ICS 35.240.01
L 67

团　体　标　准

T/ZSPH-XXX XXXX

智能门锁近场通信应用技术要求

Technical requirements of smart lock NFC application

2021-**-**发布　　2021-**-** 实施

中关村乐家智慧居住区产业技术联盟 发布

目　　次

前　　言

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

本文件由中关村乐家智慧居住区产业技术联盟提出并归口。

本文件起草单位：

本文件主要起草人：

智能门锁近场通信(NFC)应用技术要求

1 范围

本文件规定了智能门锁近场通信技术应用中的卡片要求、系统及终端要求、检测要求。

本文件适用于使用近场通信技术的智能门锁和卡片的设计、制造和应用。

2 规范性引用文件

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

GB/T 22186-2016 信息安全技术 具有中央处理器的IC卡芯片安全技术要求

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 0028—2014 密码模块安全技术要求

JR/T 0025.4 中国金融集成电路（IC）卡规范 第4部分：借记/贷记应用规范

JR/T 0025.5 中国金融集成电路（IC）卡规范 第5部分：借记/贷记应用卡片规范

3 术语和定义

3.1

集成电路 integrated circuit（IC）

具有处理和/或储存功能的电子器件。

3.2

集成电路（IC卡） integrated circuit(s) card（ICC）

内部封装一个或多个集成电路用于执行处理和储存功能的卡片。

3.3

SHA-256算法 secure hash algorithm

安全散列算法家族中的一种，256表示其摘要的比特长度。

3.4

AES-128算法 advanced encryption standard

高级加密标准，又称Rijndael加密法，128表示其分组长度。

3.5

Luhn算法 luhn algorithm

一种简单的校验和算法，一般用于验证身份识别码，也称为“模10”算法。

4 缩略语

下列符号和缩略语适用于本文件。

AES 高级加密标准（Advanced Encryption Standard）
AID 应用标识符（Application Identifier）
APDU 应用协议数据单元（Application Protocol Data Unit）
BER 基本编码规则（Basic Encoding Rules）
CA 认证中心（Certificate Authority）
CID 卡片标识符（Card Identifier）
CLA 命令报文的类别字节（Class Byte of the Command Message）
CMAC 基于对称加密算法实现消息认证（Cypher-Based Message Authentication Code）
DDA 动态数据认证（Dynamic Data Authentication）
DF 专用文件（Dedicated File）
FCI 文本控制信息（File Control Information）
GP 全球平台（Global Platform）
HCI 主机控制接口（Host Control Interface）
ICC 集成电路卡片（Integrated Circuit Card）
IIN 发卡方标识代码（Issuer Identification Number）
INS 命令报文的指令字节（Instruction Byte of the Command Message）
KID 密钥标识符（Key Identifier）
Lc 终端发出的命令报文的数据域长度
Le 命令报文响应数据的最大期望长度
MAC 报文鉴别代码（Message Authentication Code）
MF 主控文件（Master File）
NFC 近场通信（Near Field Communication）
NIST 美国国家标准与技术研究院（National Institute of Standards and Technology）
P1 命令报文的参数1（Parameter 1 of the Command Message）
P2 命令报文的参数2（Parameter 2 of the Command Message）
PIN 个人密码（Personal Identification Number）
RFU 保留将来使用（Reserved for Future Use）
RSA Rivest、Sharmir和Adleman提出的一种非对称密钥算法
SHA 安全散列算法（Secure Hash Algorithm）
TLV 标签、长度、值（Tag Length Value）
TSM 可信服务管理（Trusted Service Management）

5 总体架构

智能门锁近场通信应用总体架构见图1,并应符合如下要求：

a） 密钥管理中心负责接收发卡机构的CA公钥，向发卡机构下发卡片认证密钥和发卡机构编码，向系统下发发卡机构CA公钥和卡片认证密钥，向终端下发发卡机构CA公钥和卡片认证密钥；

b） 发卡机构负责向密钥管理中心上送发卡机构 CA 公钥和接收卡片认证密钥、发卡机构编码，使用发卡机构私钥，卡片认证密钥，发卡机构编码对卡片进行预个人化；

c） 系统负责接收密钥管理中心下发的发卡机构 CA 公钥和卡片认证密钥，并在系统授权时使用这些密钥进行系统和卡片的相互认证；

d） 终端负责接收密钥管理中心下发的发卡机构 CA 公钥和卡片认证密钥，并在终端授权时使用这些密钥进行终端和卡片相互认证；

e） 经授权后，用户可以使用卡片在终端上进行识别开锁。

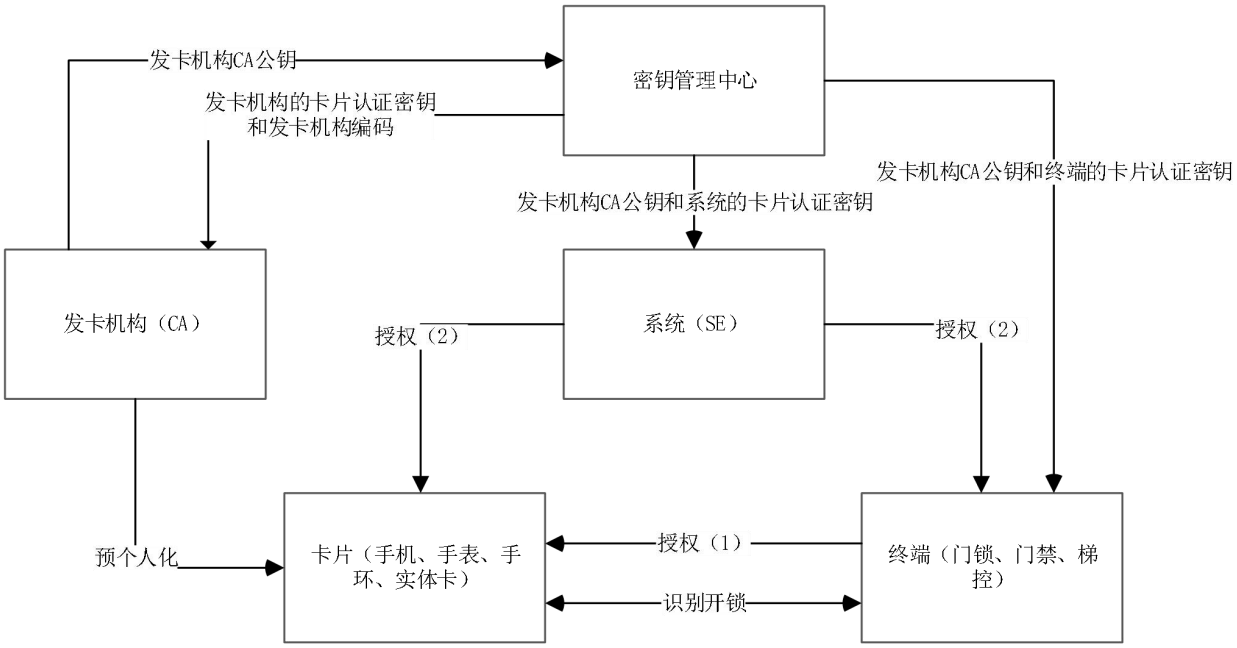

图 1　智能门锁近场通信应用总体架构图

6　卡片要求

6.1　卡片应用生命周期

卡片应用生命周期见图2，并应符合如下要求：

a） 应用实例安装后，进入预个人化状态，状态值为 01；

b） 由 TSM 完成应用实例初始化后，进入个人化状态，状态值为 03；

c） 由系统或终端完成应用实例个人化（即“授权”操作）后，进入用户使用阶段，状态值由 03

d） 转为 07；

e） 状态 07 是正常使用卡片的状态；

f） 在特定的条件下，允许在使用阶段擦除卡片个人化数据，重新进入个人化状态；

g） 生命周期状态值可以从 SELECT 命令的应答数据中获取。

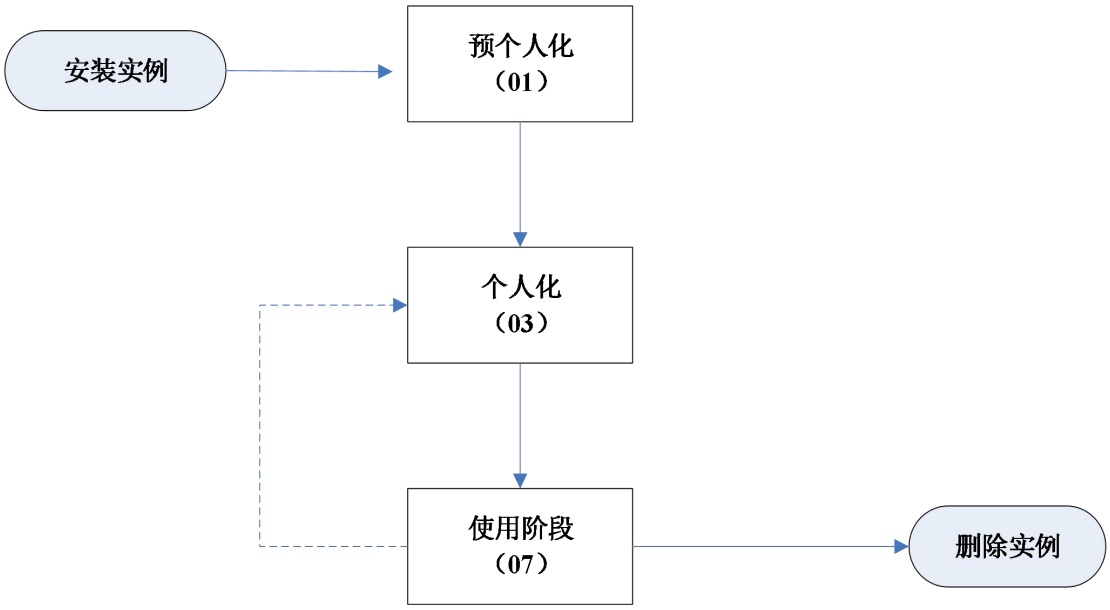

图 2　卡片应用生命周期

6.2　AID

卡片应固定一个 AID，包含固定字节和可变字节，卡片 AID 的格式应符合表 1 的要求：

表 1　卡片 AID

AID 固定字节	AID 可变字节
A0 00 00 00 4E 46 43 4B 43 41	XX YY XX：版本号，取值范围 00~FF YY：用于区分多张卡片，取值范围 00~FF

例：　A0 00 00 00 4E 46 43 4B 43 41 01 01

6.3　CID

每张卡片应有一个唯一的 CID，由 16 个 0~9 的数字组成，最后一个数字为校验位，校验位采用 Luhn 算法。前 6 位数字为发卡机构编码（IIN），可以用来区分不同发卡机构。每个发卡机构可以有多个 IIN，用于发行不同类型的卡片。从 SELECT 命令响应数据和卡片公钥证书中，可以获取 CID。

6.4　证书和密钥

6.4.1　发卡机构认证中心

脱机数据认证需要一个发卡机构认证中心（CA），认证中心拥有高级别安全性的加密设备并用来签发卡片公钥证书，认证中心应支持位数不低于1152的RSA密码算法或SM2密码算法。

6.4.2　认证中心公私钥对

认证中心公私钥对应符合下列要求：

a）　认证中心使用非对称算法产生认证中心公私钥对；

b）　认证中心会产生多个公私钥对，每个公私钥对都将分配一个唯一的认证中心公钥索引；

c）　认证中心私钥由认证中心保管并保证其私密性和安全性；

d） 终端必须有足够空间存放认证中心公钥和认证中心公钥索引；
e） 终端自主决定使用某个认证中心公钥。

6.4.3 卡片公私钥对

卡片公私钥对应符合下列要求：
a） 卡片公私钥对在卡片内生成，公钥可以导出进行证书签发，私钥不允许导出卡片；
b） 在卡片预个人化阶段，由卡片产生卡片公私钥对，卡片私钥存放在卡片中的安全存贮区域；
c） 卡片公钥安全导出后，由认证中心私钥签名，产生卡片公钥证书，并存放在卡片中；
d） 卡片公钥模长必须等于 CA 公钥模长，密码算法应和认证中心密码算法一致；
e） 终端通过认证中心公钥索引定位认证中心公钥，用 CA 公钥从卡片公钥证书恢复卡片公钥，并用卡片公钥验证卡片的动态签名数据。

6.4.4 使用 RSA 进行动态数据验证

6.4.4.1 卡片公钥证书

为了支持动态数据认证，一张卡片应拥有它自己的唯一的公私钥对，公私钥对由一个私有的签名密钥和相对应的公开的验证密钥组成。卡片公钥必须存放在卡片上的公钥证书中。

动态数据认证采用了一个二层的公钥证书方案。每一个卡片公钥由认证中心认证。这表明为了验证卡片的签名，终端需要先通过验证证书来恢复和验证卡片公钥，然后用这个公钥来验证卡片的动态签名。

将认证中心私钥S_{CA}应用到表2中指定的数据，以获得卡片公钥证书。

表 2 由认证中心签名的卡片公钥数据（即哈希算法的输入）

字段名	长度	描述	格式
证书格式	1	十六进制，值为‘04’	b
CID	10	卡片唯一 ID（在右边补上十六进制数‘F’）	cn20
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	3	由认证中心分配给这张证书的的二进制数	b
哈希算法标识	1	标识用于在数字签名方案中产生哈希结果的哈希算法	b
卡片公钥算法标识	1	标识使用在卡片公钥上的数字签名算法	b
卡片公钥长度	2	标识卡片公钥的模的字节长度	b
卡片公钥指数长度	1	标识卡片公钥指数的字节长度	b
卡片公钥或卡片公钥的最左边字节	N_{CA}–55	如果 $N_{IC} \le N_{CA}$–55，这个字段包含了在右边补上了 N_{CA}–55–N_{IC} 个值为‘BB’的字节的整个卡片公钥。 如果 $N_{IC} > N_{CA}$–55，这个字段包含了卡片公钥最高位的 N_{CA}–55 个字节	b
卡片公钥的余项	0 或 N_{IC}–N_{CA}+55	这个字段只有在 $N_{IC} > N_{CA}$–55 时才出现。它包含了卡片公钥最低位的 N_{IC}–N_{CA}+55 个字节	b
卡片公钥指数	1 或 3	卡片公钥指数等于 3 或 2^{16}+1	b

认证中心的公钥有一个N_{CA}个字节的公钥模。认证中心公钥指数必须等于3或2^{16}+1。

卡片的公钥有一个为N_{IC}个字节（$N_{IC} \le N_I \le N_{CA}$）的卡片公钥模。如果$N_{IC}$>（$N_{CA}$-55），那么卡片公钥模被分成两部分，即一部分包含模中最高的N_{CA}-55个字节（卡片公钥中最左边的数字）；另一部分包含剩下的模中最低的N_{IC}-（N_{CA}-55）个字节（卡片公钥余项）。卡片公钥指数必须等于3或2^{16}+1。

为了完成动态数据认证，终端必须首先恢复和验证卡片公钥（这一步叫做卡片公钥认证）。卡片公钥认证需要的所有信息在表3中详细说明，并存放在卡片中。这些信息可以通过读公钥证书（GET ICC CERTIFICATE）命令得到。如果缺少这些数据中的任意一项，那么动态数据认证失败。

表 3　动态认证中的公钥认证所需的数据对象

标签	长度	值	格式
8F	1	认证中心公钥索引	b
9F46	N_{CA}	卡片公钥证书	b
9F48	$N_{IC}-N_{CA}+55$	卡片公钥的余项（如果存在）	b
9F47	1 或 3	卡片公钥指数	b

6.4.4.2　卡片公钥的获取

卡片公钥的获取应符合如下要求：

a） 如果卡片公钥证书的长度不同于在前面的章节中获得的认证中心公钥模长度，那么动态数据认证失败；

b） 为了获得在表 4 中指明的恢复数据，使用 CA 公钥和相应的算法应用到卡片公钥证书上。如果恢复数据的结尾不等于“BC”，那么动态数据认证失败；

c） 检查恢复数据头。如果它不是“6A”，那么动态数据认证失败；

d） 检查证书格式。如果它不是“04”，那么动态数据认证失败；

e） 将表 4 中的第 2 个到第 10 个数据元（即从证书格式直到卡片公钥或卡片公钥的最左边字节）从左到右连接，再把卡片公钥的余项（如果有）和卡片公钥指数加在后面；

f） 把指定的哈希算法（从哈希算法标识得到）应用到上一步的连接结果从而得到哈希结果；

g） 把上一步计算得到的哈希结果和恢复出的哈希结果相比较。如果它们不一样，那么动态数据认证失败；

h） 比较恢复得到的 CID 和从卡片读出的 CID 是否相同。如果不同，那么动态数据认证失败；

i） 检验证书失效日期中指定月的最后日期是否等于或迟于今天的日期。如果不是，那么动态数据认证失败；

j） 如果卡片公钥算法标识无法识别，那么动态数据认证失败；

k） 如果以上所有的检验都通过，连接卡片公钥的最左边字节和卡片公钥的余项（如果有）以得到发卡行公钥模，继续按下章的描述执行实际的动态数据认证。

表 4　从卡片公钥证书恢复数据的格式

字段名	长度	描述	格式
恢复数据头	1	十六进制，值为‘6A’	b
证书格式	1	十六进制，值为‘04’	b
CID	10	卡片唯一标识（在右边补上十六进制数‘F’）	cn20
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	3	由发卡行分配给这张证书的唯一的二进制数	b
哈希算法标识	1	标识用于在数字签名方案中产生哈希结果的哈希算法	b
卡片公钥算法标识	1	标识使用在卡片公钥上的数字签名算法	b
卡片公钥长度	2	标识卡片公钥的模的字节长度	b
卡片公钥指数长度	1	标识卡片公钥指数的字节长度	b
卡片公钥或卡片公	N_{CA}-55	如果 $N_{IC} \le N_{CA}-55$，这个字段包含了在右边补上了	b

钥的最左边字节		N_{CA}–55–N_{IC} 个值为‘BB’的字节的整个卡片公钥。 如果 N_{IC}>N_{CA}-55，这个字段包含了卡片公钥最高位的 N_I–55 个字节	
哈希结果	32	卡片公钥以及相关信息的哈希值	b
恢复数据结尾	1	十六进制，值为‘BC’	b

6.4.4.3 动态签名的生成

动态签名的生成的步骤应符合如下要求：

a） 终端发出内部签名（INTERNAL SIGNATURE）命令，命令中包含终端生成的不可预知数（4 个字节的二进制数）；

b） 卡片使用卡片私钥和相应的算法并对表 5 中指明的数据生成数字签名。这个结果叫做签名的动态应用数据；

c） 卡片动态数据的字节长度为 LDD =4，卡片动态数字是由一个由卡片生成的不可预知数。

表 5 需签名的动态应用数据（即哈希算法的输入）

字段名	长度	描述	格式
签名的数据格式	1	十六进制，值为‘05’	b
哈希算法标识	1	标识用于产生哈希结果的哈希算法	b
卡片动态数据长度	1	标识卡片动态数据的字节长度 L_{DD}	b
卡片动态数据	L_{DD}	由卡片生成的动态数据	-
填充字节	N_{IC}–L_{DD}–37	（N_{IC}- L_{DD}–37）个值为‘BB’的填充字节	b
终端动态数据	4	4 字节不可预知数	b

6.4.4.4 DDA 动态数据验证

DDA动态数据获取应符合如下要求：

a） 如果签名的动态应用数据的长度不同于卡片公钥模的长度，那么动态数据认证失败；

b） 为了获得在表 6 中指明的恢复数据，使用卡片公钥和相应的算法恢复函数应用到签名的动态应用数据上，如果恢复数据的结尾不等于“BC”，那么动态数据认证失败；

c） 检查恢复数据头，如果它不是“6A”，那么动态数据认证失败；

d） 检查签名数据格式，如果它不是“05”，那么动态数据认证失败；

e） 将表 6 中的第 2 个到第 6 个数据元（即从签名数据格式直到填充字节）从左到右连接，并加上终端动态数据；

f） 把指定的哈希算法（从哈希算法标识得到）应用到上一步的连接结果从而得到哈希结果；

g） 把上一步计算得到的哈希结果和恢复出的哈希结果相比较。如果它们不一样，那么动态数据认证失败；

h） 如果以上所有的步骤都成功，那么动态数据认证成功。

表 6 从签名的动态应用数据恢复的数据格式

字段名	长度	描述	格式
恢复数据头	1	十六进制，值为‘6A’	b
签名数据格式	1	十六进制，值为‘05’	b
哈希算法标识	1	标识用于在数字签名方案中产生哈希结果的哈希算法	b
卡片动态数据长度	1	标识卡片动态数据的字节长度	b

卡片动态数据	L_{DD}	由卡片生成的动态数据	-
填充字节	N_{IC}-L_{DD}–37	（N_{IC}-L_{DD}–37）个值为‘BB’的填充字节	b
哈希结果	32	动态应用数据以及相关信息的哈希值	b
恢复数据结尾	1	十六进制，值为‘BC’	b

6.4.5 使用 SM2 进行动态数据验证

6.4.5.1 卡片公钥证书

认证中心使用认证中心私钥 S_{CA}，对表 7 中指明的数据使用 SM2 算法进行签名，得到格式如表 8 所示的卡片公钥证书。

表 7 由认证中心签名的卡片公钥数据（待签名数据）

字段名	长度	描述	格式
证书格式	1	十六进制，值为‘14’	b
CID	10	卡片唯一 ID（在右边补上十六进制数‘F’）	cn20
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	3	由认证中心分配给这张证书的的二进制数	b
哈希算法标识	1	标识用于在数字签名方案中产生哈希结果的哈希算法	b
卡片公钥签名算法标识	1	标识使用在卡片公钥上的数字签名算法。SM2 算法为‘04’	b
卡片公钥加密算法标识	1	标识使用在 IC 卡公钥上的加密算法，暂不使用，取值‘00’	b
卡片公钥参数标识	1	用于标识椭圆曲线，同时确定 N_{IC}	b
卡片公钥长度	1	标识卡片公钥的字节长度	b
卡片公钥	N_{IC}	如果卡片公钥算法标识对应于 SM2，该字段为椭圆曲线上的一个点	b

表 8 动态认证中的公钥认证所需的数据对象

标签	长度	值	格式
8F	1	认证中心公钥索引	b
9F46	N_{IC}	卡片公钥证书	b

6.4.5.2 卡片公钥的获取

终端获取的 IC 卡公钥证书数据如表 9 所示。IC 卡公钥以明文形式包含在 IC 卡公钥证书中，终端用认证中心的公钥验证 IC 卡公钥证书中的签名字段。如验证通过，则从 IC 卡公钥证书中提取公钥信息。

验证步骤如下：

a） 获取并解析如表 9 所示的经过卡片公钥证书数据。如果失败，则动态数据认证失败；

b） 检查证书格式的值。如果不是“14”，那么动态数据认证失败；

c） 比较证书中的主账号和从卡片读出的应用主账号是否相同。如果不同，那么动态数据认证失败；

d） 比较证书失效日期中指定年月的最后日期与当天的日期。如果证书失效日期在今天的日期之前，那么证书已过期，动态数据认证失败；

e） 准备表 9 中的前 9 个数据元以及 JR/T 0025.5 的 9.3.1 条指明的需认证的静态数据（用于验证签 名）。如果静态数据认证标签列表存在，并且其包含非“82”的标签，那么动态数据认证失败；

f） 检查卡片公钥签名算法标识，如果不是“04”，那么动态数据认证失败；

g） 使用发卡行公钥和相应的发卡行签名算法将8.2.3条中指明的验证方法对表8的数字签名进行验证。如果验证签名失败，那么动态数据认证失败；

h） 如果以上所有的检验都通过，继续下面的流程。

表 9 认证中心使用 SM2 签名的 IC 卡公钥证书的格式

字段名	长度	描述	格式
证书格式	1	十六进制，值为‘14’	b
CID	10	卡片唯一 ID（在右边补上十六进制数‘F’）	cn20
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	3	由认证中心分配给这张证书的的二进制数	b
卡片公钥签名算法标识	1	标识使用在卡片公钥上的数字签名算法。SM2 算法为‘04’	b
卡片公钥加密算法标识	1	标识使用在 IC 卡公钥上的加密算法,暂不使用,取值‘00’	b
卡片公钥参数标识	1	用于标识椭圆曲线，同时确定 N_{IC}	b
卡片公钥长度	1	标识卡片公钥的字节长度	b
卡片公钥	N_{IC}	如果卡片公钥算法标识对应于 SM2，该字段为椭圆曲线上的一个点	b
数字签名	N_{IC}	认证中心对表 6 数据计算的 SM2 签名 r||s	b

6.4.5.3 动态签名的生成

使用 SM2 算法生成动态签名的步骤应符合如下要求：

a） 终端发出内部认证（INTERNAL AUTHENTICATE）命令，命令中包含由 DDOL 指定的数据元，这些数据元按 JR/T 0025.4 中指明的规则连接在一起；

b） 卡片使用卡片私钥对表 10 中指明的数据计算 SM2 签名,得到如表 11 的格式的 SM2 签名动态应用数据。

表 10 需签名的动态应用数据（待签名数据）

字段名	长度	描述	格式
签名的数据格式	1	十六进制，值为‘15’	b
卡片动态数据长度	1	标识卡片动态数据的字节长度 L_{DD}	b
卡片动态数据	L_{DD}	由卡片生成和、或存储在卡片上的动态数据	-
终端动态数据	4	不可预知数	b

动态数据认证所需的数据对象要求见表 11。

表 11 生成和检验动态签名所需要的其它数据对象

标签	长度	值	格式
9F4B	$N_{IC}+L_{DD}+2$	SM2 签名动态应用数据	b

6.4.5.4 DDA 动态数据验证

使用 SM2 签名动态应用数据，终端获取的签名动态应用数据的格式如表 12 所示，包括被签名的明文数据及数字签名。终端使用卡片的公钥验证动态应用数据的签名。

验证步骤如下：

a） 获取并解析如表 12 所示的经过发卡行签名的动态数据，如果失败，则动态数据认证失败；

b） 检查签名的数据格式的值，如果不是“15”，那么动态数据认证失败；

c） 准备表 12 中的前 3 个数据元(即从签名数据格式直到卡片动态数据)及 DDOL 中指定的数据元，即表 12 数据；

d） 使用卡片公钥和相应的卡片签名算法将 8.2.3 条中指明的验证方法对表 12 的数字签名进行验证；

e） 如果验证签名失败，那么动态数据认证失败；

f） 如果以上所有的步骤都成功，那么动态数据认证成功。终端应将表 12 中的卡片动态数据中所包含的卡片动态数字存放在标签“9F4C”中。

表 12　卡片使用 SM2 签名的动态应用数据的格式

字段名	长度	描述	格式
签名的数据格式	1	十六进制，值为‘15’	b
卡片动态数据长度	1	标识卡片动态数据的字节长度 L_{DD}	b
卡片动态数据	L_{DD}	由卡片生成和、或存储在卡片上的动态数据	-
数字签名	N_{IC}	认证中心对表 6 数据计算的 SM2 签名 r||s	b

6.4.6 对称密钥

6.4.6.1 密钥类型

对称密钥的密钥类型见表 13，密钥算法是 16 字节 AES 密钥或 SM4 密钥。

表 13　对称密钥

密钥类型	说明
CCK 主控密钥	认证通过后改变卡片安全状态级别。连续 15 次错误后，导致密钥锁定，且不可恢复。 CCK 只能有一个， KID 固定为‘00’，只有系统及设备和卡片知晓。
CTK 传输密钥	个人化阶段的会话加密密钥，传输密钥同时用于个人化过程中的数据加密和签名计算。个人化过程结束后，传输密钥失效。CTK 仅在一次会话中有效。
EAK 外部认证密钥	认证通过后改变内部认证密钥安全状态级别。连续 15 次错误后，导致密钥锁定，且不可恢复。EAK 可以有多个，KID 不能为‘00’
IAK 内部认证密钥	加密/解密密钥，可用于设备终端对卡片的认证。 IAK 可以有多个

对称密钥由 4 字节密钥文件头和 16 字节密钥值组成，结构见表 14：

表 14　密钥头和密钥值

密钥类型 （1 字节）	密钥属性 （1 字节）	密钥标识 KID （1 字节）	算法标识 AID （1 字节）	密钥值（16 字节）

表 15　密钥类型说明

密钥类型								含义
b8	b7	b6	b5	b4	b3	b2	b1	
0	0	0	0					RFU
				1				IAK
					1			EAK
						0		RFU
							1	CCK

表 16　密钥属性

密钥属性								含义
b8	b7	b6	b5	b4	b3	b2	b1	
1								非接触界面可用
	1							接触界面可用
		1						IAK密钥被使用时，发送一条HCI事件
			0					RFU
				x	x	x	x	安全级别范围：0~15 外部认证密钥：认证成功后，设置卡片的安全状态级别 内部认证密钥： 满足密钥使用条件的安全状态级别

表 17　密钥标识

密钥标识KID								含义
b8	b7	b6	b5	b4	b3	b2	b1	
x	x	x	x	x	x	x	X	KID

注：EAK KID > 0

表 18　算法标识

密钥标识KID								含义
b8	b7	b6	b5	b4	b3	b2	b1	
x	x	x	x	x	x	0	0	AES
x	x	x	x	x	x	1	0	SM4

表 19 常见的密钥文件头示例

密钥	密钥文件头	说明
CCK	01 CF 00 00	双界面，安全级别 15，KID=00，AID = 00
EAK	04 C1 01 00	双界面，安全级别 1，KID=01，AID = 00
IAK	08 A0 01 02	仅非接触式界面，KID=01，AID = 02，被使用后发送 HCI 事件
IAK	08 A1 02 00	仅非接接触界面，允许使用的安全级别 1，KID=02，AID = 02，被使用后发送 HCI 事件

注：除了 CCK 外，其他对称密钥只能在个人化阶段写入，在使用阶段不能被修改。

6.4.6.2　安全状态级别

安全状态级别应符合下列要求：

a） 卡片在复位或者选择 MF 文件目录后，安全状态级别设置为 0；
b） 当使用 CCK/ EAK 外部认证通过后，安全状态级别更改为此密钥对应的级别。安全状态级别的取值范围是 0~15；
c） IAK 在创建时，可以设置满足其使用条件的安全状态级别，使用时必须满足该 IAK 的安全状态级别。

6.5 APDU 命令集

6.5.1 GET ICC CERTIFICATE（取卡片公钥证书）

6.5.1.1 定义和范围

GET ICC CERTIFICATE 命令用于设备终端从 NFC 卡片中读取卡片公钥证书数据。公钥证书数据包括卡片公钥证书、卡片公钥的余项（如果存在）、卡片公钥的指数和 CA 公钥索引号。

6.5.1.2 命令报文

表 20 GET ICC CERTIFICATE 命令报文

代码	长度	值（Hex）	描述
CLA	1	80	
INS	1	B4	
P1	1	04	卡片公钥证书索引，对应 2048 位长卡片公钥
P2	1	XX	返回数据类型，见表 12
Lc	1	00	
Data	-	-	不存在
Le	-	-	不存在

表 21 引用控制参数 P2

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	0	0	返回卡片公钥证书
0	0	0	0	0	0	0	1	返回公钥指数，余项和 CA 公钥索引号

6.5.1.3 应答报文数据域

应答报文数据为 BER-TLV 格式。

表 22 应答报文数据域

标签（T）	长度（Bytes）	名称	是否存在
82	2	2048 位卡片公钥证书	P2=0 时存在
9F47	1	卡片公钥指数	P2=1 时存在
9F48	1	卡片公钥余项	P2=1 时可能存在
8F	1	CA 公钥索引号	P2=1 时存在

6.5.1.4 应答报文状态码

表 23 应答报文状态码

SW1	SW2	含义

90	00	正确执行
61	XX	正确执行，XX 表示响应数据长度，可用 GET RESPONSE 命令获取
67	00	Lc 错误
6A	86	参数 P1P2 错误
6A	88	引用数据未找到

6.5.2 GET RESPONSE（取响应数据）

6.5.2.1 定义和范围

GET RESPONSE 命令用于从卡片获取额外的响应数据。

6.5.2.2 命令报文

表 24 GET RESPONSE 命令报文

代码	长度	值（Hex）	描述
CLA	1	00	
INS	1	C0	
P1	1	00	
P2	1	00	
Lc	-	-	不存在
Data	-	-	不存在
Le	1	XX	期望响应数据的长度

6.5.2.3 应答报文数据域

应答报文数据的长度由 Le 的值决定。如果 Le=0，在额外数据有效时，卡片必须回送状态码‘6Cxx’，否则回送状态码‘6F00’。

6.5.2.4 应答报文状态码

表 25 GET RESPONSE 应答报文状态码

SW1	SW2	含义
90	00	正确执行
61	XX	正确执行，XX 表示响应数据长度，可用 GET RESPONSE 命令获取
67	00	长度错误（Le 大于卡中响应数据长度）
6A	86	参数 P1P2 错误
6C	XX	长度错误（Le 不正确，XX 表示实际长度）
6F	00	数据无效

6.5.3 INTERNAL SIGNATURE（内部认证签名）

6.5.3.1 定义和范围

INTERNAL SIGNATURE 命令返回使用动态脱机数据认证的签名数据。用于设备终端验证卡片的有效性。计算方法参见 15.9 动态签名的生成。

6.5.3.2 命令报文

表 26　INTERNAL SIGNATURE 命令报文

代码	长度	值（Hex）	描述
CLA	1	80	
INS	1	B6	
P1	1	XX	CA 公钥索引号，见表 27
P2	1	00	
Lc	1	04	
Data	XX	XX...XX	终端不可预知数
Le	-	-	不存在

表 27　引用控制参数 P1

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	0	1	CA 索引 01，对应 1024 位长密钥
0	0	0	0	0	0	1	0	CA 索引 02，对应 1152 位长密钥
0	0	0	0	0	1	0	0	CA 索引 04，对应 2048 位长密钥
0	0	0	0	1	0	0	0	CA 索引 08，对应 SM2 密钥
0	0	0	0	0	0	0	0	使用缺省公钥索引

6.5.3.3　命令报文数据域

4 字节终端不可预知数。

6.5.3.4　应答报文数据域

应答报文数据为 BER-TLV 格式。

表 28　应答报文数据域

标签（T）	长度（Bytes）	值
80	2	认证签名数据

6.5.3.5　应答报文状态码

表 29　应答报文状态码

SW1	SW2	含义
90	00	正确执行
61	XX	正确执行，XX 表示响应数据长度，可用 GET RESPONSE 命令获取
67	00	Lc 错误
6A	86	参数 P1P2 错误
6A	88	引用数据未找到

6.5.4　SELECT（选择）

6.5.4.1　定义和范围

SELECT 命令通过文件名或 AID 来选择卡片中的 MF 或 DF。卡片的响应数据应由回送文件控制信息 FCI 组成。

6.5.4.2 命令报文

表 30 SELECT 命令报文

代码	长度	值（Hex）	描述
CLA	1	00	
INS	1	A4	
P1	1	XX	参见表 25
P2	1	00	
Lc	1	XX	
Data	XX	XX...XX	文件标识符或应用标识符（AID）
Le	-	-	不存在

表 31 引用控制参数 P1

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	0	0	通过文件标识符选择
0	0	0	0	0	1	0	0	通过 AID 选择

6.5.4.3 命令报文数据域

当 P1=’04’时，数据域为应用实例的 AID。

当 P1=’00’时，数据域为 ‘3F00’ 或其它 2 字节文件标识符。

6.5.4.4 应答报文数据域

表 32 选择 ADF 的应答报文（FCI）

标签	值		存在性
6F	FCI 模板		M
	84	DF 名	M
	A5	FCI 数据专用模板	M
	5A	CID	M
	50	应用标签	M
	9F0C	发卡行自定义数据 字节 1：卡片生命周期状态 字节 2：对称算法标识 (00: AES, 01: SM4) 字节 3：非对称算法标识 (00:RSA,02:SM2) 字节 4：是否需要外部认证(00: 不需要，01：需要)	M

Tag ‘50’ 应用标签，长度范围为 1~16 字节。建议发卡方在个人化时写入自定义的应用标签。缺省应用标签可以由发卡方自行定义。字节 4 为“00”不需要外部认证，为“01”需要外部认证才能写卡。

6.5.4.5 应答报文状态码

表 33 应答报文状态码

SW1	SW2	含义

90	00	正确执行
67	00	Lc 错误
6A	82	文件未找到
6A	86	参数 P1P2 错误

6.5.5 WRITE CTK（写卡片传输密钥）

6.5.5.1 定义和范围

设备终端成功从卡片公钥证书中恢复卡片公钥后，产生一个随机的会话密钥，使用卡片公钥加密后发送给卡片，作为后续 STORE DATA 命令的会话保护密钥。WRITE CTK 执行成功后会返回一个 8 字节的卡片随机数，该随机数会参与计算后续第一条 STORE DATA 命令的 MAC 值。

当使用 2048 位长 RSA 公钥加密时，数据域长度大于 255，需要连续发送 2 条 WRITE CTK 命令。

6.5.5.2 命令报文

表 31 WRITE CTK 命令报文

代码	长度	值（Hex）	描述
CLA	1	80	
INS	1	B8	
P1	1	04	CA 公钥索引号，对应 2018 位长密钥
P2	1	XX	见引用控制参数 P2
Lc	1	XX	
Data	XX	XX...XX	加密的 CTK
Le	-	-	不存在

表 32 引用控制参数 P2

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	0	0	有后续数据块
1	0	0	0	0	0	0	0	最后一个数据库

6.5.5.3 命令报文数据域

使用卡片公钥加密的 CTK 数据，数据填充方式为 RSA PKCS1。加密数据的长度等于对应卡片公钥模的长度。

6.5.5.4 应答报文数据域

8 字节卡片随机数。

6.5.5.5 应答报文状态码

表 33 应答报文状态码

SW1	SW2	含义
90	00	正确执行
67	00	Lc 错误
6A	86	参数 P1P2 错误

6A	88	不支持对应长度的密钥

6.5.6 STORE DATA（数据存储）

6.5.6.1 定义和范围

STORE DATA 命令用于完成卡片个人化。

WRITE CTK 执行成功后才允许使用 STORE DATA 命令。 STORE DATA 命令中 MAC 和加密计算中用到了 WRITE CCK 命令返回的 8 字节随机数 R。

STORE DATA 的数据域需要用 CTK 计算 MAC，并对数据域加密。

个人化过程中的最后一条 STORE DATA 命令成功执行后，卡片生命周期状态被设置为‘07’，同时卡片会向手机发送一条 HCI 事件，通知手机已经完成个人化，HCI 事件中包含了 SELECT 命令应答数据中‘A5’模板的 FCI 数据。

6.5.6.2 命令报文

表 34 STORE DATA 命令报文

代码	长度	值（Hex）	描述
CLA	1	84	
INS	1	E2	
P1	1	XX	参见表 35
P2	1	XX	数据块编号
Lc	1	XX	
Data	XX	XX...XX	加密的应用数据和 MAC
Le	-	-	不存在

表 35 引用控制参数 P1

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	-	-	-	-	-	-	-	有后续数据块
1	-	-	-	-	-	-	-	最后一个数据块

6.5.6.3 命令报文数据域

应用数据支持以下数据分组。

表 36 数据分组索引

DGI	Tag	数据名称	长度(字节）	值
9211	**密钥**			
	8000	密钥 1	20	密钥文件头+密钥值
	8001	密钥 2	20	密钥文件头+密钥值
	…	…	…	…
	8007	密钥 8	20	密钥文件头+密钥值
9210	**内部数据**			
	50	应用标签	1~16	自定义应用标签。 应用标签会在 SELECT 命令中返回。

其中 DGI 采用 <DGI 分组><1 字节长度><DGI 数据>格式编码。
MAC 计算方法应符合图 4 的要求， 其中 MAC 链数据初始值为“CID‖R”。

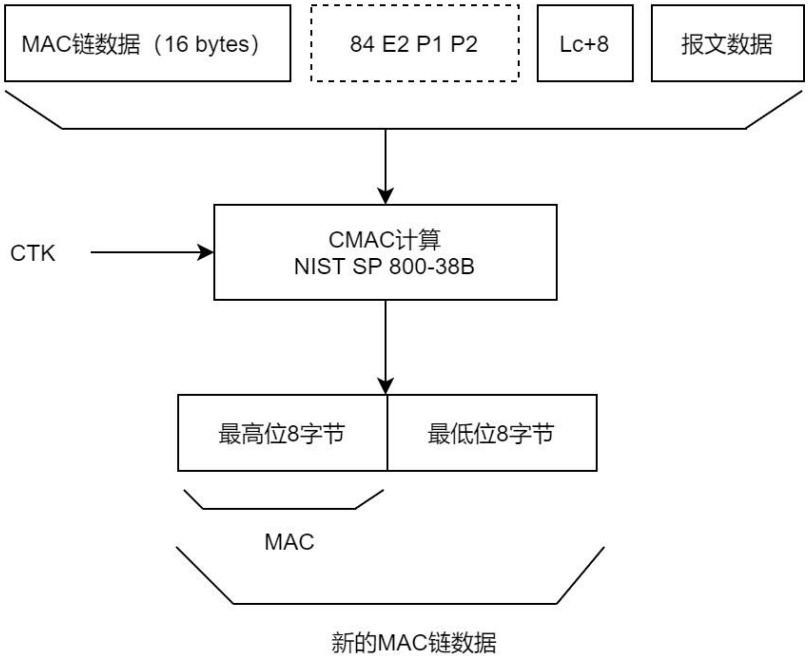

图 4 新的 MAC 链数据

命令报文应用数据加密方法应符合图 5 的要求，其中 ICV 的初始值为“CID‖R”。

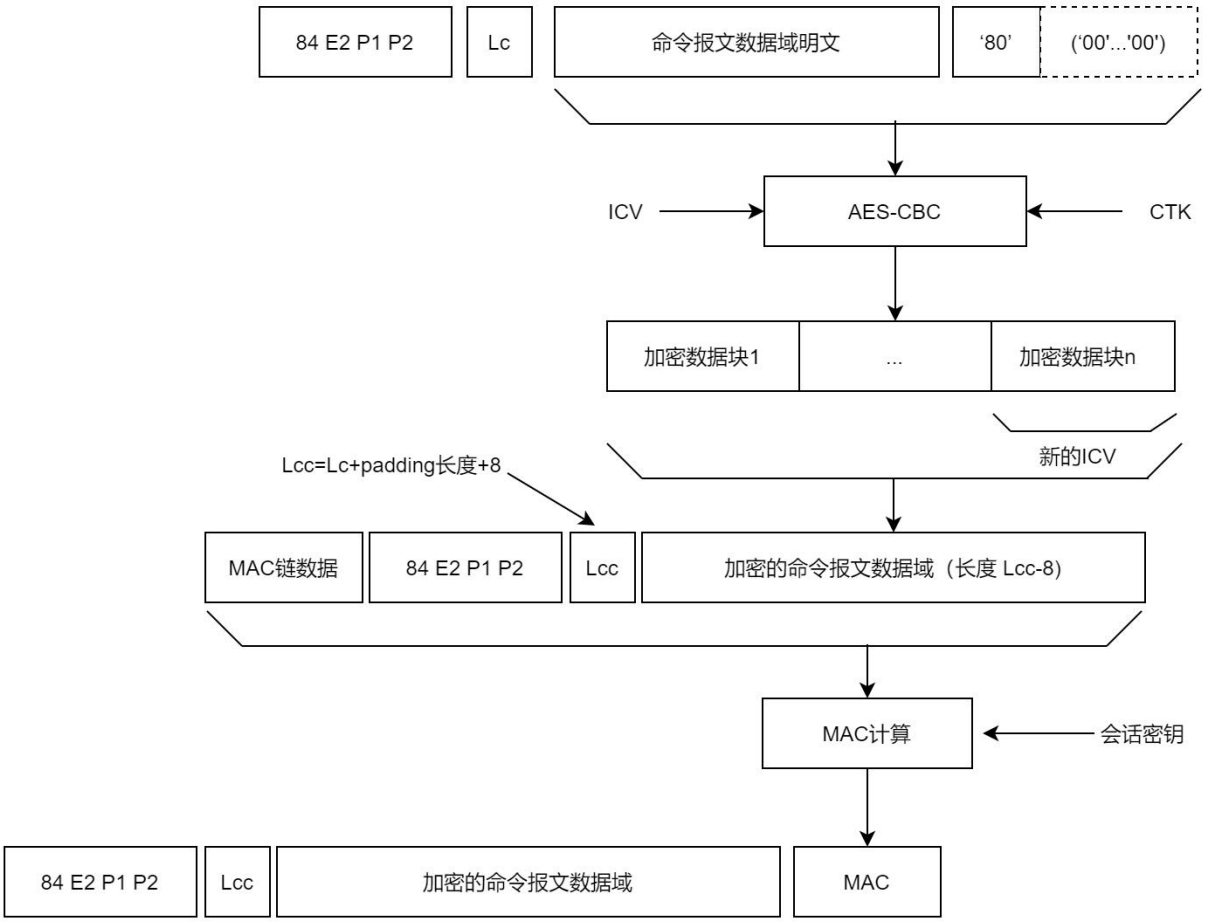

图 5 加密应用数据

数据域 DGI 举例：

写入应用标签，DGI 9210

```
9210 0F 50 0D 63707520636172642074657374
```

写入密钥 EAK/ IAK，DGI 9211

```
9211 2C 8000 14 01CF0000 11111111111111111111111111111111 8001 14 08A10000
22222222222222222222222222222222
```

6.5.6.4 应答报文状态码

表 30 应答报文状态码

SW1	SW2	含义
90	00	正确执行
6A	80	数据格式错误
6A	86	参数 P1P2 错误
69	82	安全条件不满足

6.5.7 GET CHALLENGE（取随机数）

6.5.7.1 定义和范围

GET CHALLENGE 命令请求一个用于线路保护过程的卡片随机数，该随机数仅在后续的一条命令中有效。

6.5.7.2 命令报文

表 45 GET CHALLENGE 命令报文

代码	长度	值（Hex）	描述
CLA	1	00	
INS	1	84	
P1	1	00	
P2	1	00	
Lc	-	-	不存在
Data	-	-	不存在
Le	1	08	要求卡片返回的随机数长度

6.5.7.3 应答报文数据域

长度为 Le 个字节的卡片随机数。

6.5.7.4 应答报文状态码

表 46 应答报文状态码

SW1	SW2	含义
90	00	正确执行
67	00	请求随机数的长度错误
6A	86	参数 P1P2 错误

6.5.8 EXTERNAL AUTHENTICATE（外部认证）

6.5.8.1 定义和范围

EXTERNAL AUTHENTICATE 命令用指定的外部认证密钥解密数据域，然后与上一条命令产生的卡片随机数进行比较，若一致则表示认证通过，设置卡片安全状态级别为该密钥规定的后续状态，错误计数器恢复成初始值；若比较不一致则认证失败，不改变卡片安全状态级别。

此条命令前需要执行 GET CHALLENGE 命令取卡片随机数（8 字节）。

在满足外部认证密钥的使用条件且该密钥未被锁死的情况下才能执行此命令。

当 P2 Bit8=‘1’时，需要使用会话密钥进行计算。 会话密钥 SessionKey = AES_ECB(EAK，终端随机数||卡片随机数) ，终端随机数和卡片随机数长度均为 8 字节。

当使用 AES 或 SM4 算法时，终端需要先对卡片随机数填充’80’，如果不足 16 的整数倍，在最后填充’00’至 16 的整数倍。

6.5.8.2 命令报文

表 41 EXETRNAL AUTHENTICATE 命令报文

代码	长度	值（Hex）	描述
CLA	1	00	
INS	1	82	

P1	1	XX	见表 35
P2	1	XX	外部认证密钥标识号 KID
Lc	1	XX	10：不使用会话密钥时；18：使用会话密钥时
Data	XX	XX...XX	见表 36
Le	-	-	不存在

表 42　引用控制参数 P1

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	0	0	不使用会话密钥
1	0	0	0	0	0	0	0	使用会话密钥

6.5.8.3　命令报文数据域

表 43　命令报文数据域

数据元素	长度（字节）	是否存在
加密后的随机数	16	M
终端随机数（P1=80 时存在）	8	O

6.5.8.4　应答报文状态码

表 44　应答报文状态码

SW1	SW2	含义
90	00	正确执行
63	CX	外部认证密钥还剩 X 次尝试机会
67	00	Lc 错误
69	82	密钥使用条件不满足
69	83	密钥被锁死
69	84	卡片随机数无效
6A	86	参数 P1P2 错误
6A	88	未找到外部认证密钥

6.5.9　INTERNAL AUTHENTICATE（内部认证）

6.5.9.1　定义和范围

INTERNAL AUTHENTICATE 命令对设备终端发来的随机数，使用命令中指定的内部认证密钥 IAK 进行加密，并返回计算结果。

在满足内部认证密钥的使用条件下才能执行此命令。

该命令提供了一种外部终端认证卡片的方法。

如果个人化时， IAK 密钥属性的 B6 字节设置为“1”， 则此条命令在非接界面上会发送一条 HCI 事件， 格式为 APDU 命令的前 5 个字节，即: CLA INS PI P2 Lc

当 P2 Bit8=‘1’时，需要使用会话密钥进行计算。 会话密钥 SessionKey = AES_ECB(IAK，终端随机数||卡片随机数) ，终端随机数和卡片随机数长度均为 8 字节。

使用会话密钥时，卡片在收到命令报文后，先生成卡片随机数，然后计算会话密钥，并将卡片随机数在响应数据中返回。 终端收到响应报文后， 计算会话密钥，并验证认证数据 。

当使用 AES 或 SM2 算法时，卡片需要先对终端随机数填充’80’，如果不足 16 的整数倍，在最后填充’00’至 16 的整数倍。

6.5.9.2 命令报文

表 47 INTERNAL AUTHENTICATE 命令报文

代码	长度	值（Hex）	描述
CLA	1	00	
INS	1	88	
P1	1	XX	参见表 48
P2	1	XX	内部认证密钥标识号 KID
Lc	1	XX	认证数据的长度
Data	XX	XX...XX	认证数据 （终端随机数）
Le	-	-	不存在

表 48 引用控制参数 P1

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	0	0	加密
0	0	0	0	0	0	0	1	RFU
0	-	-	-	-	-	-	-	不使用会话密钥
1	-	-	-	-	-	-	-	使用会话密钥

6.5.9.3 命令报文数据域

命令报文数据域为认证数据（即终端随机数）。

6.5.9.4 应答报文数据域

对认证数据进行加密或解密的计算结果。

表 41 应答报文数据域

数据元素	长度（字节）	是否存在
加密后的认证数据	16	M
卡片随机数（P1=80 时存在）	8	O

6.5.9.5 应答报文状态码

表 49 应答报文状态码

SW1	SW2	含义
90	00	正确执行
61	XX	正确执行，XX 表示响应数据长度，可用 GET RESPOSNSE 命令获取
67	00	Lc 错误
69	82	密钥使用条件不满足
6A	86	参数 P1P2 错误
6A	88	密钥未找到

6.5.10 READ BUFFER（读缓冲区数据）

6.5.10.1 定义和范围

卡片预置了一个长度为 192 个字节的缓冲区，用于保存卡片自定义数据。READ BUFFER 命令用于读取缓冲区内容。当同时满足以下条件时，允许读取缓冲区内容：

a） 前一条命令为内部认证命令（INTERNAL AUTHENTICATE），且必须使用会话密钥模式；或者前一条命令是成功执行的 READ BUFFER 命令，或者前一条命令是成功执行的 WRITE BUFFER 命令；

b） 卡片安全级别>=1。使用 READ BUFFER 和 WRITE BUFFER 命令的授权或应用应符合图 6 的要求：

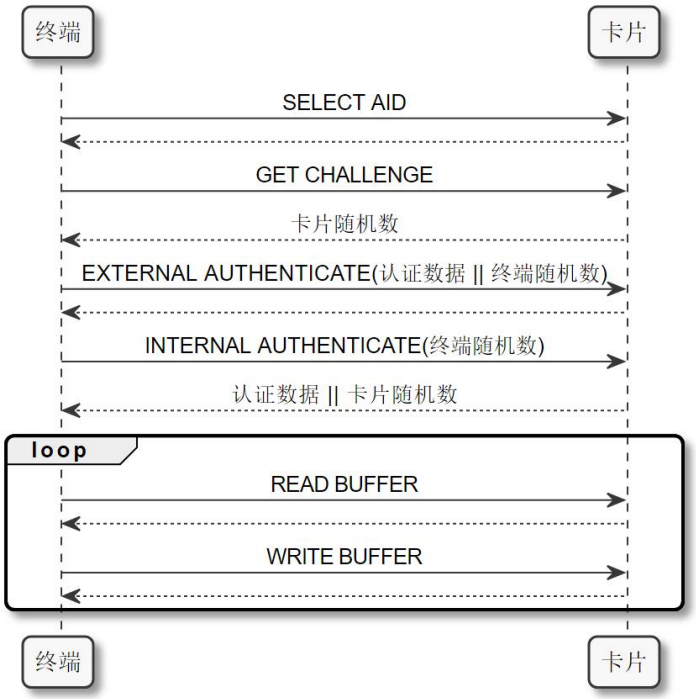

图 6 读写缓冲区数据使用流程

为保证读取数据的安全，命令返回数据使用会话密钥加密并签名。

6.5.10.2 命令报文

READ BUFFER 命令报文

代码	值
CLA	‘80’
INS	‘B0’
P1	‘00’
P2	起始位置偏移量， 取值范围’00’~’BF’
Lc	不存在
Data	不存在
Le	要读取的数据长度。

当 Le=0 时，返回文件所有内容。

当偏移量 P2+Le 大于文件实际长度时，返回警告状态 6Cxx，xx 为可读取的有效长度，请求将 Le 置为 xx 并重发命令。

6.5.10.3 应答报文数据域

加密缓冲区数据 ‖ 8 字节 MAC。

MAC 计算方法应符合图 7 的要求，其中 MAC 链数据初始值为前面内部认证命令中使用的“终端随机数‖卡片随机数”。

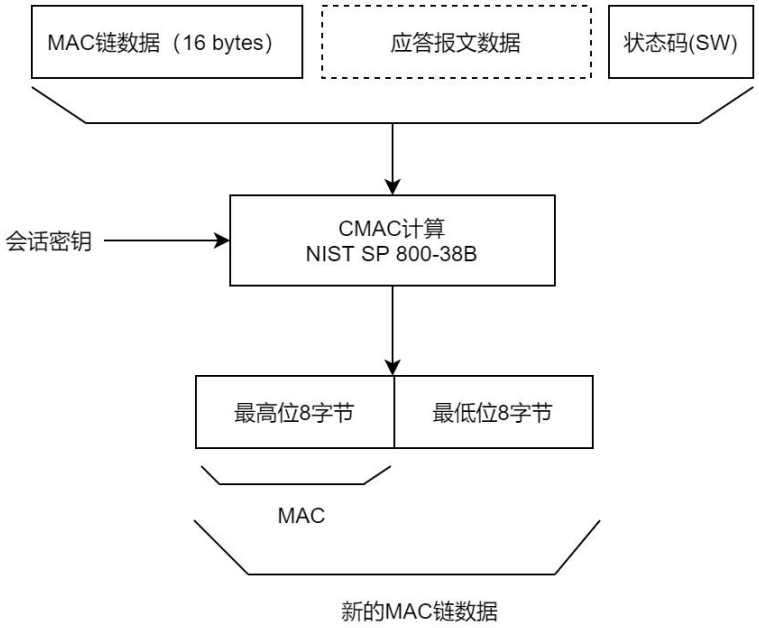

图 7 终端读缓冲区的新 MAC 链数据计算流程

应答报文加密计算方法应符合图 8 的要求， 其中 ICV 初始值为前面认证命令中使用的“终端随机数‖卡片随机数”。

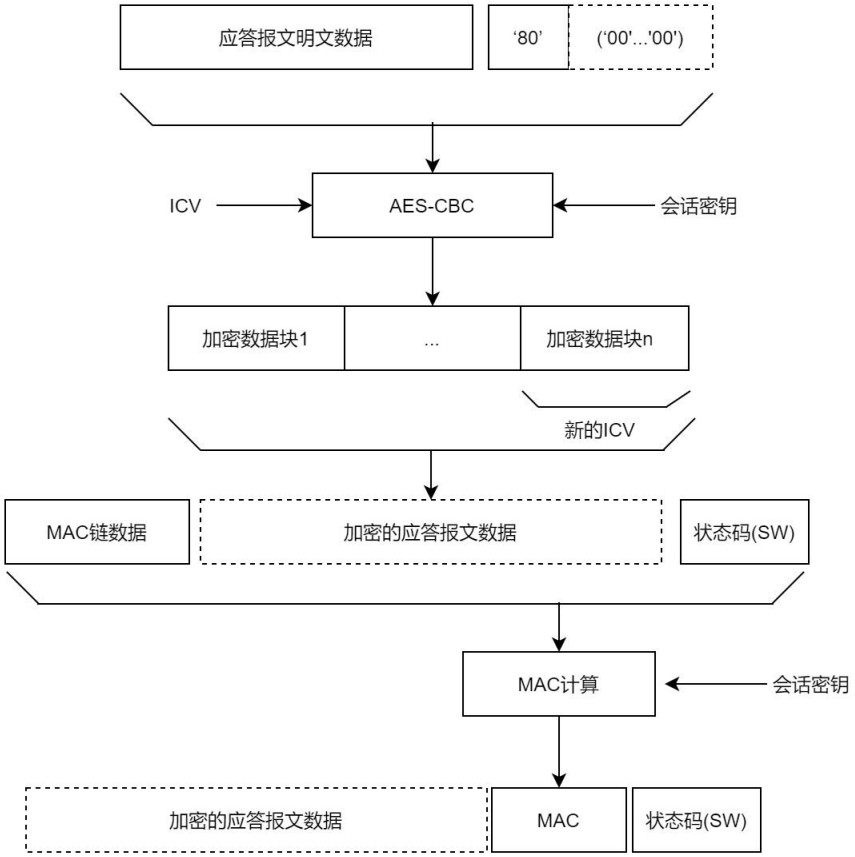

图 8 读缓冲区卡片返回的 MAC 计算流程

6.5.10.4 应答报文状态码

SW1	SW2	含义
‘68’	‘82’	安全条件不满足
‘6B’	‘00’	偏移量超出范围
‘6C’	‘xx’	Le 错误

6.5.11 WRITE BUFFER（写缓冲区数据）

6.5.11.1 定义和范围

卡片预置了一个长度为 192 个字节的缓冲区，用于保存卡片自定义数据。WRITE BUFFER 命令用于更新缓冲区内容。当同时满足以下条件时，允许更新缓冲区内容：

a） 前一条命令为内部认证命令（INTERNAL AUTHENTICATE），且必须使用会话密钥模式；或者前一条命令是成功执行的 READ BUFFER 命令，或者前一条命令是成功执行的 WRITE BUFFER 命令；

b） 卡片安全级别>=1。为保证更新数据的安全，命令报文中数据域应使用会话密钥加密并签名。

6.5.11.2 命令报文

WRITE BUFFER 命令报文

代码	值
CLA	‘84’
INS	‘D0’

P1	‘00’
P2	‘xx’起始位置偏移量，取值范围’00’~’BF’
Lc	‘xx’数据域长度
Data	写入缓冲区的数据（加密+MAC）
Le	不存在

6.5.11.3 命令报文数据域

加密数据 ‖ 8 字节 MAC。

数据加密和 MAC 的计算方式参考“STORE DATA”命令的方法。

MAC 计算方法应符合图 9 的要求，其中 MAC 链数据初始值为前面内部认证命令中使用的“终端随机数||卡片随机数”。

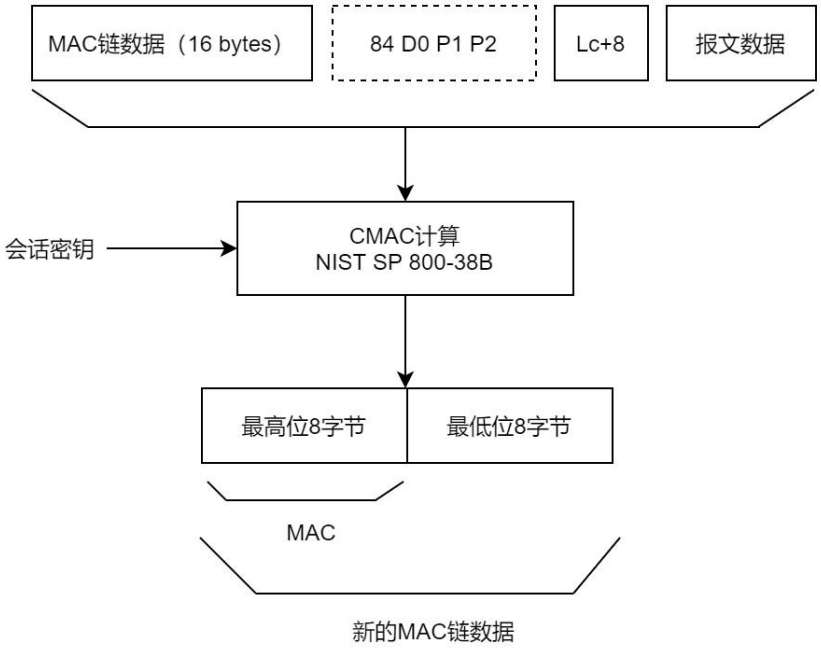

图 9 终端写缓冲区新 MAC 链数据计算流程

命令报文加密计算方法应符合图 10 的要求， 其中 ICV 初始值为前面认证命令中使用的“终端随机数||卡片随机数”。

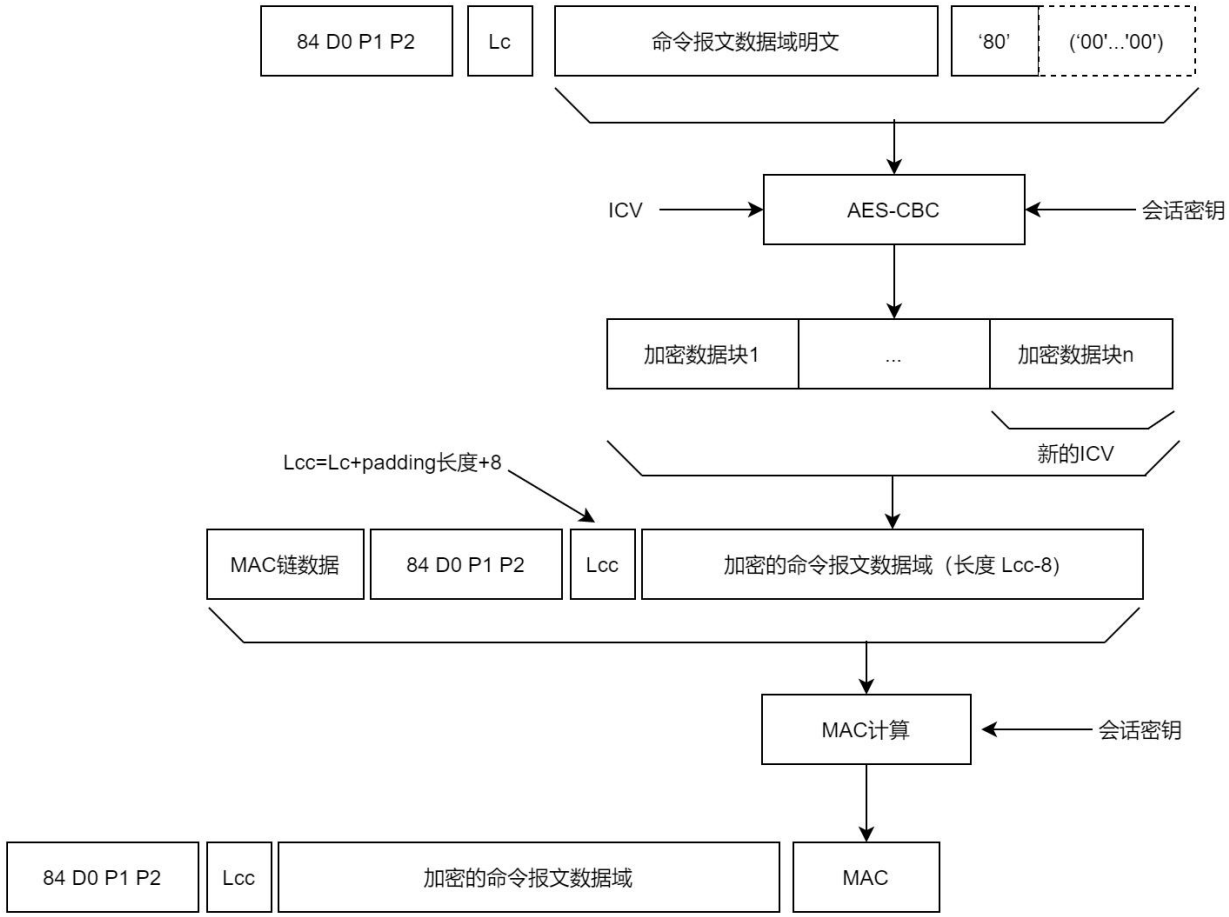

图 10 写缓冲区卡片返回的 MAC 计算流程

6.5.11.4 应答报文状态码

SW1	SW2	含义
‘67’	‘00’	数据域长度错误
‘69’	‘82’	安全状态不满足
‘6B’	‘00’	偏移量超出范围

6.6 预个人化

预个人化应符合基本的安全性需求，包括并不限于：

a） 保证应用实例 CID 的唯一性；

b） 卡片公私钥必须在应用实例中生成，并且私钥不允许被读取；

c） 建议使用 GP 安全通道机制保证从卡片读取公钥、写入证书、密钥等操作的数据安全；

d） 预个人化结束后，卡片应用生命周期状态被设置为 03。

7 系统及终端要求

7.1 安全要求

7.1.1 一般要求

系统及终端应符合下列要求：

a） 终端采用公钥算法验证卡片上的签名和证书来实现脱机数据认证，公钥技术使用私钥产生加密数据（证书或签名），该加密数据可以被公钥解密而用于验证和数据恢复；

b） 卡片采用外部认证验证终端或系统的合法性，验证通过后，终端或系统可以对卡片进行个人化操作，个人化操作包含开锁时用于身份验证的对称密钥的写入，授权数据和授权有效期的写入等；

c） 终端或系统的密钥应存储到安全模块中；

d） 安全模块包含安全芯片、SAM 卡、密码机等；

e） 安全模块存储的密钥通过发卡机构和 CID 进行密钥初始化可得到卡片的密钥，认证数据至少包含终端、系统或卡片所产生的随机数，认证密文是通过卡片的密钥加密认证数据所产生的；

f） 终端应支持唯一的设备 ID(RID)，设备 ID 存储在安全模块中。

7.1.2 安全芯片

安全芯片应符合下列要求：

a） 符合 GB/T22186-2016 《信息安全技术 具有中央处理器的 IC 卡芯片安全技术要求》、GM/T 0028-2014《密码模块安全技术要求》5.5 规定的安全二级的要求，同时应支持随机数发生，随机数应符合 GM/T 0006—2012《密码应用标识规范》及 NIST 随机数检测标准；

b） 支持非对称密码 GM/T 0003.1—2012《SM2 椭圆曲线公钥密码算法》，实现签名/验证以及密钥交换；

c） 支持杂凑密码，符合 GM/T 0004—2012《SM3 密码杂凑算法》要求，实现待签名消息的摘要运算；

d） 支持对称密码，符合 GM/T 0002—2012《SM4 分组密码算法》要求，实现数据加解密及消息认证；

e） 支持不低于 1152 位的非对称密码 RSA 算法；

f） 支持杂凑密码 SHA256 算法；

g） 支持对称密码 AES128 算法。

7.1.3 SAM 卡

SAM卡应符合下列要求：

a） 符合 GB/T22186-2016 《信息安全技术 具有中央处理器的 IC 卡芯片安全技术要求》、GM/T 0028-2014《密码模块安全技术要求》5.5 规定的安全二级的要求，同时应支持随机数发生，随机数应符合 GM/T 0006—2012《密码应用标识规范》及 NIST 随机数检测标准；

b） 支持对称密码，符合 GM/T 0002—2012《SM4 分组密码算法》要求，实现数据加解密及消息认证；

c） 支持对称密码 AES128 算法。

7.1.4 密码机

密码机应符合下列要求：

a） 符合 GB/T22186-2016 《信息安全技术 具有中央处理器的 IC 卡芯片安全技术要求》、GM/T 0028-2014《密码模块安全技术要求》5.5 规定的安全二级的要求，同时应支持随机数发生，随机数应符合 GM/T 0006—2012《密码应用标识规范》及 NIST 随机数检测标准；

b） 支持对称密码，符合 GM/T 0002—2012《SM4 分组密码算法》要求，实现数据加解密及消息认证；

c） 支持对称密码 AES128 算法。

7.2 授权要求

7.2.1 终端授权

终端授权应符合图11的要求：

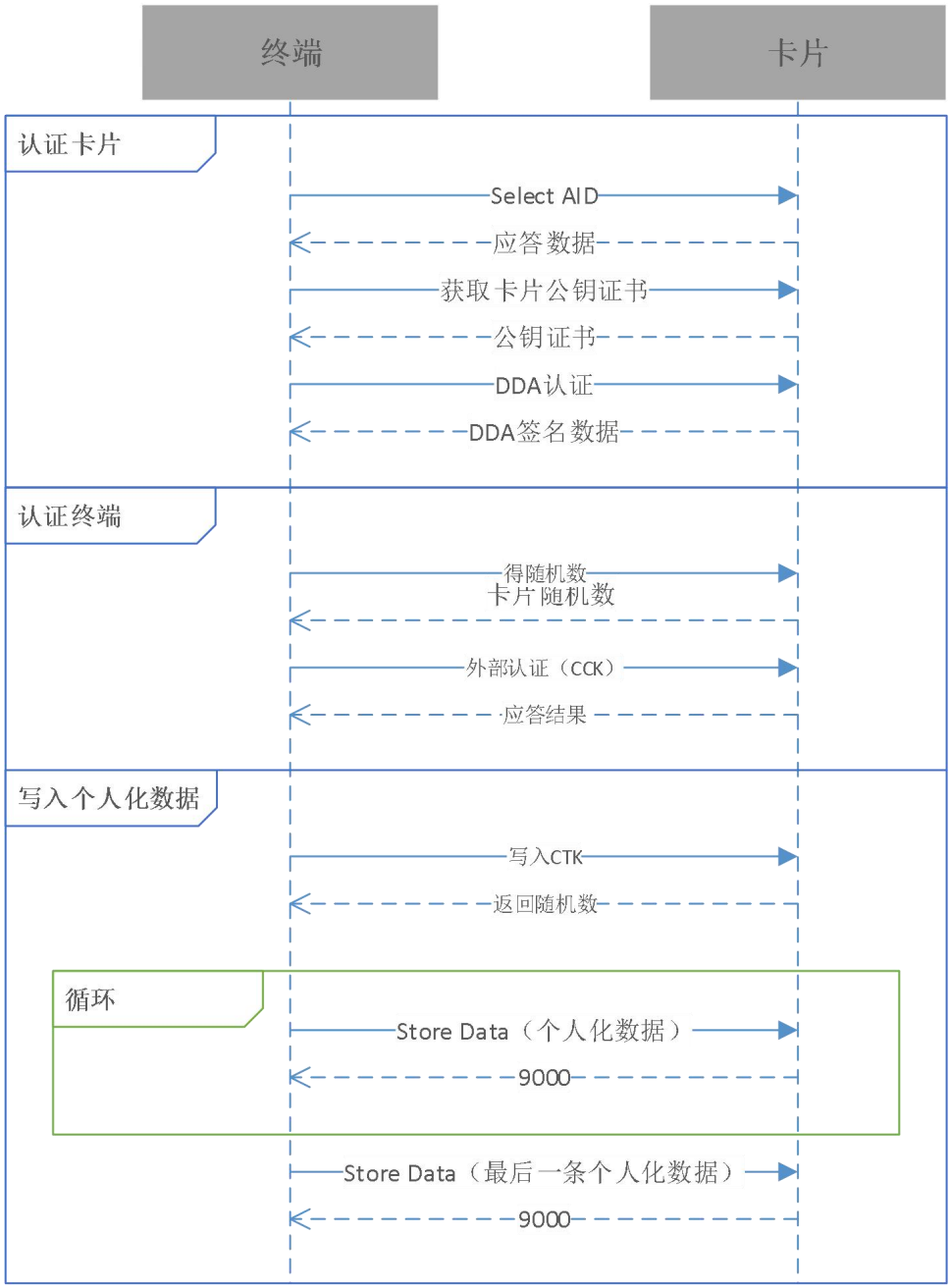

图 11 卡片个人化流程

当卡片生命周期状态为 03 时，允许对卡片进行个人化数据写入的操作，操作流程如上图。主要分为三个步骤：

a） 门锁从卡片中读取卡片公钥证书，用 CA 公钥验证签名并恢复卡片公钥，然后发起 DDA 认证，验证卡片生成的动态数据签名，从而确定卡片的有效性；

b） 门锁使用 CCK 密钥对卡片进行外部认证，获取卡片的写入权限；

c） 发起一条或多条 STORE DATA 命令，创建卡片文件结构。

7.2.2 系统授权

系统授权应符合图12的要求：

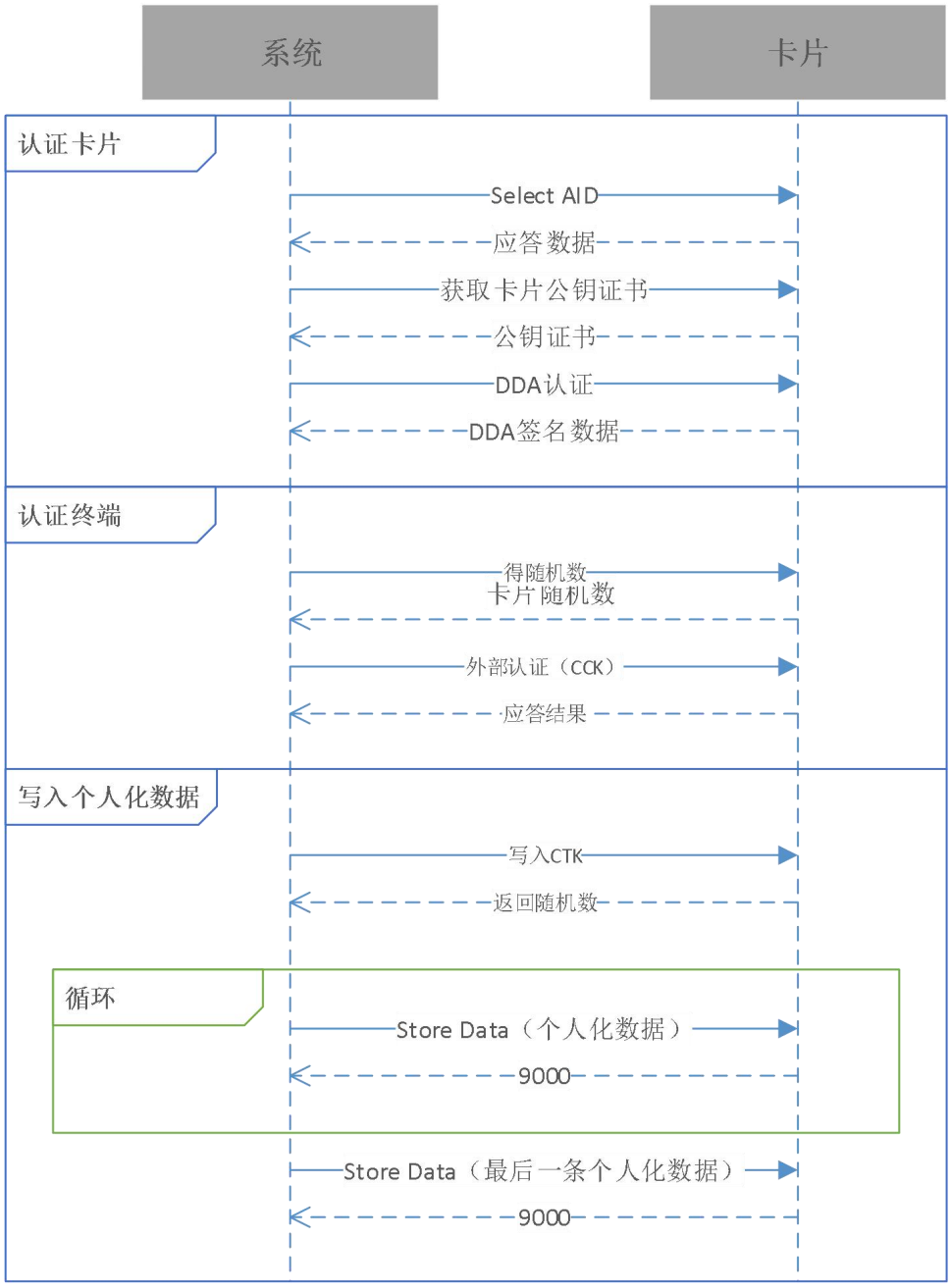

图 12 卡片个人化流程

当卡片生命周期状态为 03 时，允许对卡片进行个人化数据写入的操作，操作流程如上图。主要分为三个步骤：

a） 业务系统从卡片中读取卡片公钥证书，用 CA 公钥验证签名并恢复卡片公钥，然后发起 DDA 认证，验证卡片生成的动态数据签名，从而确定卡片的有效性；

b） 业务系统使用 CCK 密钥对卡片进行外部认证，获取卡片写入权限；

c） 发起一条或多条 STORE DATA 命令，创建卡片文件结构。

7.2.3 线上授权

线上授权应符合图13的要求：

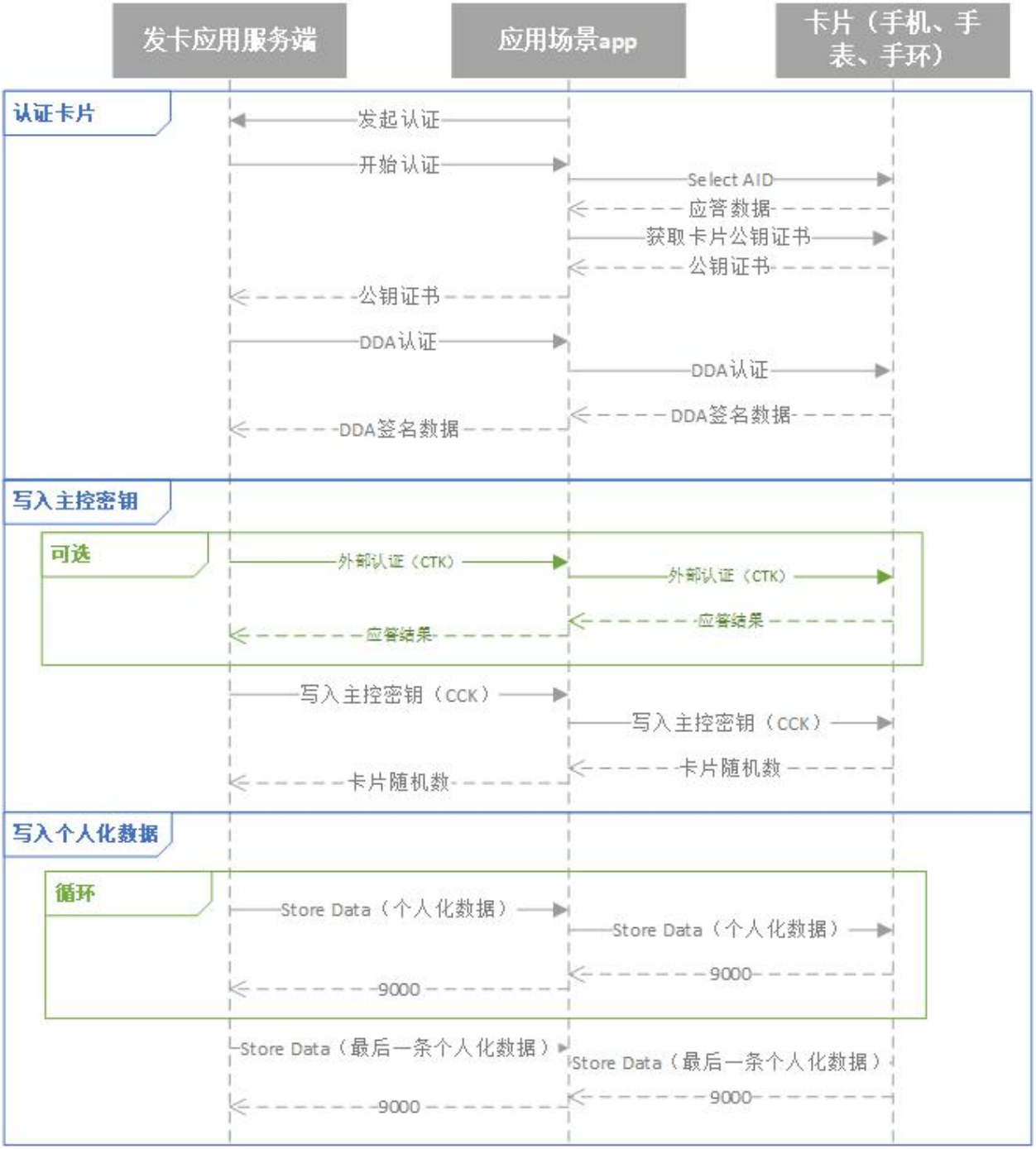

图 13 卡片个人化流程

当卡片生命周期状态为 03 时，允许对卡片进行个人化数据写入的操作，操作流程见图 13。主要分

为三个步骤：

a） 应用 APP 从卡片中读取卡片公钥证书发给发卡应用服务器，发卡应用服务器用 CA 公钥验证签名并恢复卡片公钥，然后发起 DDA 认证，验证卡片生成的动态数据签名，从而确定卡片的有效性；

b） 发卡应用服务器使用 CCK 密钥对卡片进行外部认证，获取卡片写入权限；

c） 发起一条或多条 STORE DATA 命令，创建卡片文件结构。

7.3 应用要求

应用要求应符合图14的要求：

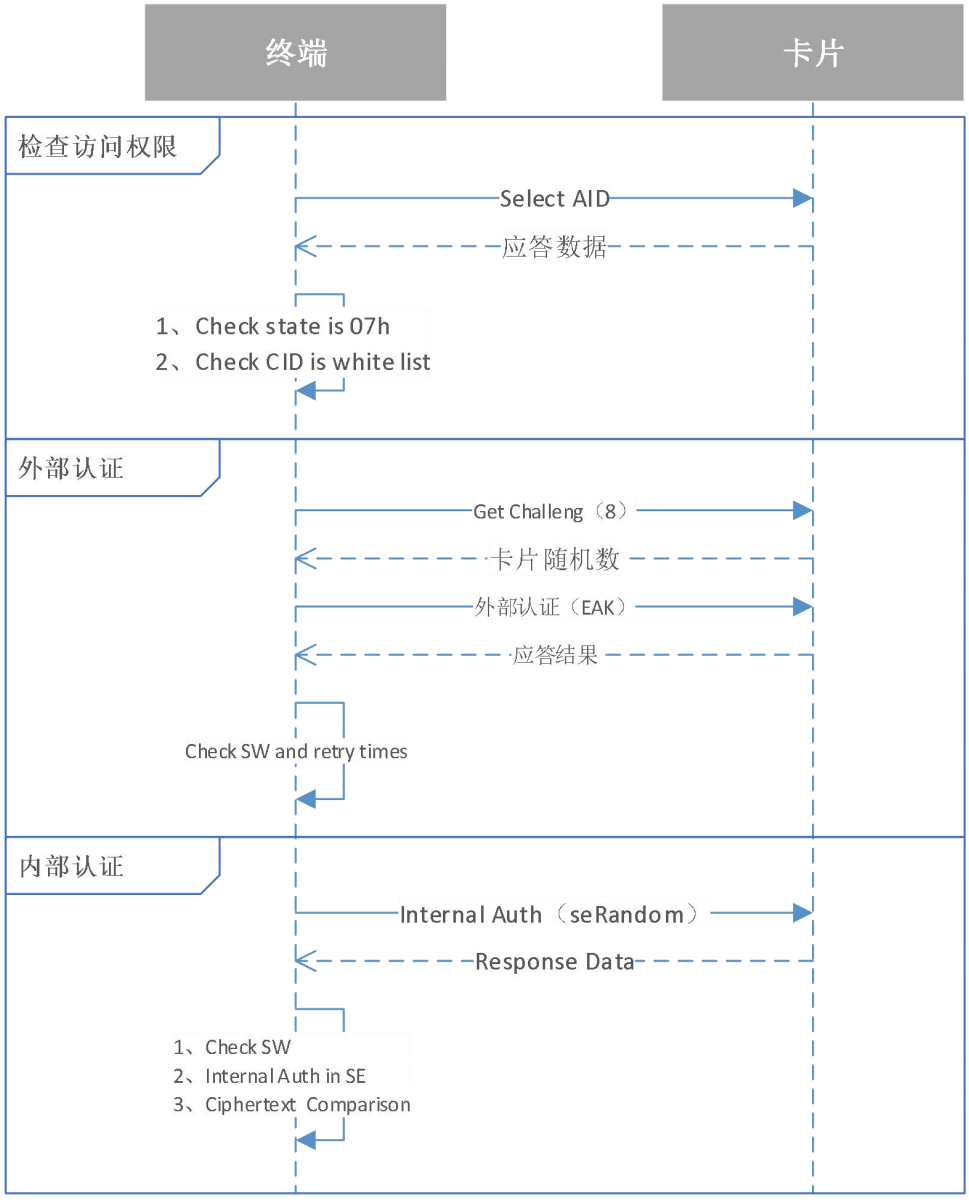

图 14 卡片使用流程

当卡片生命周期状态为 07 时，允许卡片进行开锁操作，操作流程见图 14。主要分为两个步骤：

a） 终端从卡片中读取 CID，与终端中存储的授权 CID 列表进行比对，从而确定卡片经过有效授权；

b） 终端对卡片进行外部认证，卡片确认非攻击内部认证密钥后，允许终端对卡片进行内部认证，认证通过后，终端执行开锁操作。

8 检测要求

8.1 总体测试环境

测试内容在没有特殊情况的说明下，应按照以下物理环境进行测试：

a） 温度：0° C ~ 50° C；

b） 湿度：20% ~ 90%。

8.2 卡片测试要求

8.2.1 卡片生命周期测试

卡片生命周期测试应符合下列要求：

a） 测试目的：验证卡片生命周期中的各个状态符合 6.1 的要求；

b） 初始化要求：已写入卡片公钥证书；

c） 测试方法：设计测试用例，在卡片每个生命周期的状态下进行相关测试；

d） 评价准则： 预个人化状态的状态值为 01，个人化状态的状态值为 03，用户使用阶段的状态值为 07。

8.2.2 卡片 APDU 命令测试

8.2.2.1 外部认证

外部认证应符合下列要求：

a） 测试目的：验证卡片 APDU 命令：EXTERNAL AUTHENTICATE 应符合 6.5 的要求；

b） 初始化要求：已写入外部认证密钥；

c） 测试方法：发送外部认证命令；

d） 评价准则：外部认证成功。

8.2.2.2 写入卡片主控密钥

写入卡片主控密钥应符合下列要求：

a） 测试目的：验证卡片 APDU 命令：WRITE CCK 应符合 6.5 的要求；

b） 初始化要求：已写入外部认证密钥；

c） 测试方法：使用相关命令写入主控密钥；

d） 评价准则：外部认证成功，写入主控密钥成功。

8.2.2.3 取卡片公钥证书

取卡片公钥证书应符合下列要求：

a） 测试目的：验证卡片 APDU 命令：GET ICC CERTIFICATE 应符合 6.5 的要求；

b） 初始化要求：已写入外部认证密钥；

c） 测试方法：发送正确的命令，获取卡片公钥证书；

d） 评价准则：获取卡片公钥证书成功。

8.2.2.4 数据存储

数据存储应符合下列要求：

a） 测试目的：验证卡片 APDU 命令：STORE DATA 应符合 6.5 的要求；
b） 初始化要求：已写入外部认证密钥；
c） 测试方法：按照规范组织数据，包括密钥和非密钥数据，使用命令进行数据存储；
d） 评价准则：外部认证成功，store data 执行成功。

8.2.2.5 内部认证

内部认证应符合下列要求：
a） 测试目的：验证卡片 APDU 命令：INTERNAL AUTHENTICATE 应符合 6.5 的要求；
b） 初始化要求：已写入内部认证密钥；
c） 测试方法：发送正确的命令，进行内部认证；
d） 评价准则：内部认证指令成功。

8.2.3 终端授权流程测试

终端授权流程测试应符合下列要求：
a） 测试目的：验证终端授权流程中的写卡操作应符合 7.2.1 的要求；
b） 初始化要求：已写入卡片公钥证书；
c） 测试方法：按照规范设计测试步骤，进行卡片授权测试；
d） 评价准则： 授权流程中各指令执行正确，返回 9000 或者 61XX。

8.2.4 系统授权流程测试

系统授权流程测试应符合下列要求：
a） 测试目的：验证系统授权流程中的写卡操作应符合 7.2.1 的要求；
b） 初始化要求：已写入卡片公钥证书；
c） 测试方法：按照规范设计测试步骤，进行卡片授权测试；
d） 评价准则： 授权流程中各指令执行正确，返回 9000 或者 61XX。

8.2.5 线上授权流程测试

线上授权流程测试应符合下列要求：
a） 测试目的：验证线上 授权流程中的写卡操作应符合 7.2.3 的要求； 。
b） 初始化要求：已写入卡片公钥证书；
c） 测试方法：按照规范设计测试步骤，进行卡片授权测试；
d） 评价准则： 授权流程中各指令执行正确，返回 9000 或者 61XX。

8.3 终端测试

8.3.1 安全芯片

参考 7.1.2， 安全芯片应符合下列要求：
a） 符合 GB/T22186-2016 《信息安全技术 具有中央处理器的 IC 卡芯片安全技术要求》、GM/T 0028-2014《密码模块安全技术要求》5.5 规定的安全二级的要求，同时应支持随机数发生，随机数应符合 GM/T 0006—2012《密码应用标识规范》及 NIST 随机数检测标准；
b） 安全芯片需支持国密算法 SM2、SM3 和 SM4；
c） 支持非对称密码 RSA 2048 位算法；
d） 支持杂凑密码 SHA 256 算法；
e） 支持对称密码 AES 128 算法。

8.3.2 SAM 卡

参考 7.1.3， SAM 卡应符合下列要求：

a） 符合 GB/T22186-2016 《信息安全技术 具有中央处理器的 IC 卡芯片安全技术要求》、GM/T 0028-2014《密码模块安全技术要求》5.5 规定的安全二级的要求，同时应支持随机数发生，随机数应符合 GM/T 0006—2012《密码应用标识规范》及 NIST 随机数检测标准；

b） 安全芯片需支持国密算法 SM4；

c） 支持对称密码 AES 128 算法。

8.3.3 密码机

参考 7.1.4， 密码机应符合下列要求：

a） 符合 GB/T22186-2016 《信息安全技术 具有中央处理器的 IC 卡芯片安全技术要求》、GM/T 0028-2014《密码模块安全技术要求》5.5 规定的安全二级的要求，同时应支持随机数发生，随机数应符合 GM/T 0006—2012《密码应用标识规范》及 NIST 随机数检测标准；

b） 安全芯片需支持国密算法 SM4；

c） 支持对称密码 AES 128 算法。

8.3.4 终端授权流程

终端授权流程应符合下列要求：

a） 测试目的：验证终端授权流程应符合 7.2.1 的要求；

b） 初始化要求：已写入卡片公钥证书；

c） 测试方法：按照规范设计测试步骤，进行卡片授权测试；

d） 评价准则： 授权流程中终端发出的各指令均应符合规范。

8.3.5 系统授权流程

系统授权流程应符合下列要求：

a） 测试目的：验证系统授权流程应符合 7.2.2 的要求；

b） 初始化要求：已写入卡片公钥证书；

c） 测试方法：按照规范设计测试步骤，进行卡片授权测试；

d） 评价准则： 授权流程中终端发出的各指令均应符合规范。

8.3.6 线上授权流程

线上授权流程应符合下列要求：

a） 测试目的：验证线上授权流程应符合 7.2.3 的要求；

b） 初始化要求：已写入卡片公钥证书；

c） 测试方法：按照规范设计测试步骤，进行卡片授权测试；

d） 评价准则： 授权流程中终端发出的各指令均应符合规范。

8.3.7 应用流程测试

8.3.7.1 开锁流程正常测试

开锁流程正常测试应符合下列要求：

a） 测试目的：验证授权后的门卡的应用流程应符合 7.3 的要求；

b） 初始化要求：已写入卡片公钥证书；

c） 测试方法：按照规范设计测试步骤，使用正确授权的卡片进行开锁测试；

d） 评价准则： 开锁流程中，各指令均应符合规范。

8.3.7.2 开锁流程异常测试

开锁流程异常测试应符合下列要求：

a） 测试目的：验证授权后的门卡流程中的异常情况应符合 7.3 的要求；

b） 初始化要求：已写入卡片公钥证书；

c） 测试方法：按照规范设计测试步骤，使用未正确授权的卡片进行开锁测试，如，卡片状态不满足、密钥不正确等情况；

d） 评价准则： 开锁流程中，各指令均应符合规范。