PUBLIC KEY 命令的 P1 参数说明

b7	b6	b5	b4	b3	b2	b1	b0	说明
1								导出 SM2 公钥
0	x 0 0 1	x 0 1 0						数字签名计算模式 对公钥签名导出 对公钥和卡内随机数签名导出 对公钥和卡内随机数 HASH 导出 （此情况不考虑 bit0~2）
			x 0	x 0	x 0	x 1	x 0	数字签名算法: SM2
注1：表中所述公钥值：SM2公钥为64字节公钥值 注2：卡内随机数为FID=0X3000内的128字节随机数，将其附在公钥后进行计算								

P2参数说明见表C.103。

表C.103 EXPORT PUBLIC KEY 命令的 P2 参数说明

b7	b6	b5	b4	b3	b2	b1	b0	说明
1								第二次命令，无命令数据域，响应数据为公钥参数数据
0								第一次命令，有命令数据域，响应数据为数字签名数据或 HASH 数据。SM2 签 X+Y
	x 0	x 0	x 0	x 0	x 0	x 0	x 0	Hash 算法 SM3

C.30.3 命令报文数据域

命令报载文数据域为公钥文件FID数据元和私钥文件FID数据元(均不为0),见表C.104、表C.105。

表C.104 EXPORT PUBLIC KEY 命令对应的公钥文件标识符数据元格式

T	L	V
0xC0	0x02	公钥文件 FID

表C.105 EXPORT PUBLIC KEY 命令对应的私钥文件标识符数据元格式

T	L	V
0xC2	0x02	私钥文件 FID

C.30.4 响应数据域

响应数据域包括公钥数据元和数字签名数据元，见表C.106、表C.107、表108。

表C.106 EXPORT PUBLIC KEY 命令对应的 SM2 公钥参数数据元格式

T	L	V
0xC3	0x40	SM2 公钥值（大端序模式）

表C.107 EXPORT PUBLIC KEY 命令对应的 Sm2 数字签名数据元格式

T	L	V
0xC1	0x40	SM2 数字签名

表C.108 EXPORT PUBLIC KEY 命令对应的 Sm3 Hash 数据元格式

T	L	V
0xC1	0x20	SM2 Hash 数据

C.30.5 响应报文状态字

EXPORT PUBLIC KEY命令的状态字如表C.109所示。

表C.109 EXPORT PUBLIC KEY 命令报文响应状态字

SW1	SW2	说明
90	00	命令正确执行
67	00	Lc 错误
6A	80	数据域的参数错误
6A	81	使用条件不满足
6A	86	P1 或者 P2 错误
6A	88	未找到引用数据
6D	00	指令不支持
6E	00	CLA 错误
93	03	应用被永久锁定

C.31 验证证书命令（VERFIY CERT DATA）

C.31.1 定义和范围

VERFIY CERT DATA命令用于验证并导入人员签名证书和人员加密证书。本指令为可选指令。

C.31.2 命令报文

VERFIY CERT DATA命令报文代码见表C.110。

表C.110 VERIFY CERT DATA 命令报文代码

代码	值
CLA	80
INS	C8

表 C.110 （续）

代码	值
P1	见表 C.111
P2	见表 C.112
Lc	数据长度
DATA	见 C.31.3
Le	无

P1参数说明见表C.111。

表C.111 VERIFY CERT DATA 命令的 P1 参数说明

b7	b6	b5	b4	b3	b2	b1	b0	说明
1								下一条命令，命令数据域信息包含证书数据，由 P2 指定证书数据的分块情况
0								第一次命令，命令数据域信息包含 PKI MIC 公钥文件 FID、临时公钥文件 FID、临时私钥文件 FID、用户公钥证书 FID、用户公私钥文件 FID
	x	x	x	x	x	x	x	公钥算法类型
	0	0	0	0	0	0	1	SM2

P2参数说明见表C.112。

表C.112 VERIFY CERT DATA 命令的 P2 参数说明

b7	b6	b5	b4	b3	b2	b1	b0	说明
x	x							证书数据分块：
0	0							首块
0	1							中间块
1	0							最后一块
1	1							RFU
		x	x	x	x	x	x	Hash 算法：
		0	0	0	0	0	1	sm3

C.31.3 命令报文数据域

命令报文数据域包含PKI MIC公钥文件FID、临时公钥文件FID、临时私钥文件FID、用户公钥证书FID、用户公私钥文件FID和证书数据，见表C.113、表C.114、表C.115、表C.116、表C.117。

表C.113 VERIFY CERT DATA 命令对应的 PKI MIC 公钥文件 FID 数据元格式

T	L	V
0xCC	0x02	PKI MIC 公钥文件 FID

表C.114 VERIFY CERT DATA 命令对应的临时公钥文件 FID 数据元格式

T	L	V
0xCD	0x02	临时公钥文件 FID

表C.115 VERIFY CERT DATA 命令对应的临时私钥文件 FID 数据元格式：

T	L	V
0xCE	0x02	临时私钥文件 FID

表C.116 VERIFY CERT DATA 命令对应的用户公钥证书 FID 数据元格式

T	L	V
0xCF	0x06	用户公钥证书 FID、用户公钥文件 FID 和用户私钥文件 FID

表C.117 VERIFY CERT DATA 命令对应的证书数据元格式：

T	L	V
0xC1	0x82XXXX	长度为 XXXX 字节的证书

C.31.4 响应数据域

响应报文无数据域。

C.31.5 响应报文状态字

VERFIY CERT DATA命令执行返回的状态字见表C.118。

表C.118 VERIFY CERT DATA 命令执行返回的状态字

SW1	SW2	说明
90	00	命令正确执行
67	00	Lc 错误
6A	80	数据域的参数错误
6A	81	使用条件不满足
6A	86	P1 或者 P2 错误
6A	88	未找到引用数据
6D	00	指令不支持
6E	00	CLA 错误
93	03	应用被永久锁定

C.32 写教育电子证件命令（WRITE DIPLOMA）

C.32.1 定义和范围

WRITE DIPLOMA命令用于在教育电子证件应用下写入教育电子证件相关信息。

C.32.2 命令报文

WRITE DIPLOMA命令报文代码见表C.119。

表C.119 WRITE DIPLOMA 命令报文代码

代码	值
CLA	00/04
INS	D7
P1	01 电子毕业证/结业证信息；02 电子学位证信息；03 电子毕业/结业证版式文件 PDF 信息（可选）；04 电子学位证版式信息（可选）；其他保留
P2	00
Lc	数据长度
DATA	见 C.32.3
Le	无

C.32.3 命令报文数据域

数据域格式采用TLV结构： 0x54+文件偏移字节长度+文件偏移 +0x53+待写入数据长度 +待写入数据。

C.32.4 响应报文数据域

WRITE DIPLOMA命令无响应数据。

C.32.5 响应报文的状态字

WRITE DIPLOMA命令执行返回的状态字见表C.120。

表C.120 WRITE DIPLOMA 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
65	81	内存失败（修改失败）
67	00	长度错误（Lc 域为空）
69	81	文件类型错误
69	82	不满足安全状态
69	87	安全报文数据项丢失（需要线路保护更新而采用明文更新方式时）
69	88	安全报文数据项不正确
6A	80	数据域不正确
6A	81	不支持此功能
6A	82	未找到文件
6A	84	文件中存储空间不够

表C.120 （续）

SW1	SW2	说明
6B	00	参数错误(偏移地址超出了 EF)
93	03	应用永久锁定

C.33 读教育电子证件命令（READ DIPLOMA）

C.33.1 定义和范围

READ DIPLOMA命令用于读取教育电子证件应用下的相关信息。

C.33.2 命令报文

READ DIPLOMA命令报文代码见表C.121。

表C.121 READ DIPLOMA 命令报文代码

代码	值
CLA	00
INS	B1
P1	01 电子毕业/结业证信息；02 电子学位证信息；03 电子毕业/结业证版式文件 PDF 信息（可选）；04 电子学位证版式信息（可选）；其他保留
P2	00
Lc	数据长度
DATA	见 C.33.3
Le	期望读取的数据长度

C.33.3 命令报文数据域

数据域格式采用TLV结构： 0x54+文件偏移字节长度+文件偏移。

C.33.4 响应报文数据域

成功的READ DIPLOMA命令的响应报文的数据域包含教育电子证件应用下的相关信息。

C.33.5 响应报文的状态字

READ DIPLOMA命令执行返回的状态字见表C.122。

表C.122 READ DIPLOMA 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功
69	81	不是二进制文件
69	82	读的条件不满足
67	00	长度错误
6A	82	文件未找到

表C.122 （续）

SW1	SW2	说明
6A	86	参数 P1/P2 不正确
69	85	使用条件不满足
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误
6B	00	参数错误(偏移地址超出了 EF)
6C	XX	长度错误（Le 错误；XX 为实际长度）

C.34 禁止修改教育电子证件命令（DISABLE DIPLOMA MODIFIED）

C.34.1 定义和范围

DISABLE DIPLOMA MODIFIED命令用于禁止修改教育卡内的信息，即用于设置教育卡为只读模式。该指令执行后教育卡中的数据文件不能进行修改更新。

C.34.2 命令报文

DISABLE DIPLOMA MODIFIED命令报文代码见表C.123。

表C.123 DISABLE DIPLOMA MODIFIED 命令报文代码

代码	值
CLA	00
INS	44
P1	00
P2	00
Lc	00
DATA	无数据域
Le	无

C.34.3 命令报文数据域

DISABLE DIPLOMA MODIFIED命令报文中没有数据域。

C.34.4 响应报文数据域

DISABLE DIPLOMA MODIFIED命令没有响应数据域。

C.34.5 响应报文的状态字

DISABLE DIPLOMA MODIFIED命令执行返回的状态字见表C.124。

表C.124 DISABLE DIPLOMA MODIFIED 命令执行返回的状态字

SW1	SW2	说明
90	00	命令执行成功

表C.124 （续）

SW1	SW2	说明
69	81	不是二进制文件
69	82	读的条件不满足
69	86	不满足命令执行的条件（未选择任何 EF，而使用当前文件方式操作）
67	00	长度错误
6A	82	文件未找到
6A	86	参数 P1/P2 不正确
69	85	使用条件不满足
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误
6B	00	参数错误(偏移地址超出了 EF)
6C	XX	长度错误（Le 错误；XX 为实际长度）

附 录 D
（规范性附录）
安全报文

D.1 安全报文格式

本部分的安全报文应符合GB/T 16649.4-2010。当命令中CLA字节的低半字节为4，命令使用安全报文格式。

D.2 安全机制

报文的完整性和鉴别（包括命令中的数据域部分）是使用MAC技术机制实现。MAC是对报文中所有的数据元（包括命令头）进行计算。

D.3 MAC长度和位置

MAC是命令数据域中最后的4个字节数据元。

D.4 MAC密钥生成

D.4.1 安全报文以及外部认证过程密钥计算方法

过程密钥输入数据为8字节的卡片随机数补8字节“0000000000000000”达到16字节，通过对过程密钥输入数据做SM4对称加密运算来产生过程密钥。

加密密钥是“应用密文密钥SM4密钥”。

D.4.2 联机交易相关的AC、ARPC、MAC的过程密钥计算方法

交易认证命令、联机圈存命令与联机消费命令中的过程密钥使用 SM4 算法生成，步骤如下：

将当前的ATC在其左边用十六进制数字0填充到8个字节记为数据源A，将当前的ATC异或十六进制值FFFF后在其左边用十六进制数字0填充到8个字节记为数据源B，将数据源A和数据源B串连，用选定的密钥对该数据作加密运算产生过程密钥。

加密密钥是“应用密文密钥SM4密钥”。

D.5 MAC计算

对于命令中需要加密的数据，在加密以后再计算MAC。

使用SM4算法计算MAC的步骤如下：

a)步骤1：初始值为16字节全零（或随机数）；

b)步骤2：下列数据按顺序排列得到一个数据块D：

1）CLA、INS、P1、P2 和 Lc（Lc 的长度包括 MAC 的长度）；

2）命令数据域中的明文或密文数据（若存在）。

c)步骤3：将上述数据块D分成16字节长的数据块D1、D2、D3...最后一块数据块的字节长度为1到16；

d)步骤4：

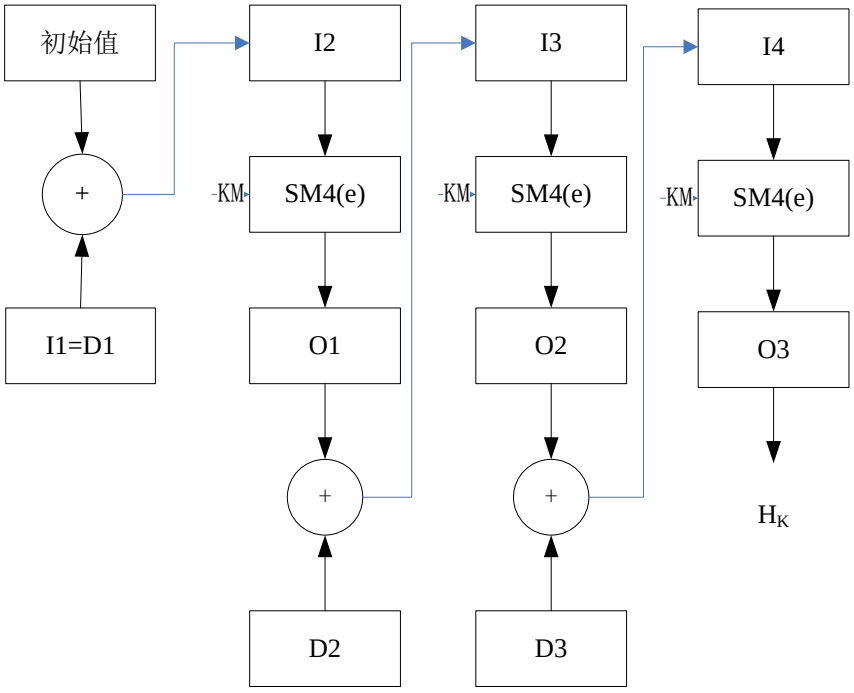
1）若最后一块数据块的长度为 16 字节，后面补 16 字节数据块：80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00，执行步骤 5；

2）若最后一块数据块的长度小于 16 字节，后面补一个字节 80，若长度到 16 字节，执行步骤 5。若仍然不够 16 字节，补 00 直到 16 字节；

e)步骤5：用指定MAC密钥对数据块进行加密；

f)步骤6：取计算结果HK按4字节左右异或得到4字节MAC值。

MAC计算过程如图D.1所示。



说明：

I = 输入　　D = X = 数据块

SM4(e)= SM4算法（加密模式）　　KM = MAC密钥

O = 输出　　+ = 异或

图 D.1 使用 SM4 算法计算 MAC

附 录 E
（规范性附录）
应用密文和授权响应密文生成方法

E.1 概述

AC和ARPC均使用SM4算法加密生成。

E.2 数据元

生成AC的数据元见表E.1。

表E.1 数据元

数据元	来自终端的数据	卡片内数据
交易金额	√	
终端机编号	√	
交易日期（主机）	√	
交易时间（主机）	√	
应用处理计数器		√
ARPC		√

E.3 应用密文生成流程

AC 生成流程如图 E.1 所示。

a)步骤 1：终端将表 E.1 中指定的终端数据通过联机消费/联机圈存命令传送给卡片。

b)步骤 2：生成密文的数据块：

1)生成应用密文命令中送进卡片的数据；

2)卡片内部数据。

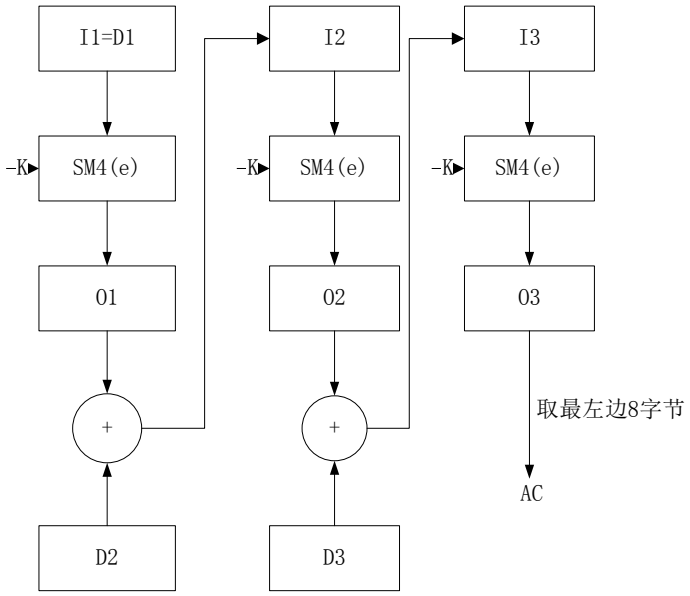
c)步骤 3：将上述数据块分成 16 字节一组：D1、D2、D3.....

d)步骤 4：

1) 若最后一块数据块的长度为 16 字节，后面补 16 字节数据块：80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00；

2) 若最后一块数据块的长度小于 16 字节，后面补一个字节 80，若仍然不够 16 字节，补 00 直到 16 字节。

e)步骤 5：使用过程密钥（由卡片中应用密文密钥分散生成）加密，取加密运算结果的左边 8 字节作为 AC。



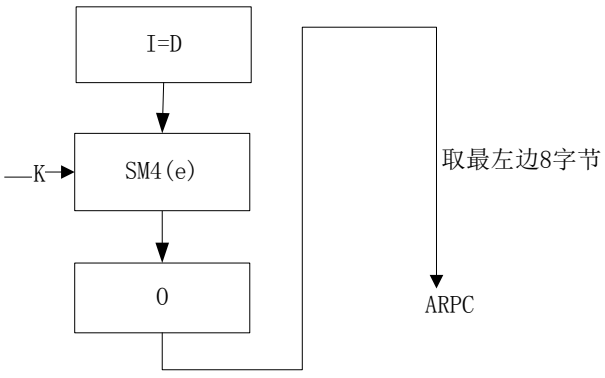
说明：

I = 输入　　D = 数据块
SM4(e)= SM4算法（加密模式）　　K = 密钥
O = 输出　　+ = 异或

图 E.1 用 SM4 算法生成 AC

E.4　生成ARPC

卡片在收到TRANS AUTHENTICATE命令时，生成一个ARPC和命令中传送进来的ARPC进行比较。使用SM4算法，生成ARPC的流程如图E.2所示。



说明：

I = 输入　　D = 数据块
SM4(e)= SM4算法（加密模式）　　K = 密钥
O = 输出

图 E.2 用 SM4 算法生成 ARPC

a)步骤1：将获取随机数命令返回的卡片8字节随机数和交易类型授权码按顺序连接，并在后面补7字节的00，得到一个16字节的数据块D1；

b)步骤 2：使用过程密钥（由卡片中应用密文密钥分散生成）加密，取加密运算结果的的左边 8 字节作为 ARPC。

附 录 F
（规范性附录）
卡面规范信息

F.1 卡面规范概述

本附录定义了对学生卡、教师卡、毕业生卡的卡面规范要求。

F.2 卡片尺寸

学生卡、教师卡、毕业生卡的卡片尺寸符合 GB/T 14916-2006 的 ID-1 型卡的规定。

F.3 卡面要素及布局

F.3.1 学生卡

F.3.1.1 学生卡正面要素及布局

学生卡正面的信息要素应包括：主标识、教育卡类型标识、教育卡卡发行单位名称标识三个区域。各信息要素的布局如图F.1所示。

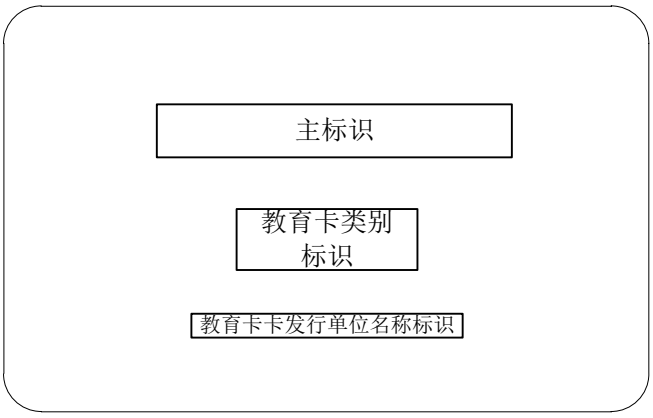


图 F.1 学生卡正面要素布局

各区域的文字内容、字体格式、位置要求见表F.1。

表F.1 学生卡正面要素要求

区域	文字内容	字体格式	区域位置要求
主标识	中华人民共和国	字体：方正大标宋简体 字号：17.75pt 色值：K：100	区域尺寸：42.7mm×5.8mm 上边缘与卡片上边缘的距离为 11.3mm 左边缘与卡片左边缘的距离为 21.45mm

表F.1 （续）

区域	文字内容	字体格式	区域位置与尺寸
教育卡类别标识	学生卡	字体：方正大标宋简体 字号：21.5pt 色值：K：100	区域尺寸：22.3mm×7.1mm 上边缘与卡片上边缘的距离为22.9mm 左边缘与卡片左边缘的距离为31.65mm
教育卡卡发行单位名称标识	教育卡卡发行单位的名称	字体：方正宋黑简体 字号：6pt 色值：K：100	区域宽度最大值：42.7mm，左右居中对齐 上边缘与卡片上边缘的距离为38mm

学生卡正面的信息要素及布局示例如图F.2所示。

图 F.2 学生卡正面要素布局示例图

F.3.1.2 学生卡背面要素及布局

学生卡背面的信息要素应包括持卡人信息、持卡人照片、ESN标识三个区域。各信息要素的布局如图F.3所示。

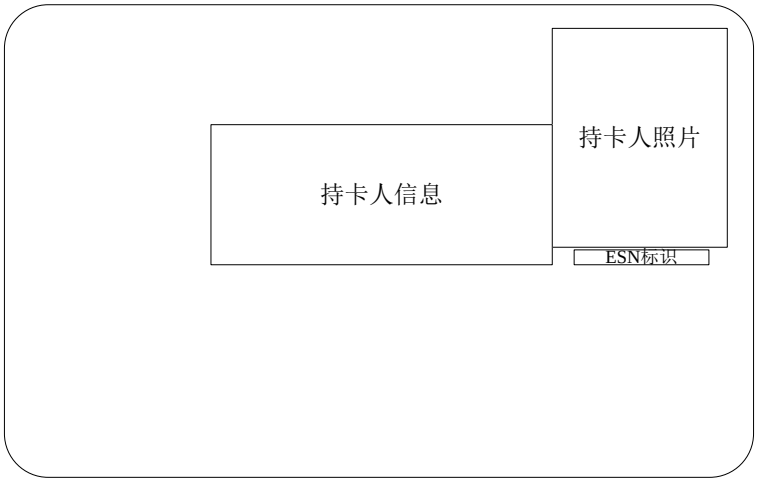


图 F.3 学生卡背面要素布局

各区域的要素描述、位置要求见表F.2。

表F.2　学生卡背面要素要求

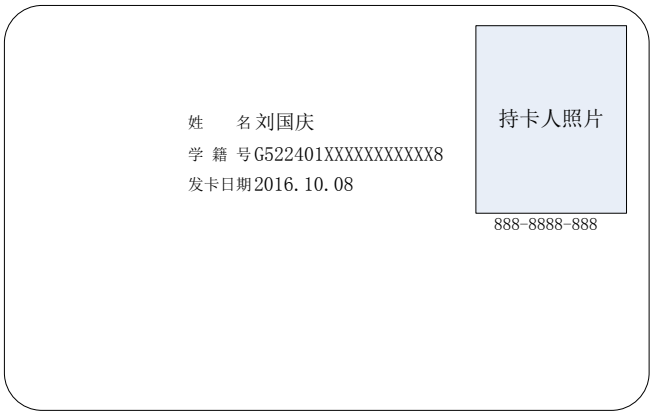
区域	内容	标准
持卡人信息	持卡人姓名、学籍号、发卡日期	区域尺寸：36.3mm×16.5mm 上边缘与卡片上边缘的距离为13.85mm 左边缘与卡片左边缘的距离为23.7mm
持卡人照片	持卡人照片	区域尺寸：20mm×25mm 上边缘与卡片上边缘的距离为3mm 右边缘与卡片右边缘的距离为3mm
ESN标识	持卡人的ESN	区域尺寸：15.2mm×1.64mm 上边缘与卡片上边缘的距离为29mm 右边缘与卡片右边缘的距离为5.35mm

持卡人信息包括：姓名标识、姓名、学籍号标识、学籍号、发卡日期标识、发卡日期等要素。学生卡背面文字的字体格式如表F.3所示。

表F.3　学生卡背面文字字体格式

标识区域	要素	字体	字号	色值
持卡人信息	姓名标识	方正黑体简体	6pt	K：100
	姓名	黑体，加粗0.25pt	7.5pt	K：100
	学籍号标识	方正黑体简体	6pt	K：100
	学籍号	黑体，加粗0.25pt	7.5pt	K：100
	发卡日期标识	方正黑体简体	6pt	K：100
	发卡日期	黑体，加粗0.25pt	6pt	K：100
教育电子身份号	教育电子身份号	方正黑体简体	6.5pt	K：100

学生卡背面要素及布局示例如图F.4所示。



图F.4 学生卡背面要素布局示例图

F.3.2　教师卡

F.3.2.1　教师卡正面要素及布局

教师卡正面的信息要素应包括：主标识、教育卡类型标识、教育卡卡发行单位名称标识三个区域。各信息要素的布局如图F.5所示。

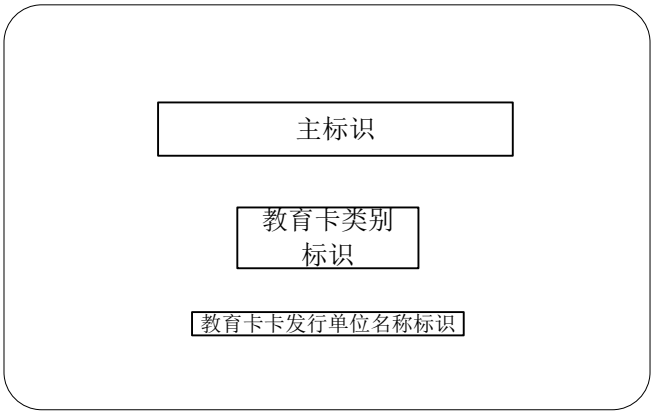


图 F.5 教师卡正面要素布局

各区域的文字内容、字体格式、位置要求见表F.4。

表F.4　教师卡正面信息要素要求

区域	文字内容	字体格式	区域位置与尺寸
主标识	中华人民共和国	字体：方正大标宋简体 字号：17.75pt 色值：K：100	区域尺寸：42.7mm×5.8mm 上边缘与卡片上边缘的距离为 11.3mm 左边缘与卡片左边缘的距离为 21.45mm
教育卡类别标识	教师卡	字体：方正大标宋简体 字号：21.5pt 色值：K：100	区域尺寸：22.3mm×7.1mm 上边缘与卡片上边缘的距离为 22.9mm 左边缘与卡片左边缘的距离为 31.7mm
教育卡卡发行单位名称标识	教育卡卡发行单位的名称	字体：方正宋黑简体 字号：6pt 色值：K：100	区域宽度最大值：42.7mm，左右居中对齐 上边缘与卡片上边缘的距离为 38mm

教师卡正面的信息要素及布局示例如图F.6所示。

图 F.6 教师卡正面要素布局示例图

F.3.2.2　教师卡背面要素及布局

教师卡背面的信息要素应包括持卡人信息、持卡人照片、ESN标识三个区域。各信息要素的布局图F.7所示。

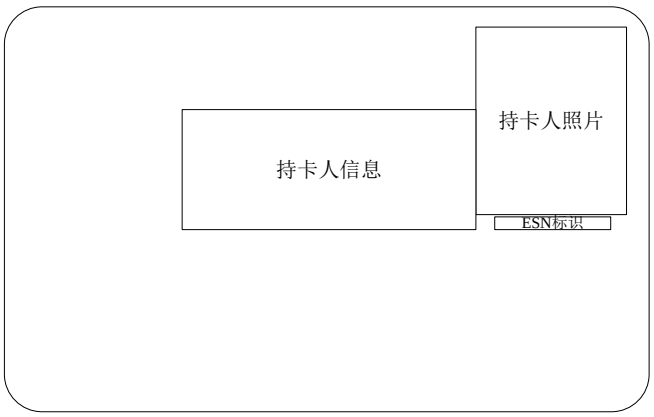


图 F.7 教师卡背面要素布局

各区域的要素描述、位置要求见表F.5。

表F.5　教师卡背面要素要求

区域	内容	标准
持卡人信息	持卡人姓名、教职工号、发卡日期	区域尺寸：36.3mm×16.5mm 上边缘与卡片上边缘的距离为 13.85mm 左边缘与卡片左边缘的距离为 23.7mm
持卡人照片	持卡人照片	区域尺寸：20mm×25mm 上边缘与卡片上边缘的距离为 3mm 右边缘与卡片右边缘的距离为 3mm
ESN 标识	持卡人的 ESN	区域尺寸：15.2mm×1.64mm 上边缘与卡片上边缘的距离为 29mm 右边缘与卡片右边缘的距离为 5.35mm

持卡人信息包括：姓名标识、姓名、教职工号标识、教职工号、发卡日期标识、发卡日期等要素。

教师卡背面文字的字体格式如表F.6所示。

表F.6　教师卡背面文字字体格式

标识区域	要素	字体	字号	色值
持卡人信息	姓名标识	方正黑体简体	6pt	K：100
	姓名	黑体，加粗 0.25pt	7.5pt	K：100
	教职工号标识	方正黑体简体	6pt	K：100
	教职工号	黑体，加粗 0.25pt	7.5pt	K：100
	发卡日期标识	方正黑体简体	6pt	K：100
	发卡日期	黑体，加粗 0.25pt	6pt	K：100
教育电子身份号	教育电子身份号	方正黑体简体	6.5pt	K：100

教师卡背面要素及布局示例如图F.8所示。

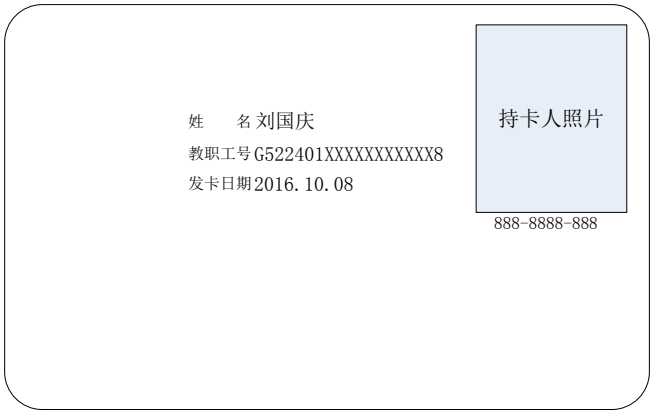


图 F.8 教师卡背面要素及布局示例图

F.3.3　毕业生卡

F.3.3.1　毕业生卡正面要素及布局

毕业生卡正面的信息要素应包括：主标识、教育卡类别标识、教育卡卡发行单位名称标识三个区域。各信息要素的布局如图F.9所示。

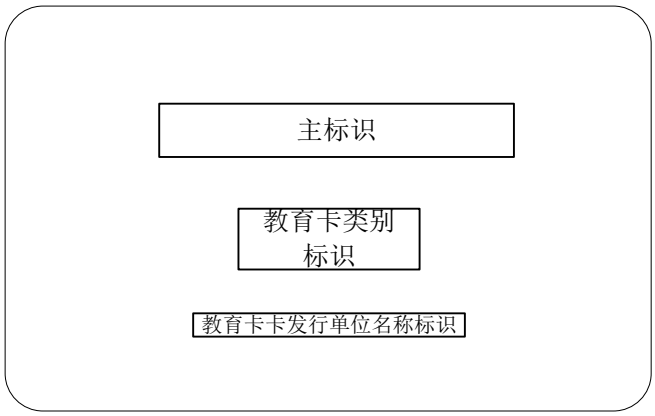


图 F.9 毕业生卡正面要素布局

各区域的文字内容、字体格式、位置要求见表F.7。

表F.7　毕业生卡正面要素要求

区域	文字内容	字体格式	区域位置与尺寸
主标识	中华人民共和国	字体：方正大标宋简体 字号：17.75pt 色值：K：100	区域尺寸：42.7mm×5.8mm 上边缘与卡片上边缘的距离为 11.3mm 左边缘与卡片左边缘的距离为 21.45mm
教育卡类别标识	毕业生卡	字体：方正大标宋简体 字号：21.5pt 色值：K：100	区域尺寸：29.8×7.1mm 上边缘与卡片上边缘的距离为 22.9mm 左边缘与卡片左边缘的距离为 27.7mm
教育卡卡发行单位名称标识	教育卡卡发行单位的名称	字体：方正宋黑简体 字号：6pt 色值：K：100	区域宽度最大值：42.7mm，左右居中对齐 上边缘与卡片上边缘的距离为 38mm

毕业生卡正面的信息要素及布局示例如图F.10所示。

图 F.10 毕业生卡正面要素布局示例图

F.3.3.2 毕业生卡背面要素及布局

毕业生卡背面的信息要素应包括持卡人信息、持卡人照片、ESN标识等三个区域。各信息要素的布局如图F.11所示。

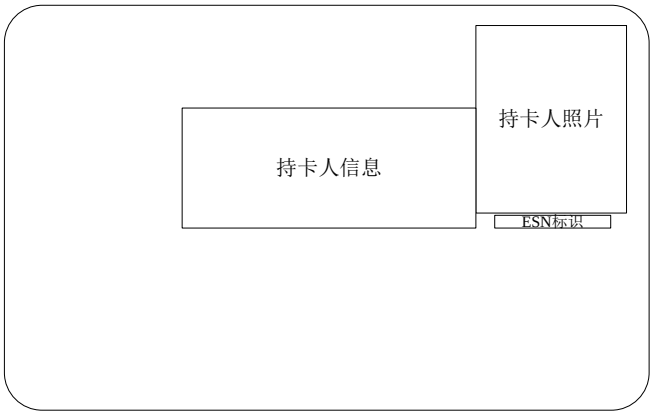


图 F.11 毕业生卡背面要素位置布局

各区域的要素描述、位置要求见表F.8。

表F.8 毕业生卡背面要素要求

区域	内容	标准
持卡人信息	持卡人姓名、学籍号、学历、毕业日期	区域尺寸：36.3mm×16.5mm 上边缘与卡片上边缘的距离为 13.85mm 左边缘与卡片左边缘的距离为 23.7mm
持卡人照片	持卡人照片	区域尺寸：20mm×25mm 上边缘与卡片上边缘的距离为 3mm 右边缘与卡片右边缘的距离为 3mm
ESN 标识	持卡人的 ESN	区域尺寸：15.2mm×1.64mm 上边缘与卡片上边缘的距离为 29mm 右边缘与卡片右边缘的距离为 5.35mm

持卡人信息包括：姓名标识、姓名、学籍号标识、学籍号、学历标识、学历、毕业日期标识、毕业日期等要素。

毕业生卡背面文字的字体格式如表F.9所示。

表F.9　毕业生卡背面文字字体格式

标识区域	要素	字体	字号	色值
持卡人信息	姓名标识	方正黑体简体	6pt	K：100
	姓名	黑体，加粗 0.25pt	7.5pt	K：100
	学籍号标识	方正黑体简体	6pt	K：100
	学籍号	黑体，加粗 0.25pt	7.5pt	K：100
	学历标识	方正黑体简体	6pt	K：100
	学历	黑体，加粗 0.25pt	6pt	K：100
	毕业年月标识	方正黑体简体	6pt	K：100
	毕业年月	黑体，加粗 0.25pt	6pt	K：100
教育电子身份号	教育电子身份号	方正黑体简体	6.5pt	K：100

毕业生卡背面要素及布局示例如图F.12所示。

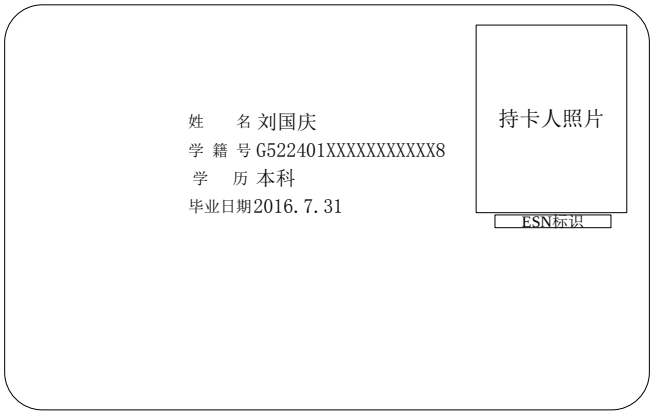


图 F.12 毕业生卡背面要素及布局示例图

附 录 G
（规范性附录）
算法标识

G.1 公钥算法标识

本部分使用的公钥签名算法标识见表G.1。

表G.1 公钥签名算法标识

公钥签名算法标识	签名算法	对应哈希算法
04	SM2（数字签名算法）	SM3

本部分使用的公钥加密算法标识见表G.2。

表G.2 公钥加密算法标识

公钥加密算法标识	加密算法
04	SM2（公钥加密算法）

G.2 哈希算法标识

本部分使用的哈希算法标识见表G.2。

表G.3 哈希算法标识

哈希算法标识	哈希算法
07	SM3

G.3 对称密钥算法标识

表G.4列出了本部分使用的对称密钥算法标识：

表G.4 对称密钥算法标识

对称密钥算法标识	对称密钥算法
04	SM4

G.4 椭圆曲线参数标识

表G.5列出了本部分使用的椭圆曲线参数标识：

表G.5 椭圆曲线参数标识

算法类型	强度	曲线	公钥长度	曲线类型	曲线标识
SM2	素数域 256 位		64 字节		11

附 录 H
（规范性附录）
C/S 应用接口函数规范

H.1 基本数据类型

本部分中的字节数组均为大端序模式存储和交换。基本数据类型定义如表 H.1 所示：

表H.1 基本数据类型定义

类型名称	描述	定义
INT8	有符号 8 位整数	
INT16	有符号 16 位整数	
INT32	有符号 32 位整数	
UINT8	无符号 8 位整数	
UINT16	无符号 16 位整数	
UINT32	无符号 32 位整数	
BOOL	布尔类型，取值为 TRUE 或 FALSE	
BYTE	字节类型，无符号 8 位整数	typedef UINT8 BYTE
CHAR	字符类型，无符号 8 位整数	typedef UINT8 CHAR
SHORT	短整数，有符号 16 位	typedef INT16 SHORT
USHORT	无符号 16 位整数	typedef UINT16 USHORT
LONG	长整数，有符号 32 位整数	typedef INT32 LONG
ULONG	长整数，无符号 32 位整数	typedef UINT32 ULONG
UINT	无符号 32 位整数	typedef UINT32 UINT
WORD	字类型，无符号 16 位整数	typedef UINT16 WORD
DWORD	双字类型，无符号 32 位整数	typedef UINT32 DWORD
FLAGS	标志类型，无符号 32 位整数	typedef UINT32 FLAGS
LPSTR	8 位字符串指针,按照 UTF8/UTF16 格式存储及交换	typedef CHAR * LPSTR
HANDLE	句柄，指向任意数据对象的起始地址	typedef void * HANDLE
HEDUCARD	句柄，指向任意数据对象的起始地址	typedef void * HANDLE

H.2 连接管理类

H.2.1 连接管理类函数名称与功能

连接管理类函数名称与功能见表H.2。

表H.2 连接管理类函数

函数名称	功能	备注
Connect	连接指定教育卡	
DisConnect	断开当前教育卡	

H.2.2 Connect

函数原型BOOL Connect（IN DWORD dwPort，OUT HEDUCARD *phEduCard）
功能描述　连接至指定的教育卡，可以用于判断教育卡是否与终端连接。
参数　dwPort：指定连接终端的端口
phEduCard：指向教育卡的句柄
输出　R_OK：连接教育卡成功
R_FAIL：检测教育卡失败
备注　使用教育卡前，应在先调用该函数

H.2.3 DisConnect

函数原型　BOOL DisConnect（IN HEDUCARD hEduCard）
功能描述　断开当前连接的教育卡。
参数　hEduCard：连接教育卡的句柄
输出　R_OK：断开成功
R_FAIL：断开失败
备注　执行该函数前应先成功调用Connect

H.3 设备操作类

H.3.1 设备操作类函数名称与功能

设备操作类函数名称与功能见表H.3。

表H.3 设备操作类函数

函数名称	功能	备注
GetKeyParam	获取教育卡信息	
SetKeyParam	设置教育卡信息	

H.3.2 GetKeyParam

函数原型　DWORD GetKeyParam（IN HEDUCARD hEduCard,
IN DWORD dwType,
OUT BYTE *pbData,
IN OUT DWORD *pdwDataLen）
功能描述　根据输入的参数类型dwType，返回相应的教育卡的参数信息。
参数　hEduCard：连接教育卡的句柄
dwType：获得信息类型
pData:输出的教育卡相关参数信息指针

pdwDataLen:输出教育卡相关参数信息长度

输出　R_OK：正确
R_BAD_TYPE：输入的信息类型错
R_NO_EDUCARD：没有检测到教育卡存在
R_BUFFER_TOO_SMALL：缓冲区太小
R_BAD_FLAG：无效的FLAG值
R_FAIL：函数调用失败

H.3.3 SetKeyParam

函数原型　DWORD SetKeyParam（IN HEDUCARD hEduCard,
IN DWORD dwType,
IN BYTE *pbData,
IN DWORD *pdwDataLen）

功能描述　根据输入的dwType类型，以及相应的教育卡信息pData，以及信息长度pdwDataLen，设置EDUCARD信息。

参数　hEduCard：连接教育卡的句柄
dwType：获得信息类型
pData：要设置的教育卡信息
pdwDataLen：教育卡信息长度

输出　R_OK：正确
R_BAD_TYPE：输入的信息类型错
R_NO_EDUCARD：没有检测到教育卡存在
R_BAD_FLAG：无效的FLAG值
R_FAIL：函数调用失败

H.4 PIN管理类

H.4.1 PIN管理类函数名称与功能

PIN管理类函数名称与功能见表H.4。

表H.4 PIN管理类函数

函数名称	功能	备注
ChangePin	修改PIN	
VerifyPin	验证PIN	
UnLockPin	解锁PIN	

H.4.2 ChangePin

函数原型　DWORD ChangePin(IN HEDUCARD hEduCard,
IN BYTE *pbOldPin,
IN DWORD dwOldPinLen,
IN BYTE *pbNewPin,
IN DWORD dwNewPinLen,

IN DWORD dwFlag)

功能描述　修改教育卡的PIN码。

参数　hEduCard：连接教育卡的句柄
pbOldPin：改变之前的PIN码
dwOldPinLen：改变之前的PIN码长度
pbNewPin：改变之后的PIN码
dwNewPinLen：改变之后的PI码值长度
dwFlag：用户标志

输出　R_OK：正确
R_NO_EDUCARD：没有检测到教育卡的存在
R_BAD_FLAG：无效的用户标识
R_FAIL：函数调用失败

H.4.3 VerifyPin

函数原型　DWORD VerifyPin(IN HEDUCARD hEduCard,
IN BYTE *pbPin,
IN DWORD dwPinLen,
IN DWORD dwFlag)

功能描述　根据用户的类型dwFlag以及输入的PIN来验证用户的身份。

参数　hEduCard：连接教育卡的句柄
pbPin：输入的待验证的PIN码
dwPinLen： PIN码长度
dwFlag：用户标识

输出　R_OK：正确
R_NO_EDUCARD：没有检测到教育卡的存在
R_BAD_FLAG：无效的用户标识
R_FAIL：函数调用失败

H.4.4 UnLockPin

函数原型　DWORD UnLockPin(IN HEDUCARD hEduCard,
IN BYTE *pbUnLockPin,
IN DWORD dwUnLockPinLen,
IN BYTE *pbNewPin,
IN DWORD dwNewPinLen)

功能描述　此函数为管理员用函数，管理员通过输入解锁PIN码，将教育卡的PIN码设置为新的值。

参数　hEduCard：连接教育卡的句柄
pbUnLockPin：解锁PIN码
dwUnLockPinLen：解锁PIN码的长度
pbNewPin：新的用户PIN码
dwNewPinLen：新的用户PIN码长度

输出　R_OK：正确
R_NO_EDUCARD：没有检测到教育卡的存在

R_FAIL：函数调用失败

H.5 文件管理类

H.5.1 文件管理类函数名称与功能

文件管理类函数名称与功能见表H.5。

表H.5 文件操作类函数

函数名称	功能	备注
CreateUserFile	创建用户文件	
ReadUserFile	读用户文件	
WriteUserFile	写用户文件	
ListUserFile	列出设备中的用户文件	
GetUserFileLength	获取文件长度	
DeleteUserFile	删除用户文件	

H.5.2 CreateUserFile

函数原型　DWORD CreateUserFile(IN HEDUCARD hEduCard,
IN CHAR *pszFileID,
IN DWORD dwSize,
IN DWORD dwFlags,
OUT HUSERFILE *phFile)

功能描述　建立文件号为pszFileID的文件，文件大小为dwSize。

参数　hEduCard：连接教育卡的句柄
pszFileID：文件ID
dwSize：文件字节大小
dwFlags:文件属性标识
phFile：所建立文件的句柄

输出　R_OK：正确
R_USER_PIN_ERROR：PIN码错误
R_FILE_ALREADY_EXIST：文件已存在
R_BAD_FLAG：错误的文件属性
R_FAIL：函数调用失败

H.5.3 ReadUserFile

函数原型　DWORD ReadUserFile(IN HUSERFILE hFile,
OUT BYTE *pbData,
IN OUT DWORD *pdwDataLen)

功能描述　从文件句柄对应的文件中读出文件数据到pbData中。

参数　phFile：返回用户文件句柄
pbData：存储文件中的数据
pdwDataLen：文件中数据长度

输出　　R_OK：正确
R_USER_PIN_ERROR：PIN码错误
R_BAD_HANDLE：错误的句柄
R_FAIL：函数调用失败

H.5.4 WriteUserFile

函数原型　　DWORD WriteUserFile(IN HUSERFILE hFile,
IN BYTE *pbData,
IN OUT DWORD *pdwDataLen)
功能描述　　在文件句柄为hFile的文件中，写入文件数据pbData，长度为pdwDataLen。
参数　　phFile：用户文件句柄
pbData：要写入的数据
pdwDataLen：数据长度
输出　　R_OK：正确
R_USER_PIN_ERROR：PIN码错误
R_BAD_HANDLE：错误的句柄
R_FAIL：函数调用失败

H.5.5 ListUserFile

函数原型　　DWORD ListUserFile(IN HEDUCARD hEduCard,
OUT CHAR *pszFileList,
IN OUT DWORD *pdwFileListLen)
功能描述　　列出指定设备中的用户文件名。
参数　　hEduCard：设备句柄
pbFileList：文件名列表，每个文件之间以ASCII码0x02间隔
pdwFileListLen：文件名列表长度
输出　　R_OK：正确
R_FAIL：函数调用失败

H.5.6 GetUserFileLength

函数原型　　DWORD GetUserFileLength(IN HEDUCARD hEduCard,
IN HUSERFILE hFile,
OUT DWORD *pdwFileLen)
功能描述　　得到指定文件的长度。
参数　　hFile：文件句柄
pdwFileLen：返回文件长度
输出　　R_OK：正确
R_USER_PIN_ERROR：PIN码错误
R_BAD_HANDLE：错误的句柄
R_FAIL：函数调用失败

H.5.7 DeleteUserFile

函数原型　DWORD DeleteUserFile（IN HUSERFILE hFile ）
功能描述　删除指定的用户文件。
参数　hFile：文件句柄
输出　R_OK：正确
R_USER_PIN_ERROR：PIN码错误
R_BAD_HANDLE：错误的句柄
R_NOT_EXIST：文件不存在
R_FAIL：函数调用失败

H.6　容器管理类

H.6.1　容器管理类函数名称与功能

容器管理类函数名称与功能见表 H.6。

表H.6　容器管理类函数

函数名称	功能	备注
CreateContainer	创建容器	
DeleteContainer	删除容器	
QueryContainerParam	获取容器信息	

H.6.2　CreateContainer

函数原型　DWORD CreateContainer(IN HEDUCARD hEduCard,
IN CHAR *pszContainerName,
OUT HCONTAINER *phContainer,
DWORD dwFlags)
功能描述　创建容器。
参数　hEduCard：设备句柄
pszContainerName：容器名称
phContainer：创建的容器句柄
dwFlags:容器属性标识
输出　R_OK：正确
R_NO_EDUCARD：没有卡片
R_FAIL：函数调用失败

H.6.3　DeleteContainer

函数原型　DWORD DeleteContainer(IN HEDUCARD hEduCard, IN CHAR *pszContainerName)
功能描述　删除指定名称的容器。
参数　hEduCard：设备句柄
pszContainerName:容器名
输出　R_OK：正确
R_NO_EDUCARD：没有卡片
R_USER_PIN_ERROR：错误的PIN码

R_FAIL：函数调用失败

H.6.4 QueryContainerParam

函数原型　DWORD QueryContainerParam(HCONTAINER hContainer,
DWROD dwParam,
OUT BYTE *pbData,
IN OUT DWORD *pdwDataLen)

功能描述　得到指定容器句柄对应的容器信息。

参数　hContainer：容器句柄
dwParam:容器属性标识
pbData：容器信息
pdwDataLen：容器信息长度

输出　R_OK：正确
R_NO_EDUCARD：没有卡片
R_NO_CONTAINER：容器不存在
R_USER_PIN_ERROR：PIN码错误
R_FAIL：函数调用失败

H.7 密钥管理类

H.7.1 密钥管理类函数名称与功能

密钥管理类函数与功能见表H.7。

表H.7 密钥管理类函数

函数名称	功能	备注
GetRand	产生随机数	
GenPKIKey	产生 PKI 密钥对	
ExportPKIKey	导出 PKI 公钥	
ImportPKIKey	导入 PKI 非对称密钥对	

H.7.2 GetRand

函数原型　DWORD GetRand(IN HEDUCARD hEduCard,
IN OUT BYTE *pbRand,
IN DWORD dwRandLen)

功能描述　产生随机数。

参数　hEduCard：设备句柄
pbRand：随机数地址
dwRandLen：要产生的随机数的长度

输出　R_OK：正确
R_NO_EDUCARD：没有卡片
R_FAIL：函数调用失败

H.7.3 GenPKIKey

函数原型　DWORD GenPKIKey (IN HEDUCARD hEduCard,
IN LONG nAlg,
IN CHAR *pszContainerName,
IN DWORD dwFlag)

功能描述　创建非对称密钥对。

参数　hEduCard：设备句柄
nAlg：算法类型，1-SM2
pszContainerName:容器名
dwFlag：密钥对类型标志：1-签名密钥对，2-加密密钥对。

输出　R_OK：正确
R_NO_EDUCARD：没有卡片
R_NO_CONTAINER：容器不存在
R_USER_PIN_ERROR：PIN码错误
R_FAIL：函数调用失败

H.7.4 ExportPKIKey

函数原型　DWORD ExportPKIKey (IN HEDUCARD hEduCard,
IN LONG nAlg,
IN CHAR *pszContainerName,
OUT BYTE *pbKeyData,
IN OUT DWORD *pdwKeyDataLen,
IN DWORD dwFlag)

功能描述　导出非对称密钥对中的公钥。

参数　hEduCard：设备句柄
nAlg：算法类型，1-SM2
pszContainerName:容器名
pbKeyData：导出的公钥数据
pdwKeyDataLen：导出的公钥数据长度
dwFlag：密钥对类型标志，1-签名公钥，2-加密公钥

输出　R_OK：正确
R_NO_EDUCARD：没有卡片
R_NO_CONTAINER：容器不存在
R_BUFFER_TOO_SMALL：缓冲区太小
R_USER_PIN_ERROR：PIN码错误
R_FAIL：函数调用失败

H.7.5 ImportPKIKey

函数原型　DWORD ImportPKIKey (IN HEDUCARD hEduCard,
IN LONG nAlg,
IN CHAR *pszContainerName,
IN BYTE *pbKeyData,

IN OUT DWORD *pdwKeyDataLen,
IN DWORD dwFlag)

功能描述　导入非对称密钥对。

参数　hEduCard：设备句柄
nAlg：算法类型，1-SM2
pszContainerName：容器名
pbKeyData：导出的公钥数据
pdwKeyDataLen：导出的公钥数据长度
dwFlag：密钥对类型标志，1-签名公钥，2-加密公钥

输出　R_OK：正确
R_NO_EDUCARD：没有卡片
R_NO_CONTAINER：容器不存在
R_BUFFER_TOO_SMALL：缓冲区太小
R_USER_PIN_ERROR：PIN码错误
R_FAIL：函数调用失败

H.8　密码运算类

H.8.1　密码运算类函数名称与功能

密码运算类函数名称与功能见表H.8。

表H.8　密码运算类函数

函数名称	功能	备注
SymCrypt	对称密钥算法加密	
SessionCrypt	会话密钥进行对称密钥算法加密	
SymDeCrypt	对称密钥算法解密	
SessionDeCrypt	会话密钥进行对称密钥算法解密	
PKICrypt	非对称密钥算法加密	
PKIDeCrypt	非对称密钥算法解密	
SignData	数字签名	
VerifyHashSign	数字签名验证	
HashData	计算散列	请补充

H.8.2　SymCrypt

函数原型　DWORD SymCrypt(IN HSYMKEY hSymKey,
IN OUT BYTE *pbData,
IN OUT DWORD *pdwDataLen)

功能描述　使用普通密钥进行对称密钥算法加密。

参数　hSymKey：加密密钥

dwAlgType：对称密钥算法类型，4-SM4算法。
pbData：待加密数据/加密以后的数据
pdwDataLen：待加密数据长度/加密后数据长度

输出　*pbData：待加密数据/加密以后的数据
dwDataLen：待加密数据长度/加密后数据长度

返回值　R_OK：正确
R_FAIL：函数调用失败

H.8.3 SessionCrypt

函数原型　DWORD SessionCrypt(HSESSIONKEY hSessionKey,
IN OUT BYTE *pbData,
IN OUT DWORD *dwDataLen,)

功能描述　使用会话密钥进行对称加密算法加密

参数　hSessionKey: 会话密钥
dwAlgType：对称密钥算法类型，4-SM4算法。
pbData：待加密数据/加密以后的数据
dwDataLen：待加密数据长度/加密后数据长度

输出　pbData：待加密数据/加密以后的数据
dwDataLen：待加密数据长度/加密后数据长度

返回值　R_OK：正确
R_FAIL：函数调用失败

H.8.4 SymDeCrypt

函数原型　DWORD SymDeCrypt(IN HSYMKEY hSymKey
IN DWORD dwAlgType,
IN OUT BYTE *pbData,
IN OUT DWORD *pdwDataLen)

功能描述　使用普通密钥进行对称解密算法加密。

参数　hSymKey：加密密钥
pbData：待加密数据/加密以后的数据
dwAlgType：对称密钥算法类型，4-SM4算法
pdwDataLen：待加密数据长度/加密后数据长度

输出　pbData：待加密数据/加密以后的数据
pdwDataLen：待加密数据长度/加密后数据长度

返回值　R_OK：正确
R_FAIL：函数调用失败

H.8.5 SessionDeCrypt

函数原型　DWORD SessionDeCrypt(HSESSIONKEY hSessionKey,
IN OUT BYTE *pbData,
IN OUT DWORD *pdwDataLen)

功能描述　使用会话密钥进行对称解密算法加密
参数　hSessionKey：加密的会话密钥秘文
dwAlgType：对称密钥算法类型，4-SM4算法。
pbData：待加密数据/加密以后的数据
pdwDataLen：待加密数据长度/加密后数据长度
输出　pbData：待加密数据/加密以后的数据
dwDataLen：待加密数据长度/加密后数据长度
返回值　R_OK：正确
R_FAIL：函数调用失败

H.8.6 PKICrypt

函数原型　DWORD PKICrypt(IN LONG nAlg,
IN HCONTAINER hContainer,
IN OUT BYTE *pbData,
IN OUT DWORD dwDataLen,
IN DWORD dwFlag)
功能描述　使用SM2算法加密信息
参数　hContainer：容器句柄
pbData：待加密数据/加密后的数据
dwDataLen：待加密数据长度/加密后数据长度
dwFlag：标志位，1-签名密钥对，2-加密密钥对
输出　pbData：加密后的数据
dwDataLen：加密后数据的长度
返回值　R_OK：正确
R_FAIL：函数调用失败

H.8.7 PKIDeCrypt

函数原型　DWORD PKIDeCrypt(IN HCONTAINER hContainer,
OUT BYTE *pbData,
IN OUT DWORD dwDataLen,
IN DWORD dwFlag)
功能描述　使用SM2解密数据
参数　hContainer：容器句柄
pbData：待加密数据/加密后的数据
dwDataLen：待加密数据长度/加密后数据长度
dwFlag：标志位，1-签名密钥对，2-加密密钥对
输出　pbData：解密后的数据
dwDataLen：解密后数据的长度
返回值　R_OK：正确
R_FAIL：函数调用失败

H.8.8 SignData

函数原型　DWORDSignData(IN HEDUCARD hEduCard,
IN CHAR *pszContainerName,
IN BYTE *pbInData,
IN DWORD dwInDataLen,
OUT BYTE *pbOutData,
OUT DWORD *pdwOutDataLen)

功能描述　对指定数据先散列再签名。

参数　hEduCard：设备句柄
pszContainerName：容器名
*pbInData：源数据值
dwInDataLen：源数据长度
*pbOutData：签名后的数据
*pdwOutDataLen：签名后数据长度

输出　R_OK：正确
R_NO_EDUCARD：没有卡片
R_USER_PIN_ERROR：PIN码错误
R_FAIL：函数调用失败

H.8.9 VerifyHashSign

函数原型　DWORD VerifyData(IN HEDUCARD hEduCard,
IN BYTE *pbCertData,
IN DWORD dwCertDataLen,
IN BYTE *pbSrcData,
IN DWORD dwSrcDataLen,
IN BYTE *pbDestData,
IN DWORD dwDestDataLen)

功能描述　验证签名。

参数　hEduCard：设备句柄
*pbCertData：证书数据
dwCertDataLen：证书数据长度
pbSourceData：源数据值
dwSrcDataLen：源数据长度
pbDestData：签名后的数据
dwDestDataLen：签名后数据长度。

输出　R_OK：正确
R_NO_EDUCARD：没有卡片
R_VERIFY_FAIL：验证失败
R_FAIL：函数调用失败

H.9 证书管理类

H.9.1 证书管理类函数名称与功能

证书管理类函数与功能见表 H.9。

表H.9 证书管理类函数

函数名称	功能	备注
ExportCertData	读证书数据	
ImortCertData	写证书数据	

H.9.2 ExportCertData

函数原型 DWORD ExportCertData (IN HEDUCARD hEduCard,
IN CHAR *pszContainerName,
OUT BYTE *pbCertData,
IN OUT DWORD *pdwCertDataLen,
IN DWORD dwCertFlag)

功能描述 读取证书数据。

参数 hEduCard：设备句柄。
pszContainerName：容器名
pbCertData：证书数据
pdwCertDataLen：证书数据长度
dwCertFlag：证书类型，1-签名证书，2-加密证书

输出 R_OK：正确
R_NO_EDUCARD：没有卡片
R_BAD_FLAG：证书类型错误
R_FAIL：函数调用失败

H.9.3 ImortCertData

函数原型 DWORD WriteCertData(IN HEDUCARD hEduCard,
IN CHAR *pszContainerName,
IN CHAR *pbCertData,
IN OUT DWORD *pdwCertDataLen,
IN DWORD dwCertFlag)

功能描述 写证书数据。

参数 hEduCard：设备句柄
pszContainerName：容器名
pbCertData：证书数据
pdwCertDataLen：证书数据长度
dwCertFlag：证书类型，1-签名证书，2-加密证书

输出 R_OK：正确
R_NO_EDUCARD：没有卡片
R_BAD_FLAG：证书类型错误
R_FAIL：函数调用失败

附 录 I
（规范性附录）
B/S 应用接口函数规范

I.1 基本数据类型

本附录中的字节数组均为大端序模式存储和交换。基本数据类型定义如表I.1所示：

表 I. 1 基本数据类型

类型名称	描述	定义
BOOL	布尔类型，取值为 TRUE 或 FALSE	
LONG	长整数，有符号 32 位整数	typedef INT32 LONG
BSTR	字符串	

I.2 连接管理类

I.2.1 连接管理类函数名称与功能

连接管理类函数名称与功能见表I.2。

表 I. 2 连接管理类函数

函数名称	功能	备注
Connect	教育卡连接	
DisConnect	教育卡断开	

I.2.2 Connect

函数原型　BOOL Connect(BSTR szEduCardName)
功能描述　是否插入了教育卡。
参数　szEduCardName：[IN]连接名
返回值　TURE：表示成功
FALSE：表示失败

I.2.3 DisConnect

函数原型　BOOLDisConnect(BSTR szEduCardName)
功能描述　断开相应教育卡的连接。
参数　szEduCardName：[IN]连接名
返回值　TURE：表示成功
FALSE：表示失败

I.3 设备管理类

I.3.1 设备管理类函数名称与功能

设备管理类函数与名称见表I.3。

表 I. 3 设备管理类函数

函数名称	功能	备注
GetEduCardSerialNum	获取教育卡序列号	

I.3.2 GetEduCardSerialNum

函数原型　BOOL GetEduCardSerialNum()
功能描述　获取教育卡序列号。Data1为序列号。
参数　无
返回值　TURE：表示成功
FALSE：表示失败

I.4 容器管理类

I.4.1 容器管理类函数名称与功能

容器管理类函数名称与功能见表I.4。

表 I. 4 容器管理类函数

函数名称	功能	备注
CreateContainer	创建容器	
ExistContainer	检测容器是否存在	

I.4.2 CreateContainer

函数原型　BOOLCreateContainer(BSTR szContainerName)
功能描述　创建容器。
参数　szContainerName：[IN]容器名称
返回值　TURE：表示成功
FALSE：表示失败

I.4.3 ExistContainer

函数原型　BOOL ExistContainer(BSTR szContainerName)
功能描述　检测容器是否存在。
参数　szContainerName：[IN]容器名称
返回值　TURE：表示成功
FALSE：表示失败

I.5 密钥管理类

I.5.1 密钥管理类函数名称与功能

密钥管理类函数名称与功能见表I.5。

表 I. 5 密钥管理类函数

函数名称	功能	备注
GetRand	产生随机数	
GenPKIKey	生成非对称密钥对	
ExportPKIKey	导出非对称密钥对中的公钥	
ImportPKIKey	密文导入密钥对	
ImportEduCardData	导入签名、加密密钥对和证书	

I.5.2 GetRand

函数原型　BOOLGetRand(LONG pRDataLen)
功能描述　产生随机数。Data1为已Base64编码的随机数。
参数　pRDataLen：[IN]随机数长度
返回值　TURE：表示成功
FALSE：表示失败

I.5.3 ExportPKIKey

函数原型　BOOL ExportPKIKey(LONG nAlg,
LONG dwFlag,
BSTR pszContainerName)
功能描述　导出非对称密钥对中的公钥。Data1为已Base64编码的公钥数据。
参数　nAlg：[IN]算法类型：1-SM2
dwFlag ：[IN]公钥类型：1-签名公钥，2-加密公钥
pszContainerName：[IN]容器名称
返回值　TURE：表示成功
FALSE：表示失败

I.5.4 ImportPKIKey

函数原型　BOOL ImportPKIKey(LONG nAlg,
LONG dwFlag,
BSTRszContainerName,
BSTR szKeyData)
功能描述　导入公钥。
参数　nAlg：[IN]算法类型：1-SM2
dwFlag：[IN]密钥对类型：1-签名密钥对，2-加密密钥对
szContainerName：[IN]容器名称
szKeyData：[IN]密文密钥对，已编码
返回值　TURE：表示成功

FALSE：表示失败

I.5.5 GenPKIKey

函数原型 BOOLGenPKIKey (LONG nAlg,
LONG nFlag,
BSTR szContainerName)
功能描述 生成非对称密钥对。
参数 nAlg：[IN]算法类型：1-SM2
nFlag：[IN]密钥对类型：1-签名密钥对，2-加密密钥对
szContainerName：[IN]容器名称
返回值 TURE：表示成功
FALSE：表示失败

I.5.6 ImportEduCardData

函数原型 BOOL ImportEduCardData(BSTRszContainerName,
BSTR szSessionKey,
BSTR szCryptKey,
BSTR szCryptCert,
BSTR szSignCert)
功能描述 导入签名、加密密钥对和证书。
参数 szContainerName：[IN]容器名称
szSessionKey：[IN]密文会话密钥，已编码
szCryptKey：[IN]密文加密密钥对和签名密钥对，已编码
szCryptCert：[IN]加密证书，已编码
szSignCert：[IN]签名证书，已编码
返回值 TURE：表示成功
FALSE：表示失败

I.6 密码运算类

I.6.1 密码运算类函数名称与功能

密码运算类函数名称与功能见表I.6。

表 I. 6 密码运算类函数

函数名称	功能	备注
UKAsymCrypt	非对称加密	
AsymDeCrypt	非对称解密	
SymCrypt	对称加密	
SymDeCrypt	对称解密	
SignData	数字签名	
VerifyData	验证签名	

I.6.2 AsymCrypt

函数原型　BOOLAsymCrypt(LONG nAlg,
LONG dwFlags,
BSTR pszContainerName,
BSTR szCertData,
BSTR szData,
LONG dwArithFlag)

功能描述　非对称加密。Data1为已base64编码的加密数据。

参数　nAlg：[IN]算法类型：1-SM2
dwFlags：[IN]加密类型：1-签名，2-加密
pszContainerName：[IN]容器名称
szCertData：[IN]证书数据，已编码，若为空，则使用容器里的证书
szData：[IN]待加密的数据，已编码
dwArithFlag：[IN]算法标识，保留

返回值　TURE：表示成功
FALSE：表示失败

I.6.3 AsymDeCrypt

函数原型　BOOLAsymDeCrypt(LONG nAlg,
LONG dwFlag,
BSTR pszContainerName,
BSTR szData,
LONG dwArithFlag)

功能描述　非对称解密。Data1为已base64编码的解密后的数据。

参数　nAlg：[IN]算法类型：1-SM2
dwFlag：[IN]加密类型：1-签名，2-加密
pszContainerName：[IN]容器名称
szData：[IN]加密后的数据，已编码
dwArithFlag：[IN]算法标识，保留

返回值　TURE：表示成功
FALSE：表示失败

I.6.4 SymCrypt

函数原型　BOOLSymCrypt(LONG dwFlags, BSTR szPaws, BSTR szData)

功能描述　对称加密。Data1为已base64编码的加密数据。

参数　dwFlags：[IN]算法类型：4-SM4
szPaws：[IN]对称密钥，已编码
szData：[IN]待加密的数据

返回值　TURE：表示成功
FALSE：表示失败

I.6.5 SymDeCrypt

函数原型　BOOLSymDeCrypt(LONG nAlgType,
BSTR szPaws,
BSTR szData)
功能描述　对称解密。Data1为解密后的明文数据。
参数　nAlgType：[IN]算法类型：4-SM4
szPaws：[IN]对称密钥，已编码
szData：[IN]加密后数据，已编码
返回值　TURE：表示成功
FALSE：表示失败

I.6.6 SignData

函数原型　BOOLSignData(LONG nAlg,
BSTR pszContainerName,
BSTR pbInData)
功能描述　数据签名。Data1为已base64编码的签名后的数据。
参数　nAlg：[IN]算法类型：1-SM2
pszContainerName：[IN]容器名称
pbInData：[IN]待签名的数据，未编码
返回值　TURE：表示成功
FALSE：表示失败

I.6.7 VerifyData

函数原型　BOOLVerifyData(LONG nAlg,
BSTR szCertData,
BSTR pbSrcData,
BSTR szDestData,
LONG nCertFlag)
功能描述　验证签名。
参数　nAlg：[IN]算法类型：1-SM2
szCertData：[IN]证书数据
pbSrcData：[IN]待签名的数据，未编码
szDestData：[IN]签名后的数据，已编码
nCertFlag：[IN]数据编码类型：0-Base64编码，1-PEM编码
返回值　TURE：表示成功
FALSE：表示失败

I.7 证书管理类

I.7.1 证书管理类函数名称与功能

证书管理类函数与功能见表I.7。

表 I. 7 证书管理类函数

函数名称	功能	备注
ReadCertData	读取证书数据	
WriteCertData	写入证书数据	
GetEduCardCertInfo	获取 EDUCARD 证书信息	

I.7.2 ReadCertData

函数原型　BOOLReadCertData(LONG nAlg,
LONG dwCertFlag,
BSTR pszContainerName)

功能描述　读取证书数据。Data1为已base64编码的证书数据。

参数　nAlg：[IN]算法类型：1-SM2
dwCertFlag：[IN]证书类型：1-签名证书，2-加密证书
pszContainerName：[IN]容器名称

返回值　TURE：表示成功
FALSE：表示失败

I.7.3 WriteCertData

函数原型　BOOLWriteCertData(LONG nAlg,
LONG dwCertFlag,
BSTR pszContainerName,
BSTR szCertData,
LONG nCertDataType)

功能描述　写入证书数据。

参数　nAlg：[IN]算法类型：1-SM2
dwCertFlag：[IN]证书类型：1-签名证书，2-加密证书
pszContainerName：[IN]容器名称
szCertData：[IN]证书数据，已编码
nCertDataType：[IN]数据编码类型：0-Base64编码，1-PEM编码

返回值　TURE：表示成功
FALSE：表示失败

I.7.4 GetEduCardCertInfo

函数原型　BOOLGetEduCardCertInfo(LONG dwCertFlag,
LONG dwDataFlag,
BSTR szContainerName)

功能描述　获取教育卡内证书信息。Data1为证书信息标识所属的信息。

参数　dwCertFlag：[IN]证书类型：1-签名证书，2-加密证书
dwDataFlag：[IN]证书信息标识：0-颁发者，1-授权者，2-有效起始时间，3-有效终止时间，4-版本，5-序列号，6-颁发者信息，17-公钥，18-签名算法，19-主题密钥标志符，20-颁发机构密钥标志符，21-密钥用法，22-基本限制

szContainerName：[IN]容器名称

返回值　　TURE：表示成功

FALSE：表示失败

I.8　输出数据类

I.8.1　输出数据类函数名称与功能

输出数据类函数与功能见表I.8。

表 I. 8 输出数据类函数

函数名称	功能	备注
DataLen1	获取第一个返回值数据长度	
DataLen2	获取第二个返回值数据长度	
Data1	获取第一个返回值数据	
Data2	获取第二个返回值数据	

I.8.2　DataLen1

函数原型　　LONG DataLen1()

功能描述　　获取第一个返回值数据长度。

参数　　无

返回值　　第一个返回值数据长度

I.8.3　DataLen2

函数原型　　LONG DataLen2()

功能描述　　获取第二个返回值数据长度。

参数　　无

返回值　　第二个返回值数据长度

I.8.4　Data1

函数原型　　BSTR Data1()

功能描述　　获取第一个返回值数据。

参数　　无

返回值　　第一个返回值数据

I.8.5　Data2

函数原型　　BSTR Data2()

功能描述　　获取第二个返回值数据。

参数　　无

返回值　　第二个返回值数据