社会保障（个人）卡规范
第 4 部分：安全机制

引言

本规范作为《社会保障（个人）卡规范》的第 4 部分，包括以下主要内容：

——社会保障卡应用中有关安全的基本要求和安全机制。

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

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　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。

3.3　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。

3.4　半字节（Nibble）

一个字节的高四位或低四位。

3.5　明文（Plain Text）

没有加密的信息。

3.6　密文（Cipher Text）

通过密码系统产生的不可理解的文字或信号。

3.7　密钥（Key）

控制加密转换操作的符号序列。

3.8　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。

3.9　对称加密技术（Symmetric Cryptographic Technique）

发送方和接收方使用相同保密密钥进行数据变换的加密技术。在不掌握保密密钥的情况下，不可能推导出发送方或接收方的数据变换。

3.10 保密密钥（Secret Key）

对称加密技术中仅供指定实体所用的密钥。

3.11 数据完整性（Data Integrity）

数据不受未经许可的方法变更或破坏的属性。

4 缩略语和符号表示

ADF 应用数据文件（Application Definition File）

APDU 应用协议数据单元（Application Protocol Data Unit）

CLA 命令报文的类别字节（Class Byte of the Command Message）

DEA 数据密码算法（Data Encryption Algorithm）

INS 命令报文的指令字节（Instruction Byte of Command Message）

ICC 集成电路卡（Integrated Circuit Card）

Lc 终端发出的命令数据的实际长度（Exact Length of Data Sent by the TA1 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 TA1 in Response to a Case 2 or 4 Command）

P1 参数 1（Parameter 1）

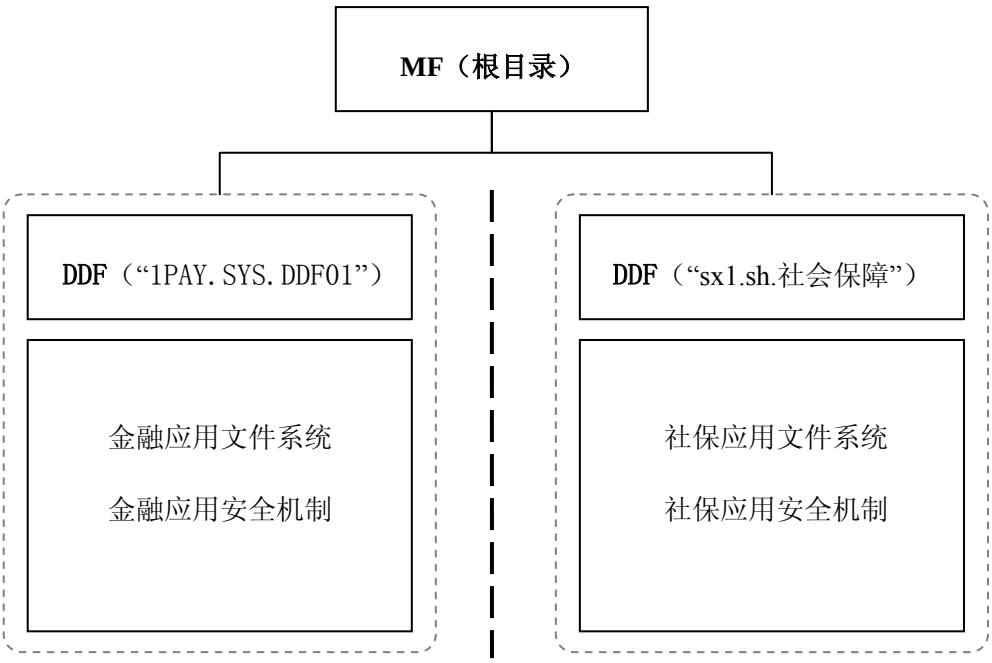
P2 参数 2（Parameter 2）

MAC 报文鉴别代码（Message Authentication Code）

SAM 安全存取模块（Secure Access Module）

5 卡片安全

5.1 整体安全架构



应用防火墙

5.2 MF 安全控制

MF 是整个 IC 卡文件系统的根，拥有卡片主控密钥。卡片主控密钥用于控制更新卡片主控密钥、创建应用环境 DDF 和装载 DDF 主控密钥；成功创建应用环境 DDF 和装载 DDF 主控密钥后，卡片主控密钥对该应用不再拥有控制权。

5.3 社保应用环境下的安全控制

社保应用环境 DDF，拥有社保环境主控密钥，社保环境主控密钥用于控制更新社保环境主控密钥、创建社保应用环境目录下的文件等。社保应用环境 DDF 下的安全机制必须符合《社会保障（个人）卡规范》的安全要求。

5.4 金融应用环境下的安全控制

金融应用环境 DDF，拥有金融环境主控密钥，金融环境主控密钥用于控制更新金融环境主控密钥、创建金融应用环境目录下的文件等。金融应用环境 DDF 下的安全机制必须符合 JR/T 0025 的安全要求。

5.5 应用防火墙机制

金融应用环境和社保应用环境在 IC 卡中通过应用防火墙相互隔离，互不影响。

6 基本安全要求

6.1 共存应用

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

6.2 安全计算的操作环境

与密钥有关的所有计算（包括产生、派生、传输、鉴别等）过程都应该在保密、安全和

可靠的环境中进行。这种环境可以是由采取了相关措施的物理空间（如保密室）所提供的，也可以是经过国家密码管理机构认定的设备（如密码机、专用 IC 卡）所提供的。

6.3 密码算法的安全要求

密码算法用于实现密钥派生（分散）、内部认证、外部认证、数据加密、数据解密及 MAC 计算等六种类型的安全功能。

社会保障（个人）IC 卡芯片中所存储的实现密码算法的代码模块，在卡的整个生命周期中不能被修改，也不能读取、泄露至 IC 卡外部。

6.4 个人密码的存放

如果使用个人密码，则应保证其在 IC 卡中的安全存放，且在任何情况下都不会被泄露。

7 密钥的安全要求

7.1 密钥的独立性

用于一种特定功能（例如，读取数据）的加密（解密）密钥不能被任何其它功能所使用，包括保存在 IC 卡中的密钥和用来产生、派生、传输这些密钥的密钥。

如果应用要求使用 SAM，其对终端、发卡方和私有 SAM 的安全要求请参阅《社会保障（个人）卡规范》第 8 部分：终端技术要求中的有关规定。

7.2 密钥的生成和派生

在密钥的生成和派生过程中，必须有物理的随机数发生器所产生的随机数参与计算，同时这种计算不会导致密码算法所规定密钥空间的缩小。

7.3 密钥的装载和更新

密钥的装载和更新应该采用安全报文传送，传输过程中的密钥应该经过加密。

7.4 密钥的存放和访问

IC 卡应该能够保证密钥在没有授权的情况下，不会被泄露出来。同时，IC 卡也应该保证密钥除在卡操作系统的控制下用于芯片内部的安全计算外，不能被外界直接访问。

7.5 密钥的终止

IC 卡应该具有对其所存储密钥的生命期管理功能，以阻止已失效或过期密钥的使用。

如果应用被永久锁定，与该应用相关的密钥就全部失效。

密钥生成和派生过程中可能产生或使用的临时密钥，只能存放在密码机或 IC 卡的挥发性电存储介质中，以确保在密钥生成和派生过程结束后，随着电源的消失而被销毁。

8 安全报文传送

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

8.1 安全报文传送格式

本规范中定义的安全报文传送格式符合 ISO/IEC 7816-4 的规定。当 CLA 字节的第二个半字节等于十六进制数字‘4’时，表明对发送方命令数据要采用安全报文传送。某个命令的数据域的数据是否需要加密传输，是否应该以加密的方式处理等由应用事先确定。

8.2 报文完整性和验证

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

8.2.1 MAC 的位置

MAC 是命令数据域中最后一个数据元。

8.2.2 MAC 的长度

本规范中，MAC 的长度规定为 4 个字节。

8.2.3 MAC 密钥的产生

在安全信息处理过程中用到的 MAC 过程密钥是按照 8.4 中描述的过程密钥的产生过程产生的。MAC 密码算法密钥的原始密钥用于产生 MAC 过程密钥。

8.2.4 MAC 的计算

8.2.4.1 8 字节分组长度数据密码算法

按照如下的方式使用单重或三重 DEA 加密方式产生 MAC：

第一步：取 8 个字节的十六进制数字‘00’作为初始变量。

第二步：按照顺序将以下数据连接在一起形成数据块：

——CLA，INS，P1，P2，Lc[1)]；

——所有在《社会保障（个人）卡规范》中定义的数据；

——在命令的数据域中（如果存在）包含明文或加密的数据 （例如要更改个人密码，加密后的个人密码数据块放在命令数据域中传输）；

——医疗保险交易 MAC 的计算不含有 CLA，INS，P1，P2，Lc 数据块。

第三步：将该数据块分成 8 字节为单位的数据块，标号为 D1，D2，D3，D4……等。最后的数据块有可能是 1-8 个字节。

第四步：如果最后的数据块长度是 8 字节的话，则在其后加上十六进制数字‘80 00 00 00 00 00 00 00’，转到第五步。

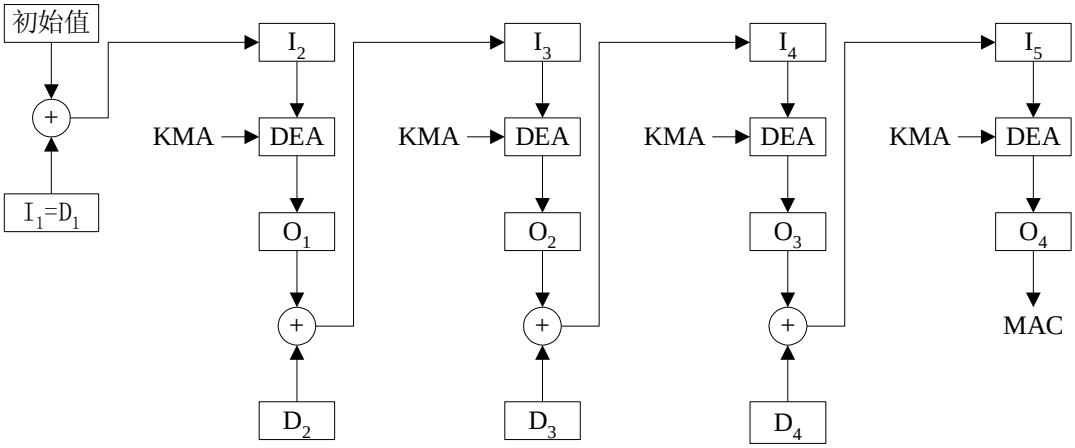
如果最后的数据块长度不足 8 字节，则在其后加上十六进制数字‘80’，如果达到 8 字节长度，则转入第五步；否则在其后加入十六进制数字‘00’直到长度达到 8 字节。

第五步：对这些数据块使用 MAC 过程密钥进行加密，过程密钥按照 8.2.3 描述的方式产生。如果安全报文传送支持单长度的 MAC 密码算法密钥，则依照图 1 的方式使用 MAC 过程密钥来产生 MAC。

第六步：最终得到从计算结果左侧取得的 4 字节长度的 MAC。

---

[1] Lc 表示命令数据域后面 4 个字节 MAC 数据的长度，例如：“APPLICATION BLOCK”命令需要产生一个 MAC，计算 MAC 的 Lc 的输入值是‘04’-‘FE’，而不是‘00’，CLA 包括安全报文的标志（‘x4’）。



图例：

I = 输入 D = 数据块

DEA = 数据密码算法（加密模式） KMA = MAC 过程密钥

O = 输出 + = 异或运算

图 1 8 字节分组密码算法单长度密钥的 MAC 算法

8.2.4.2 16 字节分组长度数据密码算法

按照图-2 所示做 DEA（e）运算产生 MAC：

第一步：取 16 个字节的十六进制数字‘00’作为初始变量。

第二步：按照顺序将以下数据连接在一起形成数据块：

——CLA，INS，P1，P2，Lc[2)]；

——所有在《社会保障（个人）卡规范》中定义的应用数据；

——在命令的数据域中（如果存在）包含明文或加密的数据 （例如要更改个人密码，加密后的个人密码数据块放在命令数据域中传输）；

——医疗保险交易 MAC 的计算不含有 CLA，INS，P1，P2，Lc 数据块。

第三步：将该数据块分成 16 字节为单位的数据块， 标号为 D1，D2，D3，D4……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 字节的话，则在该数据块之后再加一个完整的 16 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。

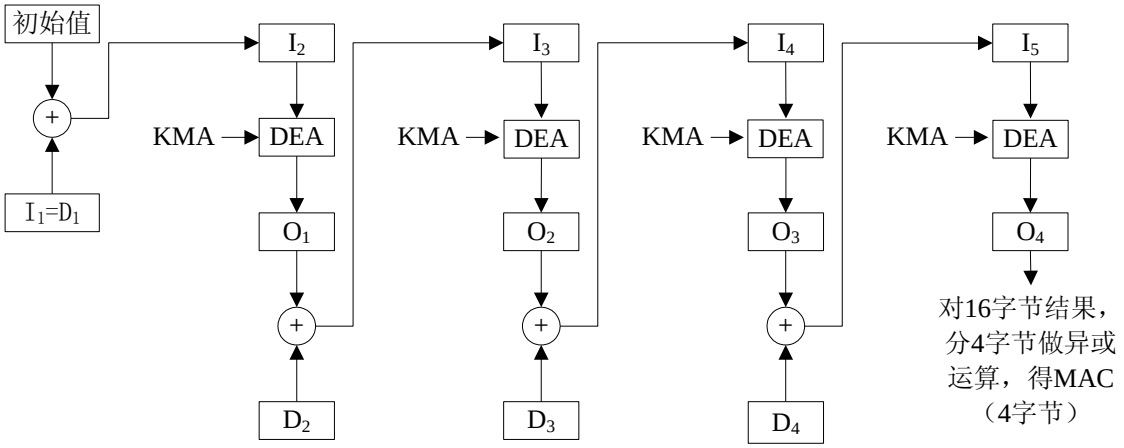
如果最后的数据块的长度不足 16 字节，则在其后加入 16 进制数‘80’，如果达到 16 字节长度，则转到第五步；否则接着在其后加入 16 进制数‘00’直到长度达到 16 字节。

第五步：对这些数据块使用 MAC 过程密钥进行加密，过程密钥按照 8.2.3 描述的方式产生。如果安全报文传送支持单长度的 MAC 密码算法密钥，则依照图 2 的方式使用 MAC 过程密钥来产生 MAC。

第六步：按照图 2 所述将 16 字节运算结果按 4 字节分块做异或运算。最终取计算结果作为 MAC。

---

[2] Lc 表示命令数据域后面 4 个字节 MAC 数据的长度，例如：“APPLICATION BLOCK”命令需要产生一个 MAC，计算 MAC 的 Lc 的输入值是‘04’－‘FE’，而不是‘00’，CLA 包括安全报文的标志（‘x4’）。



图例：

I = 输入　　D = 数据块

DEA = 16 字节分组数据密码算法（加密模式）　　KMA = MAC 过程密钥

O = 输出　　+ = 异或运算

图 2　16 字节分组密码算法的 MAC 算法

8.3　数据可靠性

为保证命令中明文数据的保密性，可以将数据加密。所使用的数据加密技术应被命令发送方和当前卡中被选择的应用所了解。

8.3.1　数据加密密钥的计算

在安全报文处理过程中用到的数据加密过程密钥按照 8.4 中描述的方式产生。数据加密过程密钥的产生过程是从卡中的数据加密的密码算法密钥开始的。

8.3.2　被加密数据的结构

当命令中要求的明文数据需要加密时，它先要被格式化为以下形式的数据块：

——明文数据的长度，不包括填充字符（L_D）；

——明文数据；

——填充字符（根据 8.3.3 的要求）。

然后整个数据块使用 8.3.3 中描述的数据加密技术进行加密。

8.3.3　数据加密计算

8.3.3.1　8 字节分组长度数据密码算法

数据加密技术如下所述：

第一步：用 L_D 表示明文数据的长度，在明文数据前加上 L_D 产生新的数据块。

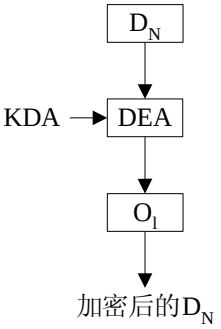
第二步：将第一步中生成的数据块分解成 8 字节数据块，标号为 D1，D2，D3，D4……等。最后一个数据块长度有可能不足 8 位。

第三步：如果最后（或唯一）的数据块长度等于 8 字节，转入第四步；如果不足 8 字节，在右边添加十六进制数字‘80’。如果长度已达 8 字节，转入第四步；否则，在其右边添加 1 字节十六进制数字‘00’，直到长度达到 8 字节。

第四步：每一个数据块使用 8.3.1 中描述的数据加密过程密钥加密。

如果采用单长度数据加密的密码算法密钥，数据块的加密如图 3 所示（使用数据加密过程密钥进行加密）。

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（加密后的 D1，加密后的 D2，等等），并将结果数据块插入到命令数据域中。



图例：

DEA = 数据密码算法（加密模式） D = 数据块

O = 输出 KDA = 数据加密过程密钥

图 3 8 字节分组密码算法单长度密钥的数据加密

8.3.3.2 16 字节分组长度数据密码算法

按照图 4 所示做 DEA（e）运算，对数据进行加密：

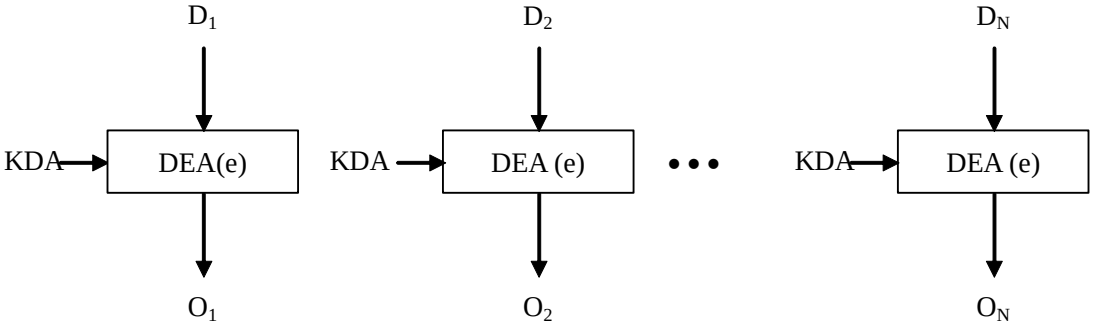
第一步：用 L_D（1 字节）表示明文数据的长度，在明文数据前加上 L_D 产生新的数据块，L_D 的值不小于 1。

第二步：将该数据块分成 16 字节为单位的数据块，表示为 D1，D2，D3，D4……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 字节，转到第四步；如果不足 16 字节，则在其后加入 16 进制数‘80’，如果达到 16 字节长度，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 字节。

第四步：按照图 4 所述的算法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。



DEA(e) = 16 字节分组数据密码算法（加密模式） D = 数据块

O = 输出 KDA = 数据加密过程密钥

图 4　16 字节分组密码算法的数据加密

8.3.4　数据解密计算

8.3.4.1　8 字节分组长度数据密码算法

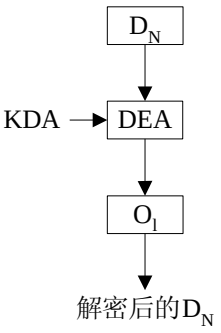
卡片接收到命令之后，需要将包含在命令中的加密数据进行解密。数据解密的技术如下：

第一步：将命令数据域中的数据块分解成 8 字节长的数据块，标号为 D1，D2，D3，D4……等。每个数据块使用如 8.3.1 所描述的方法产生的数据加密过程密钥进行解密。

如果采用单长度数据加密的密码算法密钥，数据块解密如图 5 所示（使用数据加密过程密钥进行解密）。

第二步：计算结束后，所有解密后的数据块依照顺序（解密后的 D1，解密后的 D2，等等）链接在一起。数据块由 L_D、明文数据、填充字符（如果在 8.3.3 描述的加密过程中增加的话）组成。

第三步：因为 L_D 表示明文数据的长度，因此，它被用来恢复明文数据。



图例：

DEA = 数据密码算法（解密模式）　D = 数据块

O = 输出　　KDA = 数据加密过程密钥

图 5　8 字节分组密码算法单长度密钥的数据解密

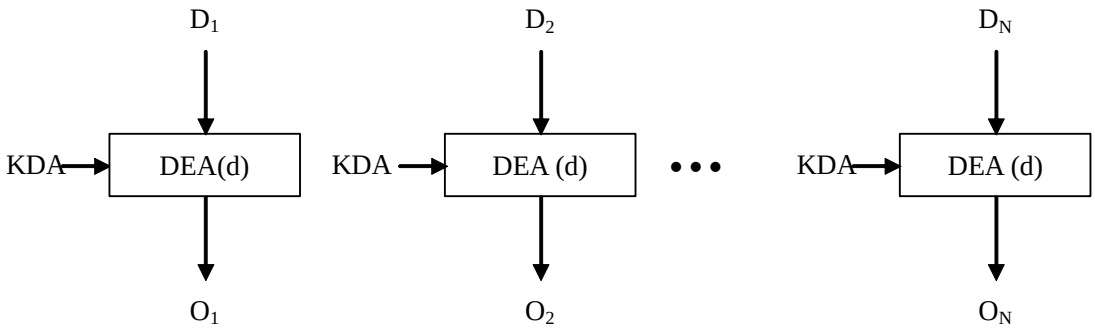
8.3.4.2　16 字节分组长度数据密码算法

按照图 6 的过程，对数据进行解密。

第一步：将命令数据域中的数据块分解成 16 字节长的数据块，标号为 D1，D2，D3，D4……等。每个数据块使用如 8.3.1 所描述的方法产生的数据加密过程密钥进行解密。

第二步：计算结束后，所有解密后的数据块依照顺序（解密后的 D1，解密后的 D2，等等）链接在一起。数据块由 L_D、明文数据、填充字符（如果在 8.3.3 描述的加密过程中增加的话）组成。

第三步：因为 L_D 表示明文数据的长度，因此，它被用来恢复明文数据。



DEA(d) =16 字节分组数据密码算法（解密模式）　　D = 数据块

O = 输出　　KDA = 数据加密过程密钥

图 6　16 字节分组密码算法的数据解密

8.4　过程密钥的产生

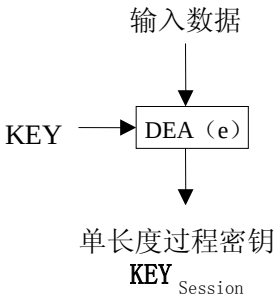
8.4.1　8 字节分组长度数据密码算法

MAC 和数据加密过程密钥是用可变数据产生的单长度密钥，按照图 7 或图 8 中描述的方法产生。

计算交易过程中的过程密钥时，输入数据参见《社会保障（个人）卡规范》第 7 部分：应用流程中的说明。

过程密钥产生后只能在某过程中使用一次。

图 7 和图 8 分别描述了基于单长度 DEA 密钥和基于双长度 DEA 密钥产生过程密钥的机制。输入数据是随机数，过程密钥所用随机数建议取 8 字节，取 4 字节随机数时则补十六进制数字‘00’后达到 8 字节。

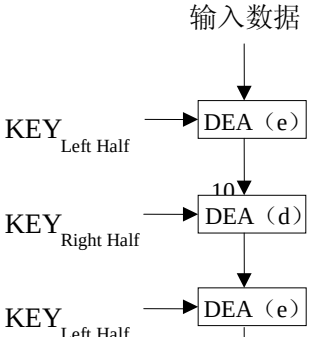


图例：

DEA（e） = 数据密码算法（加密模式）

$Key_{Session}$ = 过程密钥

图 7　基于单长度 DEA 密钥的过程密钥的产生



图例：

$KEY_{Left\ Half}$ = 密钥左 8 字节

$KEY_{Right\ Half}$ = 密钥右 8 字节

DEA（e） = 数据密码算法（加密模式）

DEA（d） = 数据密码算法（解密模式）

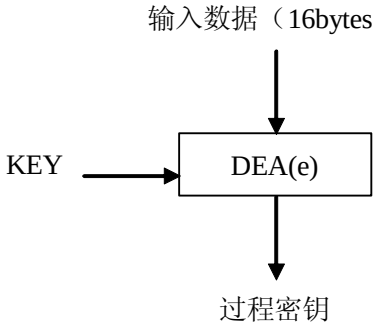
$Key_{Session}$ = 过程密钥

图 8　基于双长度 DEA 密钥的过程密钥的产生

8.4.2　16 字节分组长度数据密码算法

通过对过程密钥输入数据做 DEA（e）运算来产生过程密钥。如图 9。

过程密钥输入数据为 4 字节随机数补 12 字节“000000000000000000000000”达到 16 字节；或 8 字节随机数补 8 字节“0000000000000000”达到 16 字节；或 16 字节随机数。计算交易过程中的过程密钥时，输入数据参见《社会保障（个人）卡规范》第 7 部分：应用流程中的说明。



DEA(e) =16 字节分组数据密码算法（加密模式）

图 9　16 字节分组密码算法过程密钥的产生

8.5　安全报文传送的命令情况

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

情况一：这种情况时，没有数据送到 ICC（IC）中，也没有数据从卡中返回（Le）。没

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	MAC

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

情况二：这种情况时，命令中没有数据送到卡中，但有数据从卡中返回。没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Le

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	MAC	Le

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

情况三：这种情况时，命令中有数据传送到卡中，但没有数据从卡中返回。没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据	MAC

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

情况四：这种情况时，在命令中有数据送到卡中，也有数据从卡中返回。没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据	Le

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据	MAC	Le

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

9 操作权限鉴别

操作权限鉴别的目的是验证终端对卡中数据进行读写操作的合法性。

9.1 鉴别数据的长度

本规范中，鉴别数据的长度规定为 8 个字节。

9.2 操作权限鉴别密钥的产生

在操作权限鉴别过程中用到的操作权限鉴别过程密钥是在鉴别过程中用可变数据产生的密钥，按照 8.4 中描述的方法产生。

操作权限鉴别密码算法密钥的原始密钥用于产生操作权限鉴别过程密钥。

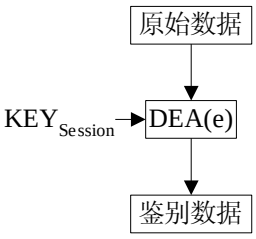
过程密钥产生后只能在鉴别过程中使用一次。

输入数据是鉴别命令引用的可变数据（如随机数）。

9.3 鉴别数据的计算

9.3.1 8 字节分组长度数据密码算法

使用 9.2 中描述的操作权限鉴别过程密钥对原始数据进行加密，见图 10：



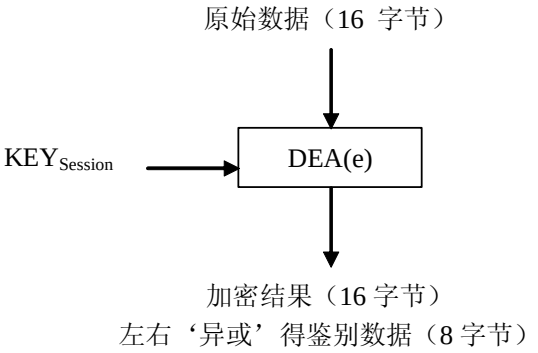
$KEY_{Session}$=由指定密钥产生的过程密钥

DEA（e） =数据密码算法（加密模式）

图 10 鉴别数据的生成

9.3.2 16 字节分组长度数据密码算法

鉴别数据输入因子由 8 字节设定值补 8 字节十六进制数字‘00’构成，这里 $KEY_{Session}$ 是由指定密钥产生的过程密钥。见图 11。



$KEY_{Session}$=由指定密钥产生的过程密钥

DEA(e) =16 字节分组数据密码算法（加密模式）

图 11 16 字节分组密码算法鉴别数据的生成