社会保障（个人）卡规范
第 9 部分：PSAM 卡应用技术要求

引言

本部分作为《社会保障（个人）卡规范》的第 9 部分，包括以下主要内容：

——文件结构。定义了社会保障卡安全访问模块（PSAM 卡）的文件结构，及如何向社会保障 PSAM 卡导入本地应用密钥。

——密钥说明。定义了 PSAM 卡中密钥的类型、参数和记录格式等。

——安全管理。定义了 PSAM 卡对用户卡中涉及的所有计算类型进行安全计算的方法。

——应用方式。定义了在应用系统中如何使用 PSAM 卡。

——命令。定义了 PSAM 卡在应用中所涉及命令的使用条件、格式、响应信息等。

1 适用范围

本规范适用于人力资源和社会保障领域面向各类参保人员发行的社会保障卡。其使用对象主要是与社会保障卡应用相关的卡片设计、制造、管理、发行和受理以及应用系统的研制、开发、集成和维护等组织机构。

2 参考标准

ISO/IEC 9797．1：1997	信息技术　安全技术　电文鉴别代码(MACS)　第 1 部分：用块密码的机制
ISO/IEC 9797．2：2002	信息技术　安全技术　电文鉴别代码(MACS)　第 2 部分：专用散列函数的机械结构
ISO/IEC 10116：2006	信息技术　安全技术　n 位块加密算法的运算方法

3 定义

以下定义适用于本规范。

3.1 终端（Terminal）

为处理社会保障卡业务而在服务网点安装的设备，用于同 IC 卡的连接。它包括接口设备，也可包括其他部件和接口，例如与主机通信的接口。

3.2 命令（Command）

终端向 IC 卡发出的一条信息，该信息启动一个操作或请求一个应答。

3.3 响应（Response）

IC 卡处理完成收到的命令报文后，返回给终端的报文。

3.4 交易（Transaction）

持卡者和业务、管理部门之间根据社会保障卡所支持的应用接受、提供服务的行为。

3.5 功能（Fuction）

由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。

3.6 集成电路卡（IC 卡）（Integrated Circuit（s）Card）

内部封装一个或多个集成电路的 ID-1 型卡（如 ISO/IEC 7810、ISO/IEC 7811 第 1 至第 5 部分、ISO/IEC 7812 和 ISO/IEC 7813 中描述的）。

3.7 报文（Message）

由终端向卡或卡向终端发出的，不含传输控制字符的字节串。

3.8 报文鉴别代码（Message Authentication Code）

对交易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。

3.9 密钥（Key）

控制加密转换操作的符号序列。

3.10 密码算法（Cryptographic Algorithm）

为了隐藏或揭露信息内容而变换数据的算法。

3.11 社会保障应用（Social Security Application）

在人力资源和社会保障各专业领域管理和服务工作中的社会保障卡应用总称。

3.12 帐户划入（Wipe In Account）

将持卡人基本医疗保险个人帐户上尚未写入卡内的资金额度写到卡内基本医疗保险个人帐户中。

3.13 医疗消费（Medical Treatment Consume）

指持卡人就医、取药等与医疗有关的消费，从资金来源上划分，包括帐户支付、现金支付、统筹基金支付。卡内记录帐户支付、个人自付和统筹基金支付三种形式。

3.14 帐户支付（Account Payment）

指持卡人从卡内基本医疗保险个人帐户中支付医疗费用。

4 缩略语和符号表示

以下缩略语和符号表示适用于本规范。

ADF	应用数据文件（Application Definition File）
AID	应用标识符（Application Identifier）
b	二进制（Binary）
CLA	命令报文的类别字节（Class Byte of the Command Message）
cn	压缩数字（Compressed Numeric）
DDF	目录定义文件（Directory Definition File）
DEA	数据密码算法（Data Encryption Algorithm）
DF	专用文件（Dedicated File）
DIR	目录（Directory）
EF	基本文件（Elementary File）
FCI	文件控制信息（File Control Information）
IC	集成电路（Integrated Circuit）
IEC	国际电工委员会（International Electrotechnical Commission）
INS	命令报文的指令字节（Instruction Byte of Command Message）

ISO	国际标准化组织（International Organization for Standardization）
Km	主控密钥（Master Key）
Ks	过程密钥（Session Key）
Lc	终端发出的命令数据的实际长度（Exact Length of Data Sent by the TAL in a Case 3 or 4 Command）
Le	响应数据的最大期望长度（Maximum Length of Data Expected by the TAL in Response to a Case 2 or 4 Command）
MAC	报文鉴别代码（Message Authentication Code）
MF	主控文件（Master File）
P1	参数 1（Parameter 1）
P2	参数 2（Parameter 2）
PSAM	服务网点终端安全存取模块（Practice Secure Access Module）
RFU	保留为将来使用（Reserved for Future Use）
SFI	短文件标识符（Short File Identifier）
SSSE	社会保障系统环境（Social Security System Environment）
SW1	状态码 1（Status Word One）
SW2	状态码 2（Status Word Two）
TAC	交易验证码（Transaction Authorization Cryptogram）
TAL	终端应用层（Terminal Application Layer）
‘0’-‘9’ ‘A’-‘F’	十六进制数字
xx	任意值

5 文件结构

图 1 给出了社会保障 PSAM 卡的文件结构。

社会保障 DES 算法环境 DDF：

FID=’3F00’，AID=’7378312E73682EC9E7BBE1B1A3D5CF’

社会保障 SSF33 算法环境 DDF：

FID=’DDF1’，AID=’7378322E73682EC9E7BBE1B1A3D5CF’

在任何情况下，均可以通过 SELECT 命令进入以上两个环境。

DIR 目录数据文件： FID = ‘0001’，线性变长记录文件。

卡片公共信息文件： FID = ‘0015’，二进制文件。

终端信息文件： FID = ‘0016’，二进制文件。

DES 算法环境社会保障应用 ADF：

FID = ‘DF01’，AID = ‘D15600000590’

SSF33 算法环境社会保障应用 ADF：

FID = ‘DF01’，AID = ‘D15600000590’

终端交易序号文件： FID = ‘0019’，二进制文件。

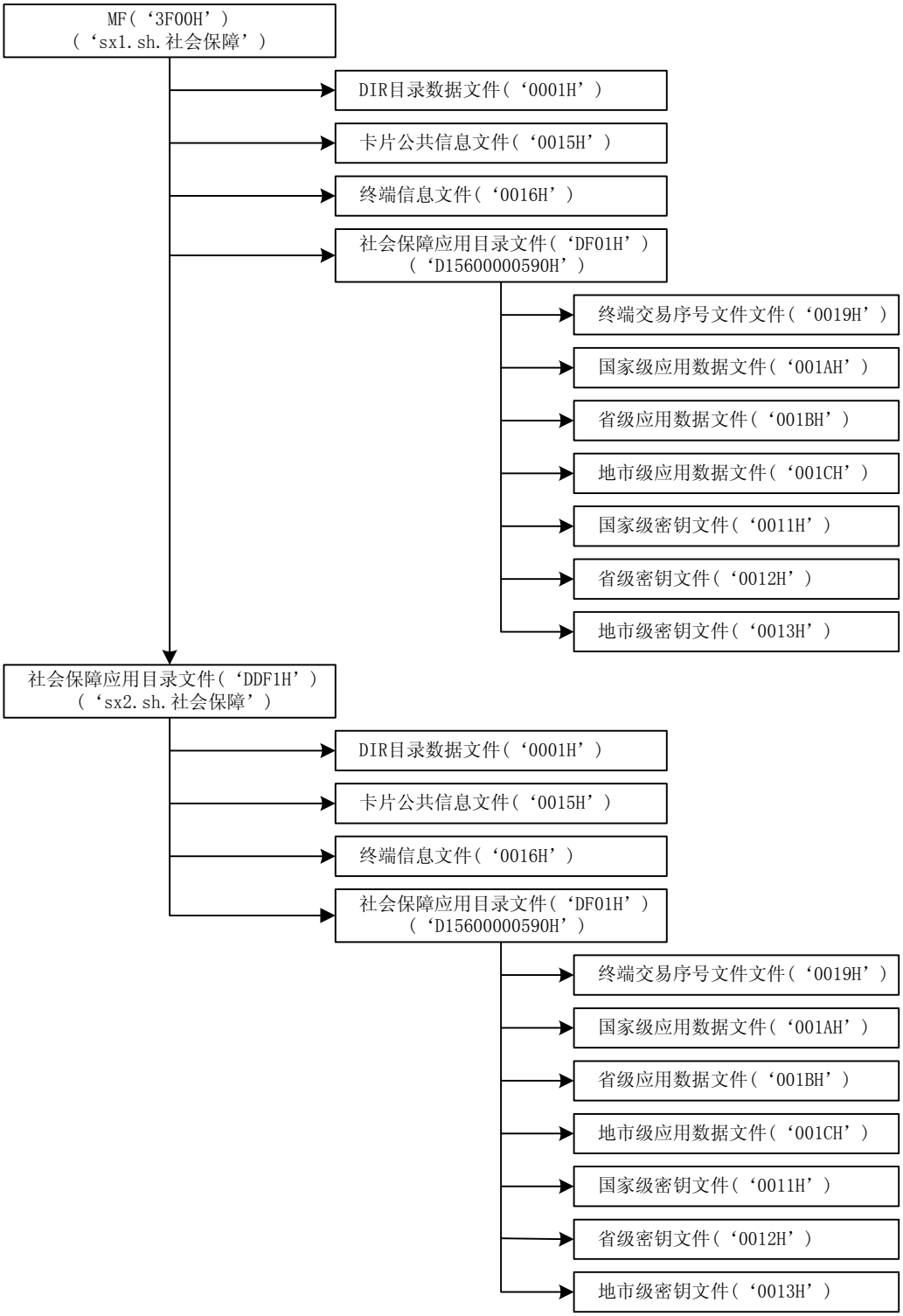


图 1　社会保障 PSAM 卡文件结构

国家级应用信息文件：FID = ‘001A’，二进制文件。

省级应用信息文件：　FID = ‘001B’，二进制文件。

地市级应用信息文件：FID = ‘001C’，二进制文件。

国家级密钥文件：　FID = ‘0011’。用密钥 KID-01 认证授权后，ADF-MK 控制写入国家

级密钥（密文+MAC）。

省级密钥文件：　FID = ‘0012’。 用密钥 KID-02 认证授权后，ADF-MK 控制写入省级密钥（密文+MAC）。

地市级密钥文件：　FID = ‘0013’。用密钥 KID-03 认证授权后，ADF-MK 控制写入地市级密钥（密文+MAC）。

注：

DDF-MK 是 DDF 文件的主控密钥（MF 是最高层的 DDF）；ADF-MK 是 ADF 文件的主控密钥。

透明文件：文件数据是通过连续空间中的字节地址进行存取。

记录文件：数据以记录为单位进行存取，同一文件内所有记录的长度可以不相等。同一文件内最多可以容纳 254 条记录。

5.1 DIR 目录数据文件

表 1 DIR 目录数据文件

文件标识（SFI）		‘0001’
文件类型		记录
文件大小		
文件存取控制	读=自由	改写= DDF-MK
记录 1		
记录 2		

5.2 卡片公共信息文件

表 2 卡片公共信息文件

文件标识（SFI）			‘0015’
文件类型			透明
文件大小			15
文件存取控制		读=自由	改写= DDF-MK
字节	数据元	类型	长度
1	发行机构标识	b	1
2－11	PSAM 序列号	cn	10
12	PSAM 版本号	b	1
13	密钥卡类型	b	1
14－15	发卡方自定义 FCI 数据	b	2

5.3 终端信息文件

表 3 终端信息文件

文件标识（SFI）			‘0016’
文件类型			透明
文件大小			6
文件存取控制		读=自由	改写= DDF-MK
字节	数据元	类型	长度
1－6	终端机编号	cn	6

5.4 终端交易序号文件

表 4 终端交易序号文件

文件标识（SFI）			‘0019’
文件类型			透明
文件大小			4
文件存取控制		读=自由	改写=不允许
字节	数据元	类型	长度
1－4	终端交易序号	b	4

5.5 国家级应用信息文件

表 5 国家级应用信息文件

文件标识（SFI）			‘001A’
文件类型			透明
文件大小			10
文件存取控制		读=自由	改写= KID-01
字节	数据元	类型	长度
1	国家级医疗消费密钥索引号	b	1
2	国家级鉴别密钥版本号	b	1
3－6	应用启用日期	cn	4
7－10	应用有效日期	cn	4

5.6 省级应用信息文件

表 6 省级应用信息文件

文件标识（SFI）			‘001B’
文件类型			透明
文件大小			10
文件存取控制		读=自由	改写= KID-02
字节	数据元	类型	长度
1	省级医疗消费密钥索引号	b	1
2	省级鉴别密钥版本号	b	1
3－6	应用启用日期	cn	4
7－10	应用有效日期	cn	4

5.7 地市级应用信息文件

表 7 地市级应用信息文件

文件标识（SFI）			‘001C’
文件类型			透明
文件大小			10
文件存取控制		读=自由	改写= KID-03
字节	数据元	类型	长度
1	地市级医疗消费密钥索引号	b	1
2	地市级鉴别密钥版本号	b	1
3－6	应用启用日期	cn	4
7－10	应用有效日期	cn	4

5.8 国家级密钥文件

表 8 国家级密钥文件

文件标识（SFI）		‘0011’
文件类型		密钥
文件大小		
文件存取控制	使用=自由	改写= KID-01
密钥记录 1		
密钥记录 2		
...		

5.9 省级密钥文件

表 9 省级密钥文件

文件标识（SFI）		‘0012’
文件类型		密钥
文件大小		
文件存取控制	使用=自由	改写= KID-02
密钥记录 1		
密钥记录 2		
..		

5.10 地市级密钥文件

表 10 地市级密钥文件

文件标识（SFI）		‘0013’
文件类型		密钥
文件大小		
文件存取控制	使用=自由	改写= KID-03
密钥记录 1		
密钥记录 2		
..		

6 密钥说明

社会保障 PSAM 卡中，除主控密钥 MK 存储在 MF、DDF 或 ADF 缺省的位置上外，其余所有密钥都以记录的形式存储在密钥文件中。每一条密钥包括用途、标识/版本、算法和密钥数据等参数信息。

6.1 密钥记录格式

格式 1 MAC 密钥，加密密钥，MAC、加密密钥，帐户划入密钥，TAC 密钥

用途	标识	RFU	算法	使用权限	RFU	RFU	密钥值

格式 2 医疗消费密钥

用途	版本	RFU	算法	使用权限	RFU	RFU	密钥值

6.2 参数说明

用途： 左 3 位（b8-b6）表示密钥的分散级数，右 5 位定义密钥的类型。

标识： 密钥的标识符。

版本： 密钥的版本序号。

算法： 安全计算法。‘00h’为 Triple-DES 算法，同时决定密钥值的长度为 16 个字节；‘01h’为 DES 算法，同时决定密钥值的长度为 8 个字节；‘02h’为 SSF33 算法，同时决定密钥值的长度为 16 个字节。

使用权限： 两个字节，‘0000h’。

密钥值： 有效长度为 8 个字节（DES 算法）或 16 个字节（Triple-DES 算法、SSF33 算法）。

RFU： 保留将来使用，‘00h’。

6.3 密钥类型

——2，医疗消费密钥：只能进行医疗消费认证

——6，MAC 密钥：只能进行 MAC 计算

——7，加密密钥：只能进行加密计算

——8，MAC、加密密钥：可以 MAC 和加密计算

——9，帐户划入密钥：帐户划入专用密钥

——12，TAC 密钥：计算 TAC 的密钥

7 安全管理

7.1 安全计算方法（DES 算法）

安全计算涉及用户卡中的所有计算类型。包括数据加密计算、普通 MAC 计算、医疗消费 MAC1 计算和 MAC2 认证等。MAC 总是命令或命令响应数据域中最后一个数据元素。

本节涉及的数据密码算法 DEA 均是 DES 算法。

7.1.1 密钥分散计算方法

对单倍长密钥，用指定的分散因子作为输入数据，做 DEA 加密计算，产生的 8 个字节的结果作为子密钥。参见图 2。

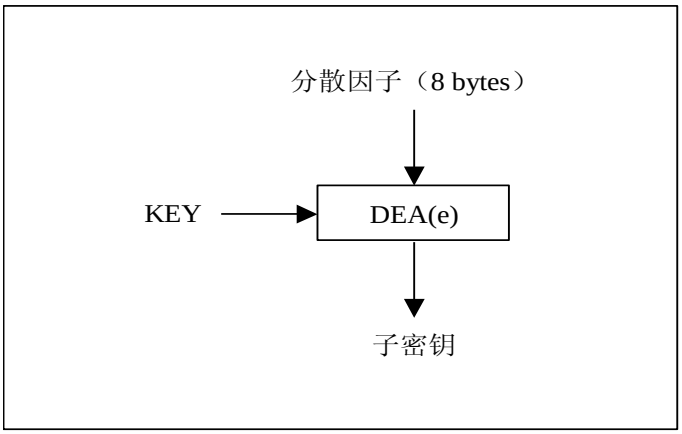


图 2　单倍长密钥分散出单倍长子密钥

对双倍长密钥，需要分别推导子密钥的左右两部分。

左半部分的推导方法是：

——将系统提供的分散因子（8 个字节）作为输入数据；

——用主密钥作为加密密钥，对输入数据进行 Triple-DEA 运算。

右半部分的推导方法是：

——将系统提供的分散因子（8 个字节）求反作为输入数据；

——用主密钥作为加密密钥，对求反后的输入数据进行 Triple-DEA 运算。

将左右两部分连接在一起，产生双倍长子密钥，参见图 3。

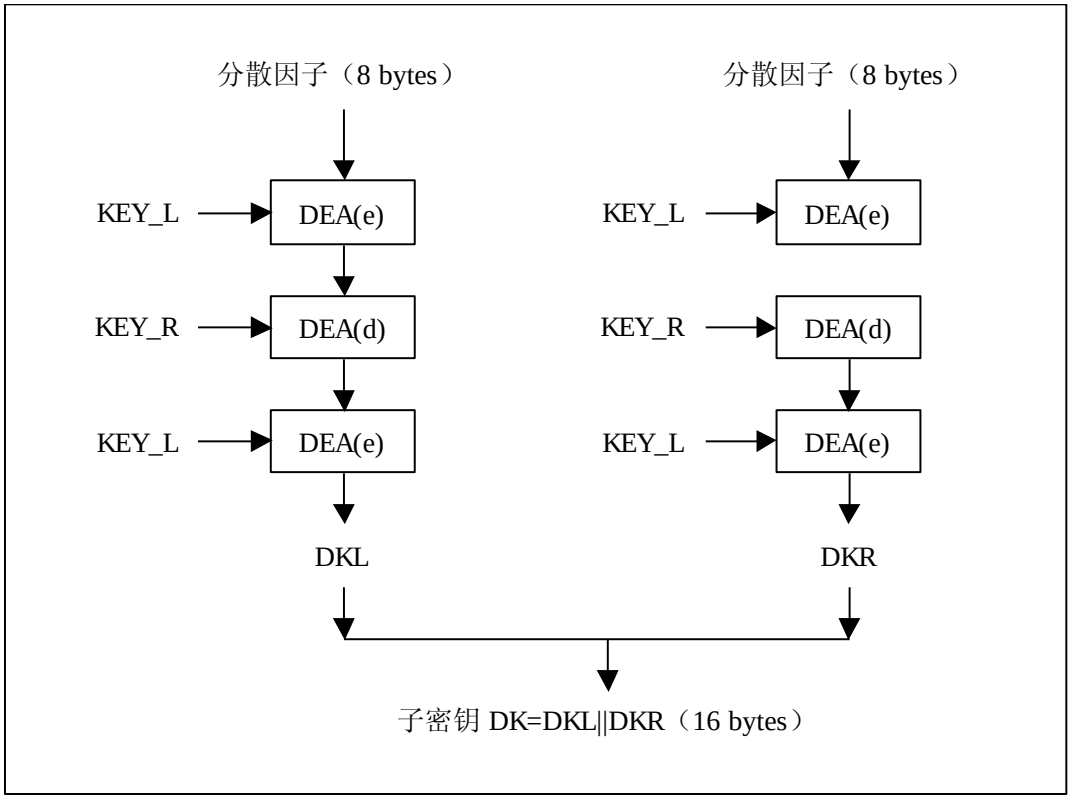


图 3　双倍长密钥分散出双倍长子密钥

7.1.2　数据加密的计算方法

CREATE KEY 和 CHANGE KEY 命令中，数据加密的计算方法如下：

第一步：用 LD（1 个字节）表示明文数据的长度，在明文数据前加上 LD 产生新的数据块。

第二步：将该数据块分成 8 个字节为单位的数据块，分别表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~8 个字节。

第三步：如果最后（或唯一）的数据块的长度是 8 个字节，则转到第四步。

如果最后（或唯一）的数据块的长度不足 8 个字节，则在其后加入 16 进制数‘80’，如果长度达到 8 个字节，则转到第四步；否则，在其后加入 16 进制数‘00’直到长度达到 8 个字节。

第四步：按照图 4 所述的算法使用指定密钥对每一个数据块进行加密。

第五步：计算结束后，所有加密后的数据块依照原顺序连接在一起。

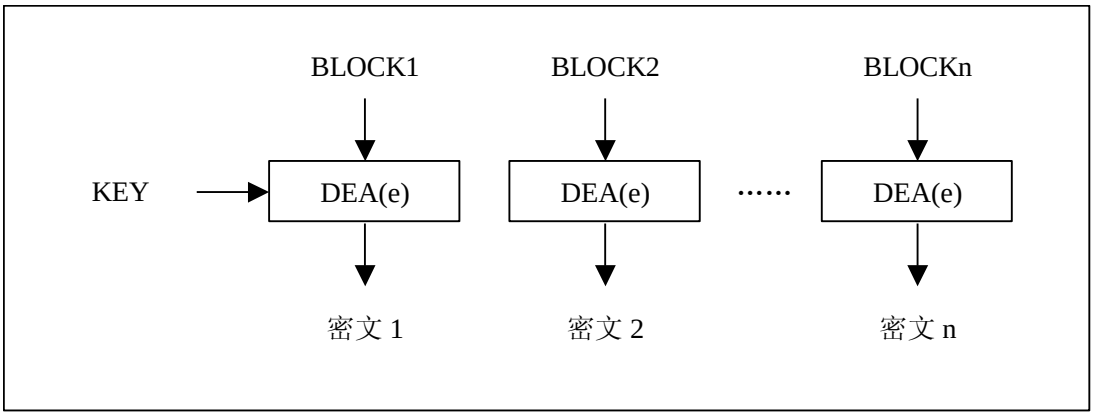


图 4 （A）单倍长 DES 密钥数据密码算法

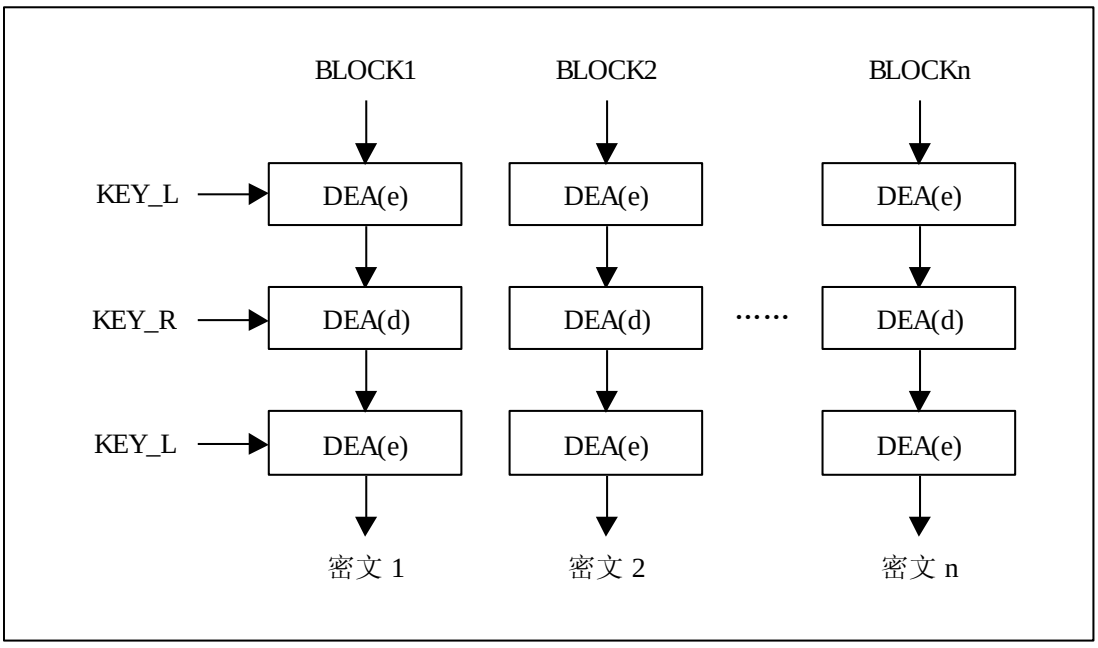


图 4 （B）双倍长 DES 密钥数据密码算法

7.1.3 安全报文 MAC 的计算方法

CREATE KEY 和 CHANGE KEY 命令中，MAC 的计算方法如下：

第一步：终端通过向 IC 卡发 GET CHALLENGE 命令获得一个 4 个字节的随机数，其右侧补‘00 00 00 00’作为初始值。

第二步：将 5 个字节命令头（CLA，INS，P1，P2，Lc）和命令数据域中的明文或密文数据连接在一起形成数据块。其中，Lc 的长度应是数据长度加上将计算出的 MAC 的长度（4 个字节）后得到的实际长度。

第三步：将该数据块分成 8 个字节为单位的数据块，分别表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~8 个字节。

第四步：如果最后的数据块的长度是 8 个字节的话，则在该数据块之后再加一个完整的 8 个字节数据块‘80 00 00 00 00 00 00 00’，转到第五步。

如果最后的数据块的长度不足 8 个字节，则在其后加入 16 进制数‘80’，如果长度达到 8 个字节，则转到第五步；否则，继续在其后加入 16 进制数‘00’直至长度达到 8 个字节。

第五步：按照图 5 所述的算法，使用指定密钥对这些数据块进行加密来产生 MAC。

第六步：最终取计算结果（高 4 个字节）作为 MAC。

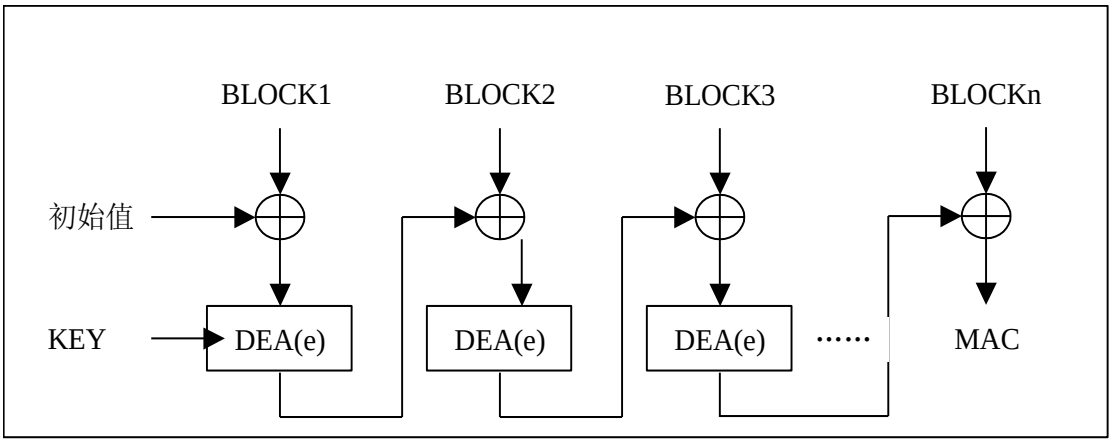


图 5　（A）安全报文中单倍长 DES 密钥 MAC 算法

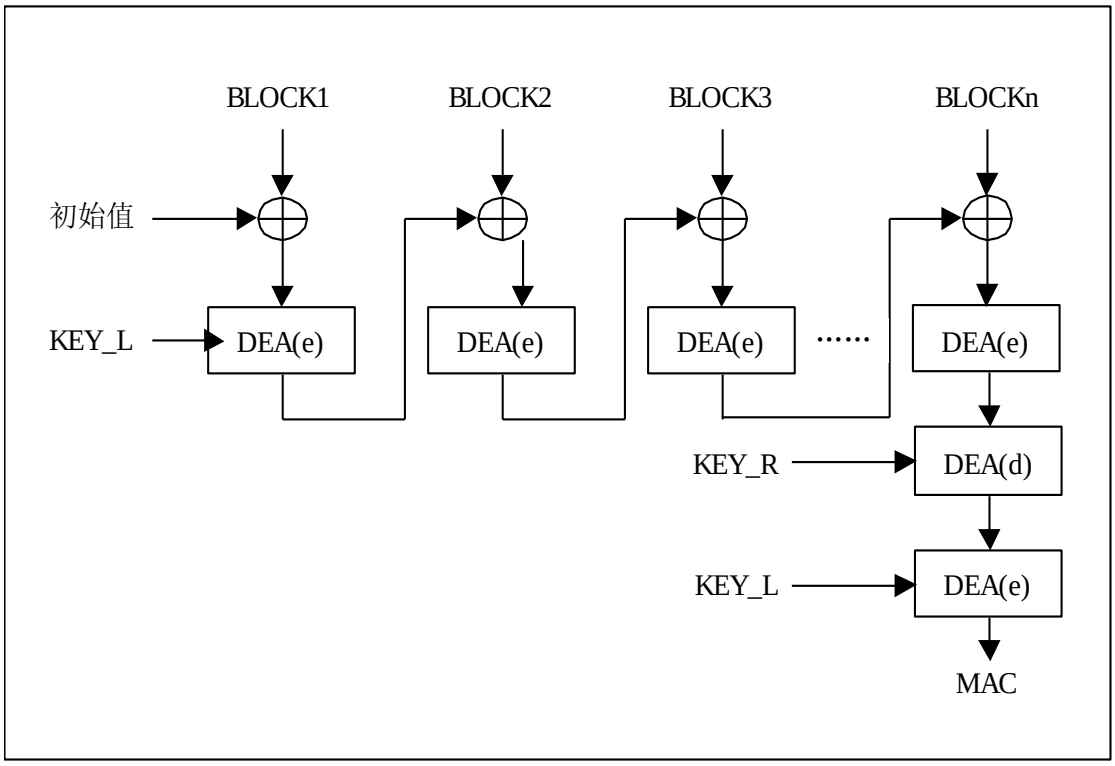


图 5　（B）安全报文中双倍长 DES 密钥 MAC 算法

7.1.4 医疗保险脱机交易中的安全报文（MAC1、MAC2）的计算方法

MAC1 和 MAC2 的计算方法请参照《社会保障（个人）卡规范》第 4 部分：安全机制。

7.1.5 外部认证指令过程密钥的计算方法

用指定密钥对过程密钥产生因子（8 字节）做 DES 加密，得到的加密结果即为过程密钥。如图 6 和图 7。

过程密钥产生因子是卡内当前有效的随机数，如果不足 8 字节，则右补’00’，补齐 8 字节构成过程密钥产生因子。

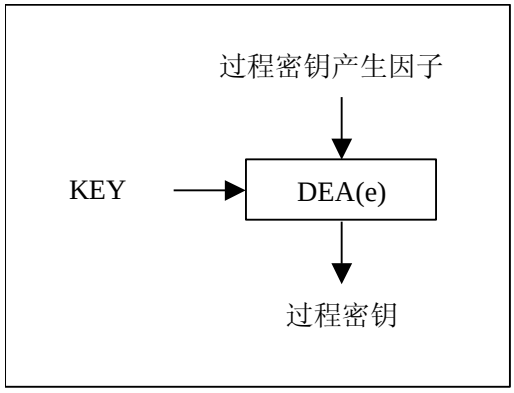


图 6　单倍长密钥产生过程密钥

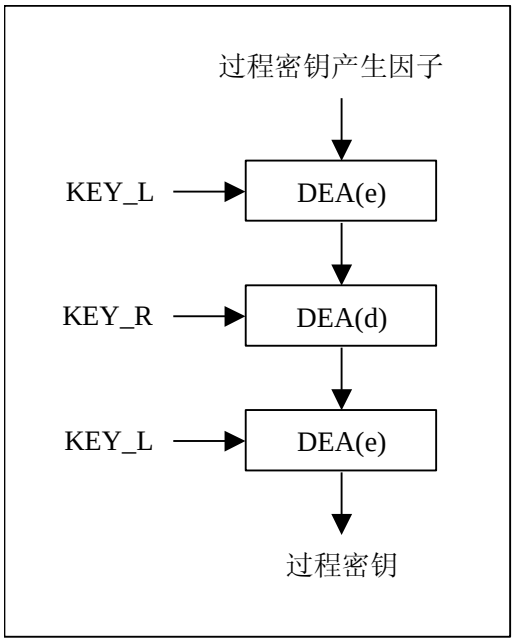


图 7　双倍长密钥产生过程密钥

7.2 安全计算方法（SSF33 算法）

安全计算涉及用户卡中的所有计算类型。包括数据加密计算、普通 MAC 计算、医疗消费 MAC1 计算和 MAC2 认证等。MAC 总是命令或命令响应数据域中最后一个数据元素。

本节涉及的数据密码算法 DEA 均是 SSF33 算法。

7.2.1 密钥分散计算方法

分散因子为 8 字节，用分散因子作为输入数据的高 8 字节，对分散因子求反作为输入数据的低 8 字节，使用指定密钥对输入数据做 DEA 加密运算，产生的 16 字节结果作为子密钥，

参见图 8。

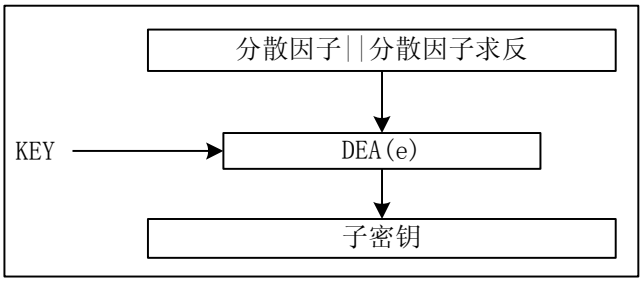


图 8　SSF33 算法的密钥分散计算

7.2.2　数据加密的计算方法

CREATE KEY 和 CHANGE KEY 命令中，数据加密的计算方法如下：

第一步：用 LD（1 个字节）表示明文数据的长度，在明文数据前加上 LD 产生新的数据块。

第二步：将该数据块分成 16 个字节为单位的数据块，分别表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~16 个字节。

第三步：如果最后（或唯一）的数据块的长度是 16 个字节，则转到第四步。

如果最后（或唯一）的数据块的长度不足 16 个字节，则在其后加入 16 进制数‘80’，如果长度达到 16 个字节，则转到第四步；否则，在其后加入 16 进制数‘00’直到长度达到 16 个字节。

第四步：按照图 9 所述的算法使用指定密钥对每一个数据块进行加密。

第五步：计算结束后，所有加密后的数据块依照原顺序连接在一起。

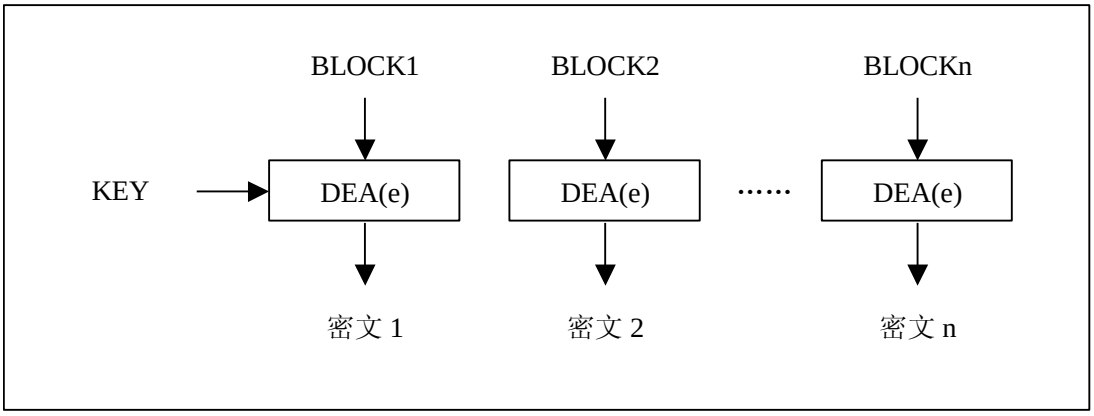


图 9　SSF33 算法的数据加密

7.2.3　安全报文 MAC 的计算方法

CREATE KEY 和 CHANGE KEY 命令中，MAC 的计算方法如下：

第一步：终端通过向 IC 卡发 GET CHALLENGE 命令获得一个 4/8/16 字节的随机数.若随机数据长度不足 16 字节，在其右侧补’00’，补齐 16 字节作为初始值。

第二步：将 5 个字节命令头（CLA，INS，P1，P2，Lc）和命令数据域中的明文或密文数据连接在一起形成数据块。其中，Lc 的长度应是数据长度加上将计算出的 MAC 的长度（4 个字节）后得到的实际长度。

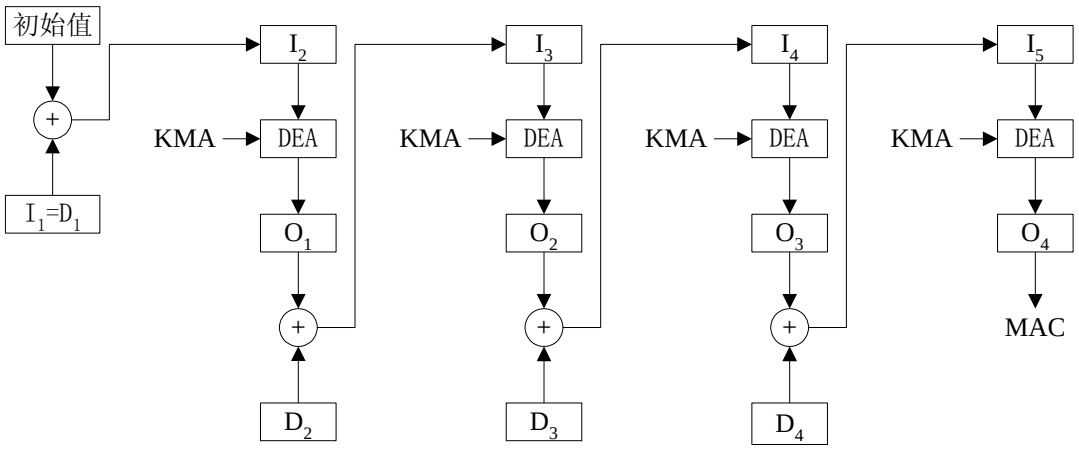
第三步：将该数据块分成 16 个字节为单位的数据块，分别表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~16 个字节。

第四步：如果最后的数据块的长度是 16 个字节的话，则在该数据块之后再加一个完整的 16 个字节数据块‘80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00’，转到第五步。

如果最后的数据块的长度不足 16 个字节，则在其后加入 16 进制数‘80’，如果长度达到 16 个字节，则转到第五步；否则，继续在其后加入 16 进制数‘00’直至长度达到 16 个字节。

第五步：按照图 10 所述的算法，使用指定密钥对这些数据块进行加密来产生 MAC。

第六步：将 16 字节运算结果按 4 字节分块做异或运算，最终结果作为 MAC。



图例：

I = 输入　　D = 数据块

DEA = SSF33 算法（加密模式）　　KMA = MAC 密钥

O = 输出　　+ = 异或运算

图 10　SSF33 算法的 MAC 算法

7.2.4　医疗保险脱机交易中的安全报文（MAC1、MAC2）的计算方法

MAC1 和 MAC2 的计算方法请参照《社会保障（个人）卡规范》第 4 部分：安全机制。

7.2.5　外部认证指令过程密钥的计算方法

用指定密钥对过程密钥产生因子（16 字节）做 SSF33 加密，得到的加密结果即为过程密钥。如图 11。

过程密钥产生因子是卡内当前有效的随机数，如果不足 16 字节，则右补’00’，补齐 16 字节构成过程密钥产生因子。

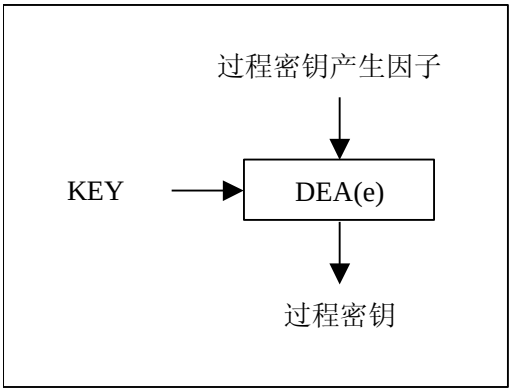


图 11　SSF33 算法过程密钥的计算方法

7.3 分散产生子密钥的方式

分散密钥通过 DELIVERY SESSION KEY 命令进行。密钥经分散产生子密钥，并通过进一步变换产生过程密钥。

医疗消费密钥对应医疗消费 MAC1 计算和 MAC2 认证专用命令。

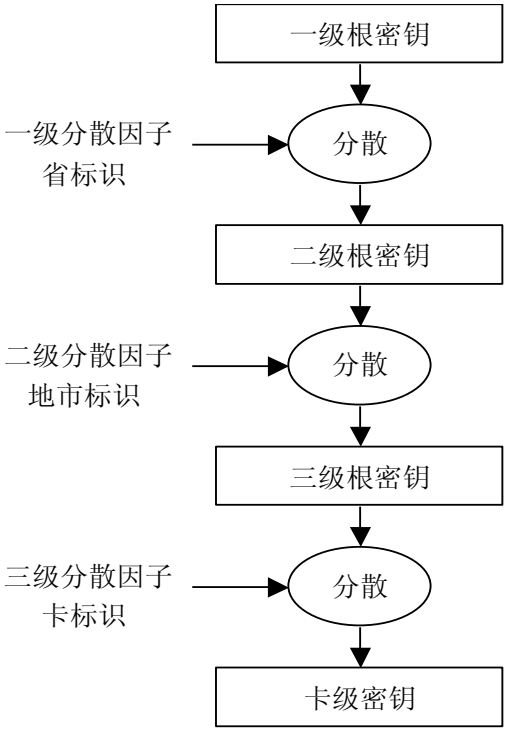


图 12　社会保障卡密钥分散过程

7.3.1 一级分散因子

一级分散因子是以省份标识号为基本元素构成的，构成方法如下：取用户卡中 MF 下的 EF05 文件中的“卡的识别码”记录的前三个字节“应用城市代码”（6 位十进制数），将其展开为 6 个字节的 ASCII 码（如：650100 展开为‘36 35 30 31 30 30’），取其中头两个字节，后补十六进制数’30 30 30 30 73 68’，形成 8 个字节的一级分散因子。

7.3.2 二级分散因子

二级分散因子是以地市标识号为基本元素构成的，构成方法如下：取用户卡中 MF 下的 EF05 文件中的“卡的识别码”记录的前三个字节“应用城市代码”（6 位十进制数），将其展开为 6 个字节的 ASCII 码（如：650100 展开为‘36 35 30 31 30 30’），后补十六进制数‘73 78’，形成 8 个字节的二级分散因子。

7.3.3 三级分散因子

三级分散因子是由卡标识号构成的，构成数据为：用户卡复位应答历史字节的第 6~13 个字节。历史字节定义见《社会保障（个人）卡规范》第 2 部分：机电特性、逻辑接口与传输协议，其中 T8-T9 为发卡地区所在地的行政区划代码前四位，如长春市位‘2201’，TA-TD 由发卡地区自行编排并保持每张卡的唯一性。

终端机编号定义：前 6 位为发卡地区城市代码，第 7-12 位由 PSAM 卡发放机构定义。

7.4 数据的安全计算步骤

数据的安全计算是指对外部提供的数据进行 DEA 变换。主要计算有：DEA 加密、DEA

MAC 计算。DEA 可以是 DES 算法，也可以是 SSF33 算法。

PSAM 卡中完成数据的安全计算必须经过两个步骤：

1. 使用 DELIVERY SESSION KEY 命令，在卡内准备好参与计算的密钥；

2. 使用 CIPHER DATA 命令，用产生的临时密钥对外部提供的数据进行处理。

8 应用系统的兼容性

在 PSAM 卡的使用中，各地应确保其应用软件可以满足载有不同密钥级别的 PSAM 卡兼容性问题，即对于分别载有三级根密钥、二级根密钥、一级根密钥的不同 PSAM 卡，应同时支持。各地可以选择以下方案。

方案一：

应用软件每次在使用某一密钥时，如果分散因子的个数与 PSAM 卡内要求的个数不符（即 PSAM 卡实际密钥分散级数与应用软件首选的密钥级数不一致），命令将报错，此时应用软件应尝试另外两种分散级数的可能性，直到获得命令的正确响应。

方案二：

含有 PSAM 卡的终端，在开机时为 PSAM 卡（支持多 PSAM 卡的终端需针对每个 PSAM 卡）建立个卡内密钥分散级数的索引表，以便应用程序根据实际密钥的分散级数使用密钥。建立索引表的方法参见方案一。

9 命令

9.1 SELECT 命令

9.1.1 命令描述

“SELECT”命令通过文件名或 AID、文件标识符来选择 IC 卡中的 SSSE、DDF 或 ADF，通过文件标识符来选择 ADF 中的 EF。

命令执行成功后，SSSE、DDF 或 ADF、EF 的路径被设定。

除选择 EF 外，IC 卡的响应报文应由回送的 FCI 组成。

9.1.2 使用条件和安全

无。

9.1.3 命令格式

表 11 命令格式

代码	值
CLA	‘00’
INS	‘A4’
P1	‘00’ --- 按照 FID 选择 DF ‘02’ --- 按照 FID 选择 EF ‘04’ --- 按照 AID 选择 DF
P2	‘00’
Lc	‘02’ --- P1=’00’/’02’ ‘05’~’10’ --- P1=’04’
Data	空、FID 或 AID
Le	响应 FCI 信息的长度

9.1.4 响应信息

响应信息中可能返回的状态码见表 12：

表 12 响应信息

SW1	SW2	含 义
‘67’	‘00’	P1P2 与 Lc 不一致
‘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

9.2 GET CHALLENGE 命令

9.2.1 命令描述

向卡片请求一个用于安全相关过程（例如：安全报文、安全鉴别）的随机数。

9.2.2 使用条件和安全

无条件。

9.2.3 命令格式

表 13 命令格式

代码	值
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’
Lc	不存在
Data	不存在
Le	‘04’/’08’ --- DES 算法 ‘04’/’08’/’10’ --- SSF33 算法

9.2.4 响应信息

响应报文数据域包括随机数，长度为指定字节数。

响应信息中可能返回的状态码见表 14：

表 14 响应信息

SW1	SW2	含 义
‘6A’	‘86’	P1、P2 参数错
‘67’	‘00’	Lc 错误

9.3 INITIALIZE ENVIRONMENT 命令

9.3.1 命令描述

社会保障 PSAM 卡环境初始化。

9.3.2 使用条件和安全

无。

9.3.3 命令格式

表 15　命令格式

代码	值
CLA	‘BF’
INS	‘EC’
P1	‘00’
P2	‘00’
Lc	‘01’
Data	社会保障（个人）卡的数据项“卡的识别码”左边第一个字节
Le	不存在

9.3.4　响应信息

响应信息中可能返回的状态码见表 16：

表 16　响应信息

SW1	SW2	含 义
‘67’	‘00’	Lc 错误
‘69’	‘85’	使用条件不满足
‘6A’	‘80’	命令数据域错误
‘6A’	‘86’	P1、P2 参数错

9.4　EXTERNAL AUTHENTICATION 命令

9.4.1　命令描述

使用指定密钥和当前有效的随机数，对外部输入数据进行认证，认证通过，将获得指定密钥对应的权利。

DES 算法认证数据的获得：使用指定密钥的过程密钥对认证原始数据做 DES 加密，得到 8 字节认证数据。过程密钥的计算见 7.1.5

SSF33 算法认证数据的获得：认证原始数据右补’00’至 16 字节，使用指定密钥的过程密钥对补零后的认证原始数据做 SSF33 加密，将加密结果做左右 8 字节的异或，得到认证数据。过程密钥的计算见 7.2.5。

9.4.2　使用条件和安全

无条件。

命令格式

表 17　命令格式

代码	值
CLA	‘00’
INS	‘82’
P1	‘00’
P2	认证密钥索引
Lc	‘10’/’11’
Data	认证数据||认证原始数据||认证密钥版本
Le	不存在

9.4.3 响应信息

响应信息中可能返回的状态码见表 18：

表 18 响应信息

SW1	SW2	含 义
‘6A’	‘86’	P1、P2 参数错
‘69’	‘85’	当前应用不存在
‘67’	‘00’	Lc 错误
‘69’	‘84’	随机数无效
‘6A’	‘88’	密钥未找到
‘69’	‘82’	密钥使用条件不满足
‘69’	‘83’	密钥锁定

9.5 CREATE KEY 命令

9.5.1 命令描述

CREATE KEY 命令用于建立一个新的密钥。

MAC 密钥，加密密钥，MAC、加密密钥，帐户划入密钥，TAC 密钥的信息结构：

用途+标识+‘00’+ 算法+‘00 00 00 00’+密钥值

医疗消费密钥的数据结构：

用途+版本+‘00’+ 算法+‘00 00 00 00’+密钥值

使用应用主控密钥对以上结构进行加密和计算 MAC，产生命令的数据域数据。

9.5.2 使用条件和安全

CREATE KEY 命令执行必须满足密钥改写控制属性。

9.5.3 命令格式

表 19 命令格式

代 码	值
CLA	‘84’
INS	‘D4’
P1	‘00’
P2	密钥文件标识
Lc	DES 算法：‘1C’或 ‘24’ SSF33 算法：‘24’
DATA	密文密钥信息||MAC
Le	不存在

9.5.4 响应信息

响应信息中可能返回的状态码见表 20：

表 20 响应信息

SW1	SW2	含 义
‘90’	‘00’	命令执行成功
‘65’	‘81’	写 EEPROM 失败
‘67’	‘00’	Lc 长度错误

续表

SW1	SW2	含 义
‘69’	‘82’	不满足安全状态
‘69’	‘83’	认证密钥锁定
‘69’	‘84’	引用数据无效（未申请随机数）
‘69’	‘85’	使用条件不满足
‘69’	‘88’	安全信息（MAC 和密文）数据错误
‘6A’	‘80’	数据域参数错误
‘6A’	‘81’	功能不支持
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到密钥数据
‘6A’	‘84’	文件空间已满
‘6A’	‘86’	P1、P2 参数错
‘6A’	‘88’	未找到密钥数据
‘6D’	‘00’	命令不存在
‘6E’	‘00’	CLA 错

9.6 CHANGE KEY 命令

9.6.1 命令描述

CHANGE KEY 命令用于更新一个已经存在的密钥。

MAC 密钥，加密密钥，MAC、加密密钥，帐户划入密钥，TAC 密钥的信息结构：

用途+标识+‘00’+密钥值

医疗消费密钥的数据结构：

用途+版本+‘00’+密钥值

使用应用主控密钥对以上结构进行加密和计算 MAC，产生命令的数据域数据。

9.6.2 使用条件和安全

CHANGE KEY 命令执行必须满足密钥改写控制属性。

9.6.3 命令格式

表 21 命令格式

代 码	值
CLA	‘84’
INS	‘D4’
P1	‘01’
P2	密钥文件标识
Lc	DES 算法：‘14’或‘1C’ SSF33 算法：‘24’
DATA	密文密钥信息||MAC
Le	不存在

9.6.4 响应信息

响应信息中可能返回的状态码见表 22：

表 22　响应信息

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

9.7　DELIVERY SESSION KEY 命令

9.7.1　命令描述

DELIVERY SESSION KEY 命令将指定的密钥先进行分散，然后产生过程密钥，并临时存放在卡中。

9.7.2　使用条件和安全

无条件。

9.7.3　命令格式

表 23 命令格式

代码	值
CLA	‘BF’
INS	‘DE’
P1	密钥用途
P2	密钥标识
Lc	M+8*N M 为过程密钥产生因子长度，M=8（DES 算法）/16（SSF33 算法） N 为分散级数，N=0/1/2/3
DATA	分散因子||过程密钥产生因子
Le	不存在

9.7.4 响应信息

响应信息中可能返回的状态码见表 24：

表 24 响应信息

SW1	SW2	含 义
‘90’	‘00’	命令执行成功
‘67’	‘00’	Lc 长度错误
‘69’	‘82’	不满足安全状态
‘69’	‘83’	认证密钥锁定
‘69’	‘85’	使用条件不满足
‘6A’	‘80’	分散级数不符
‘6A’	‘81’	功能不支持
‘6A’	‘86’	P1、P2 参数错
‘6A’	‘88’	未找到密钥数据
‘6D’	‘00’	命令不存在
‘6E’	‘00’	CLA 错

9.8 CIPHER DATA 命令

9.8.1 命令描述

CIPHER DATA 命令用于对输入数据进行加密或 MAC 安全计算。加解密采用 ECB 模式，计算 MAC 采用 CBC 模式。

9.8.2 使用条件和安全

CIPHER DATA 命令执行前，必须先执行 DELIVERY SESSION KEY 命令。当 P1=‘00’、‘01’或 ‘05’时，CIPHER DATA 命令在完成同类型计算前，临时密钥寄存器中的密钥保持有效。同类型计算指的是：加密计算，MAC 计算。当 P1=‘05’或 ‘07’时，第一个数据块为 MAC 计算初始值。

9.8.3 命令格式

表 25 命令格式

代码	值
CLA	‘80’
INS	‘FA’
P1	‘00’ 无后续块加密 ‘01’ 最后一块 MAC 计算 ‘02’ 有后续块加密 ‘03’ 下一块 MAC 计算 ‘05’ 唯一一块 MAC 计算 ‘07’ 第一块 MAC 计算
P2	‘00’

续表

代码	值
Lc	DES 算法： 当 P1≠‘05’时：‘08’≤Lc≤ ‘40’（模 8） 当 P1= ‘05’时：‘10’≤Lc≤ ‘40’（模 8） SSF33 算法： 当 P1≠‘05’时：‘10’≤Lc≤ ‘80’（模 16） 当 P1= ‘05’时：‘20’≤Lc≤ ‘80’（模 16）
DATA	待处理数据
Le	返回数据长度

9.8.4 响应信息

响应信息中可能返回的状态码见表 26：

表 26 响应信息

SW1	SW2	说 明
‘90’	‘00’	命令执行成功
‘61’	‘xx’	有 xx 个字节要返回
‘67’	‘00’	Lc 长度错误
‘69’	‘01’	Delivery Key 命令没有执行或无效
‘69’	‘85’	使用条件不满足
‘6A’	‘81’	功能不支持
‘6A’	‘86’	P1、P2 参数错
‘6D’	‘00’	命令不存在
‘6E’	‘00’	CLA 错

9.9 INIT SAM FOR PURCHASE 命令（MAC1 计算）

9.9.1 命令描述

INIT SAM FOR PURCHASE 命令支持三级医疗消费密钥分散机制，并产生 MAC1。用省份标识因子、城市标识因子、卡片应用序列号进行密钥分散。PSAM 卡产生医疗保险脱网方式交易流程中 MAC1 的过程如下所示：

——PSAM 在其内部用全国医疗消费主密钥对省份标识分散，得到二级医疗消费主密钥 BMPK；

——PSAM 在其内部用 BMPK 对城市标识分散，得到城市医疗消费主密钥 MPK；

——PSAM 在其内部用 MPK 对卡片应用序列号分散，得到卡片医疗消费子密钥 DPK；

——PSAM 在其内部用 DPK 对卡片传来的伪随机数、医疗消费交易序号、终端交易序号加密，得到过程密钥 SESPK，作为临时密钥存放在卡中；

——PSAM 在其内部用 SESPK 对交易金额、交易类型标识、终端机编号、交易日期（终端）和交易时间（终端）加密得到 MAC1，将 MAC1 传送出去。

9.9.2 使用条件和安全

INIT SAM FOR PURCHASE 命令支持三级医疗消费密钥分散机制，医疗消费密钥的分

散过程由 Lc 和医疗消费密钥共同确定，如果二者不一致，则返回错误信息。只有执行 INIT SAM FOR PURCHASE 命令后，才可执行 MAC2 校验命令。

9.9.3 命令格式

表 27 命令格式

代码	值
CLA	‘80’
INS	‘70’
P1	‘01’
P2	‘00’
Lc	‘1C’＋8×N（N＝1，2，3）
Data	用户卡随机数，4 个字节 用户卡交易序号，2 个字节 个人帐户交易金额，4 个字节 统筹项目个人帐户支付金额，4 个字节 统筹基金支付金额，4 个字节 交易类型标识，1 个字节 交易日期（终端），4 个字节 交易时间（终端），3 个字节 医疗消费密钥版本号，1 个字节 医疗消费密钥算法标识，1 个字节 三级分散因子，8 个字节 二级分散因子，8 个字节 一级分散因子，8 个字节
Le	‘08’（终端交易序号，4 个字节；MAC1，4 个字节）

9.9.4 响应信息

响应信息中可能返回的状态码见表 29：

表 29 响应信息

SW1	SW2	含 义
‘90’	‘00’	命令执行成功
‘67’	‘00’	Lc 长度错
‘69’	‘85’	使用条件不满足（应用非永久锁定）
‘6A’	‘81’	功能不支持（卡锁定）
‘6A’	‘86’	参数 P1，P2 不正确
‘6A’	‘88’	未找到密钥参数
‘6D’	‘00’	命令不存在
‘6E’	‘00’	CLA 错

9.10 CREDIT SAM FOR PURCHASE 命令（校验 MAC2）

9.10.1 命令描述

CREDIT SAM FOR PURCHASE 命令利用 INIT SAM FOR PURCHASE 命令产生的过程密钥 SESPK 校验 MAC2。MAC2 校验失败，回送状态码‘63CF’。

9.10.2 使用条件和安全

CREDIT SAM FOR PURCHASE 命令必须在 INIT SAM FOR PURCHASE 命令成功执行后才能进行。

9.10.3 命令格式

表 30 命令格式

代码	值
CLA	‘80’
INS	‘72’
P1	‘00’
P2	‘00’
Lc	‘04’
Data	MAC2
Le	不存在

9.10.4 响应信息

响应信息中可能返回的状态码见表 31：

表 31 响应信息

SW1	SW2	含 义
‘90’	‘00’	命令成功执行
‘67’	‘00’	Lc 长度错
‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足（应用非永久锁定）
‘6A’	‘81’	功能不支持（卡锁定）
‘6A’	‘86’	参数 P1，P2 不正确
‘6D’	‘00’	命令不存在
‘6E’	‘00’	CLA 错
‘93’	‘02’	MAC 无效

附录 A：PSAM 卡内密钥标识分配表

由于 PSAM 卡中同时存在国家级、省级和地市级控制的密钥，密钥安装分散，为了保证卡内密钥能协调工作，不相互冲突，各级发放和应用 PSAM 卡的机构，应按照下表密钥标识的分配原则来定义 PSAM 卡内的密钥标识号。

表 A1　PSAM 卡内密钥标识分配表

	国家级	省级	地市级
PSAM 卡自用密钥	‘00’~‘07’		
针对用户卡 DDF 下的密钥	‘08’~‘0F’	‘10’~‘17’	‘18’~‘1F’
针对用户卡各应用下的密钥	‘20’~‘3F’	‘40’~‘7F’	‘80’~‘BF’

注：‘C0’～‘FF’保留为将来使用，各级机构不得占用。

附录B：PSAM 卡内国家级密钥与用户卡内密钥标识对照表

表 B1　PSAM 卡内国家级密钥与用户卡内密钥标识对照表

用户卡内密钥				PSAM 卡内密钥			
名称	标识	组数	长度（字节）	用途	标识	密钥级别	分散级数
IRK	‘00’	3	16	‘67’	‘08’	国家	一级根密钥
PUK	‘06’						
STK	‘02’	1	8***	‘26’	‘09’	国家	三级根密钥**
STK_{DF01}	‘82’	1	8***	‘26’	‘20’	国家	三级根密钥
STK_{DF02}	‘82’	1	8***	‘26’	‘21’	国家	三级根密钥
STK_{DF03}	‘82’	1	8***	‘26’	‘22’	国家	三级根密钥
STK_{DF04}	‘82’	1	8***	‘26’	‘23’	国家	三级根密钥
BK	‘05’						
LK_{DF03}	‘83’						
LK_{DF04}	‘83’						
UK_{MF}	‘04’						
$UK1_{DF01}$	‘83’						
$UK2_{DF01}$	‘84’						
$UK3_{DF01}$	‘85’	3	16	‘27’	‘24’	国家	三级根密钥
$UK4_{DF01}$	‘86’	3	16	‘27’	‘25’	国家	三级根密钥
$UK5_{DF01}$	‘87’						
$UK1_{DF02}$	‘83’	3	16	‘27’	‘26’	国家	三级根密钥
$UK2_{DF02}$	‘84’						
$UK3_{DF02}$	‘85’						
$UK4_{DF02}$	‘86’	3	16	‘27’	‘27’	国家	三级根密钥
$UK5_{DF02}$	‘87’	3	16	‘27’	‘28’	国家	三级根密钥
$UK1_{DF03}$	‘86’						
$UK2_{DF03}$	‘87’	3	16	‘27’	‘29’	国家	三级根密钥
$UK3_{DF03}$	‘88’						
$UK1_{DF04}$	‘85’						
$UK2_{DF04}$	‘86’	3	16	‘27’	‘2A’	国家	三级根密钥
DSK							
DLK							
DPK		3	16	‘22’	‘01’* ‘02’ ‘03’	国家 （三组）	三级根密钥
DTK							

续表

用户卡内密钥				PSAM 卡内密钥			
名称	标识	组数	长度（字节）	用途	标识	密钥级别	分散级数
$RK1_{DF03}$	‘84’	3	16	‘67’	‘2B’	国家	一级根密钥
$RK2_{DF03}$	‘85’	3	16	‘67’	‘2C’	国家	一级根密钥
$RK1_{DF04}$	‘84’	3	16	‘67’	‘2D’	国家	一级根密钥

表中空白行由各个省份组织定义。

注： 这里描述的是版本号。*

*** 本表所列为对地市通常分配密钥的情况，目前，以放置国家三级根密钥为主。各省份可以向人力资源和社会保障部申请升级为二级根密钥，以做到本省内信息通写。*

****在 SSF33 算法环境下，这些密钥的长度均为 16 字节。*