ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

DB

北　京　市　地　方　标　准

DB XX/ XXXXX—XXXX

市政交通一卡通技术规范
第 4 部分：安全规范

Municipal Administration & Communication Card Technology Standard

Part 4：Security Specifications

（征求意见稿）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

北京市质量技术监督局　　发 布

目　　次

前　言

DBxxxx-xxxx -《市政交通一卡通技术规范》分为五个部分：

---- 第1部分：总则；

---- 第2部分：卡片规范；

---- 第3部分：终端规范；

---- 第4部分：安全规范；

---- 第5部分：检测规范；

本部分为规范的第4部分。

本部分按照GB/T 1.1-2009给出的规则起草

本部分为新增部分，将原标准：DB11T159.1---2002《市政交通一卡通技术标准第1部分：卡片》和DB11T159.3---2005《市政交通一卡通技术标准第3部分：应用》中涉及安全的相关内容进行了整合，独立成文，作为市政交通一卡通技术规范的第4部分。

本部分由北京市交通委员会提出并归口。

本部分由北京市交通委员会组织实施。

本部分主要起草单位：北京市交通信息中心、一卡通公司。

本部分主要起草人员：

引　　言

本部分为DBxxxx-xxxx的第4部分，与DBxxxx-xxxx的第1部分、第2部分、第3部分、和第5部分一起构成《市政交通一卡通技术规范》。

市政交通一卡通技术规范

第 4 部分：安全规范

1 范围

本部分对市政交通一卡通系统的密钥及算法安全、卡片安全、交易安全、系统安全进行了规定和要求。

本部分适用于市政交通一卡通系统工程的设计、开发、实施、验收、运营与管理。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

GB/T 18238.3 信息技术 安全技术 散列函数 第 3 部分：专用散列函数

GB/T 22239 信息系统安全等级保护基本要求

GB 50174 电子信息系统机房设计规范

GM/T 0002 SM4 分组密码算法

GM/T 0003 SM2 椭圆曲线公钥密码算法

GM/T 0004 SM3 密码杂凑算法

CJ/T 166 建设事业 IC 卡应用技术

JR/T 0025 中国金融集成电路（IC）卡规范

DBxxxx-xxxx.1 市政交通一卡通技术规范第 1 部分：总则

DBxxxx-xxxx.2 市政交通一卡通技术规范第 2 部分：卡片规范

ISO/IEC 10116 信息技术.保密技术.n-比特条形密码的操作模式

ISO 16609 银行业务 对使用对称技术对电文认证的要求

3 术语和定义

本部分采用以下术语和定义。

3.1

集成电路 Intergrated Circuit（s）（IC）
用于执行处理和/或存储功能的电子器件。

3.2

无触点IC卡Contactless Card

在卡内部封装一个集成电路和简单的天线，卡内无电池，用射频方式与外部集成电路进行耦合操作的IC卡。

3.3

卡读写器IC Card Reader
可以对IC卡进行数据交换的终端设备。

3.4

充值机Add-value Machine
可以对IC卡中电子钱包进行充值的终端设备。

3.5

初始化Initialization
在卡发行前，由卡的发行机构对IC卡进行格式化，并在卡中写入卡的发行信息的过程。

3.6

密码Password
相当于通行字或口令，当一方能向另一方提交出预先约定的密码时，提交一方的合法性才得以承认。

3.7

密钥Key
对数据进行加密时使用的秘密参数，经过加密后的数据文件称为密文，利用密钥可对密文解密，使原数据文件恢复。

3.8

电子钱包Electronic Purse
一种为方便持卡人进行小额消费而设计的IC卡应用，它支持圈存/消费等交易，除圈存交易外，其它任何交易均无须提交个人密码。

3.9

加密算法 Cryptographic Algorithm
为了隐藏或揭露信息内容而变换数据的算法。

3.10

明文 Plaintext
没有加密的信息。

3.11

密文 Ciphertext
通过密码系统产生的不可理解的文字或信号。

3.12

数字签名 Digital Signature
一种非对称加密数据变换，他使得接收方能够验证数据的原始性和完整性，保护发送和接受的数据不被第三方伪造，同时对于发送方来说，还可以防止接收方的伪造。

3.13

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者接收方的数据交换。

3.14

非对称加密技术 Asymmetric Cryptographic Technique

采用两种相关变换进行的加密技术，一种是公开变换（由公共密钥定义），另一种是私有变换（由私有密钥定义）。这两种变换具有以下属性，即私有变换不能通过给定的公开变换导出。

3.15

私钥 Private Key

一个实体的非对称密钥对中仅供实体自身使用的密钥，在数字签名模式中，私钥用于签名功能。

3.16

公钥 Public Key

一个实体的非对称密钥对中可以公开的密钥，在数字签名模式中，公钥用于验证功能。

3.17

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。

3.18

Timing攻击 Timing Attack

Timing 攻击，又叫时序攻击方法。在加密过程中，由于各分支语句的执行、频率、RAM命中率等因素所造成时间不一致。时序的攻击可以利用这些漏洞对系统进行攻击。

3.19

SPA/DPA攻击 Simple Power Analysis/Differential Power Analysis Attack

系统消耗功率的大小随微处理器执行的指令不同而不同。通过观察系统的功耗,来提取与密钥有关的信息，称之为SPA/DPA攻击。

4 缩略语

API 应用程序接口（Application Programming Interface）

MAC 报文验证码（Message Authorization Code）

PKI 公开密钥基础设施（Public key infrastructure）

RSA 一种非对称加密算法（Rivest,Shamir,Adleman）

SAM 安全存取模块（Secure Access Module）

SHA 安全哈希算法（Secure Hash Algorithm）

SNR 序号（Serial Number）

TAC　交易验证码（Transaction Authorization Code）

5　卡片安全

5.1　卡片通信安全

a) 一卡通卡应采用一卡一密的密钥管理体系，卡的密钥利用卡的序列号（SNR）及其它有关信息，通过规定的加密算法，由卡的发行机构在对卡进行初始化时，记录在 IC 卡中。
b) 卡片应用验证应通过内置在终端的 SAM 卡、一卡通 API 模块或后台金融加密机完成；
c) 卡在交易过程中，为防止信号被意外截取，其数据通信均应加密，并按照 ISO/IEC9798 规定方法鉴别。
d) 卡片在每次写操作时，均需经过 MAC 验证，MAC 的计算需要通过卡内密钥经过特定的计算方法计算得到，MAC 的具体算法见附录 A.

5.2　卡片交易安全

a) 卡片消费交易流程应满足交通行业的应用，金融应用应完全符合 JR/T0025-2013 消费交易；
b) 卡片充值交易流程应满足交通行业的应用，金融应用应完全符合 JR/T0025-2013 中的圈存交易。

5.3　卡片防攻击

5.3.1　防 Timing 攻击

须能够抵御通过卡片 CPU 运算的时间差异分析卡片机密信息的攻击。

5.3.2　防 SPA/DPA 攻击

必须能够抵御卡片计算过程中能量消耗的变法而泄露卡片机密信息的攻击。

5.3.3　随机数产生器的随机性

卡片随机数的产生必须符合相关国家标准的随机性测试，确保随机数产生器的随机性符合安全要求。

6　终端安全

6.1　终端数据安全

终端一般存在两种类型的数据：
a) 通用数据：如终端交易记录等。外界可以对这些数据进行访问，但不允许进行无授权修改。
b) 敏感数据：包括卡片应用密钥、公私钥、及终端内部参数。在未授权的情况下，外界不允许对这类数据进行访问和修改。

6.1.1　通用数据的安全要求

通用数据一般存放在存储器中。在更新参数以及下载新的应用程序时，终端必须做到：
a) 验证更新方的身份。
b) 校验下载参数及应用程序的完整性。
c) 无论在什么情况下，终端的应用数据都不会随意改变或丢失，并保证数据有效。
d) 所有与交易相关的数据均应以记录形式存储于终端存储器中，终端须保证这些数据的完整性。

6.1.2　敏感数据的安全要求

a) 敏感数据一般应存放在终端安全模块 SAM 或 API Module 中。安全模块提供必要的安全机制以防止外界对终端所储存或处理的数据进行非法攻击的硬件加密模块。这些数据包括各种密钥和内部参数。
b) 安全模块的硬件设计必须能保证在物理上限制对其内部存贮的敏感数据的存取与窃取，以及对安全模块的非授权使用和修改。一旦安全模块受到非法的攻击，其自身必须能够立即完成对内部敏感数据的删除。
c) 安全模块的逻辑设计应保证，调用任何单一功能或组合功能，都不会导致敏感数据的泄露。对于某些敏感操作，必须有一定的权限限制。

6.2 终端设备安全

设备需具有防入侵功能，保证在正常的运行环境中，设备或它的接口不会泄露或改变任何输入或输出设备的、存储在设备中的或者在设备中处理的敏感数据。

终端需限制对内部存储的敏感数据的物理访问，并且阻止窃取数据，未经授权的使用或者未经授权的对设备的修改包括：

a) 不允许轻易入侵设备并对设备的软硬件进行增加、替换或修改；不允许测定或修改任何敏感数。
b) 据后重新安装设备。
c) 当设备的任何部件发生任何故障时，不会导致秘密或敏感的数据的泄露。
d) 如果设备的设计需要部分部件在物理上分离，并且处理的数据或持卡人的指令在这些分离的部件之间传递，那么对设备的所有部件的保护等级应该是相同的。

7 交易安全

交易的安全包括消费类交易的安全、充值类交易的安全和退卡类交易的安全。

应保证卡与终端之间、终端与后台系统之间的通信数据正确传输，防止通信数据被非法窃取或篡改。

7.1 消费类交易安全

a) 公共交通领域消费终端应使用 SAM 卡或一卡通 API 模块完成卡片的脱机交易验证。
b) 非公共交通领域消费终端应使用一卡通 API 模块完成卡片的脱机交易验证，对于消费交易所需安全性较高的行业及应用，应采用联机消费方式进行。
c) 消费交易时，首先应验证卡的合法性，包括是否为本系统卡、卡片状态是否正常等。
d) 应验证卡的可用性，包括是否为黑名单卡、是否为可用卡、余额是否足够等。
e) 消费交易应符合一卡通下发的消费类参数规定，如消费可用卡类型等。
f) 消费成功后应正确生成和完整保存消费交易数据，并确保数据存储的安全性。
g) 消费交易数据包含 TAC。
h) 系统应及时将黑名单下发到每一台终端上，应拒绝黑名单卡的交易并进行锁卡。

7.2 充值类交易的安全

a) 为确保售卡充值类交易的安全，交易须采用联机方式进行，即交易过程中，终端与一卡通中心计算机系统实时通讯，通过终端及其内置的一卡通联机模块、后台认证系统及硬件加密机，完成卡片的联机认证及后台合法性检查。
b) 联机交易终端与一卡通中心计算机系统的交互流程应采用 PKI 体系安全机制，采用非对称算法及动态工作密钥报文加密技术，确保传输报文的安全，报文中附带 MAC 校验码防篡改。

c) 对于互联网交易，须采用向用户颁发数字证书、交互报文附带数字签名的方式，加强交易的安全性和抗抵赖性。
d) 支持充值类业务的终端须成功签到取得授权，并在有效时间范围内进行一卡通卡的充值类交易，授权验证的权限在断电、复位、关机或超时后失效。
e) 一卡通中心计算机系统应具有对支持充值类业务的终端、商户、单位充值额度的三级配置管理功能，如：累计充值额度、当日最大充值额度限制等，对超出充值额度的终端、商户和单位，系统将拒绝其继续交易。
f) 充值交易时，应验证卡的合法性和可用性，包括是否为本系统卡、卡片状态是否正常、是否为黑名单卡等。
g) 充值成功后，终端应正确生成和完整保存充值交易数据，并将交易数据实时上传至一卡通中心计算机系统；充值交易数据包含 TAC。

7.3 退卡类交易的安全

a) 为确保退卡类交易的安全，交易须采用联机方式进行，即交易过程中，终端与一卡通中心计算机系统实时通讯，通过终端及其内置的一卡通联机模块、后台系统及硬件加密机，完成卡片的联机认证及后台合法性检查。
b) 联机交易终端与后台系统的交互流程应采用 PKI 体系安全机制，采用非对称算法及动态工作密钥报文加密技术确保传输报文的安全，报文中附带 MAC 校验码防篡改。
c) 退卡类终端须成功签到取得授权，并在权限有效时间范围内进行一卡通卡的退卡退资交易，授权验证的权限在断电、复位、关机或超时后失效。
d) 退卡类交易应符合一卡通下发的退卡类参数规定。
e) 退卡交易时，首先应验证卡的合法性和可用性，包括是否为好卡、是否为本系统卡、卡片状态是否正常、是否为黑名单卡等。
f) 卡片合法性、可用性、参数符合性验证，由终端和后台系统共同完成，通过验证的卡准许进行交易。
g) 退卡退资成功后，终端应正确生成和完整保存交易数据，并将交易数据实时上传至一卡通中心计算机系统。
h) 退卡退资交易数据包含 TAC。

8 密钥管理体系

8.1 密钥管理通用要求

市政交通一卡通系统密钥管理要求应符合CJ/T 166的相关规定。

8.2 密钥的生成与发行

市政交通无触点（IC）卡系统的主密钥及读写器安全认证模块由卡的发行机构负责管理，在卡发生交易时，由加载在读卡器内的安全模块根据卡的特性判定卡的合法性。

为了保证密钥的安全和防止密钥的泄露，在密钥生成时，应采取以下措施：
a) 密钥生成采用多人生成或硬件加密的方式。
b) 密钥生成环境的安全管理，使其生成环境可视为绝对安全。
c) 参加密钥生成的特殊人员的安全管理规定。
d) 密钥生成的过程必须按照严格的操作规程进行。

8.2.1 密钥的生成

8.2.1.1 密钥生成方式

密钥一般采用集中方式生成，即由管理机构生成相应的主密钥组，其它密钥由该组主密钥分散生成。密钥生成的两种基本方法为：

a) 不重复的密钥生成：随机生成不可恢复的密钥，每次的数值不相同。
b) 可重复的密钥生成：密钥变换、密钥衍生；而且密钥的生成是可重复的，在需要的情况下，能够重新得到与原来相同的密钥值。

8.2.1.2 密钥生成的安全技术

不需重复生成的密钥采用随机产生的办法生成，由系统随机产生这些密钥，写入安全存取模块中保存，可重复生成的密钥采用密钥变换或密钥衍生的办法生成，确保密钥变换或密钥衍生的过程绝对安全。

8.2.2 密钥的发行

8.2.2.1 密钥发行方式

密钥的发行采用梯级生成、下发方式。即由上一级生成下一级所需的各种子密钥，并以卡片的形式传递给下一级。

8.2.2.2 密钥发行的安全技术

使用传输密钥控制密钥的加密装载、直接加密导出、分散加密导出。

9 安全机制

9.1 对称加密技术

卡片须支持对称加密技术，具体算法标准参见 CJ/T 166-2006.包括：

a) 数据加解密
b) 报文鉴别码算法
c) 过程密钥的产生
d) 子密钥分散

9.2 非对称加密技术

算法被用来进行静态数据和动态数据的验证以及数字签名。

在选择公开密钥模数长度时，应该考虑到密钥的生命周期以及在此生命周期内被解密的可能性。每个密钥的长度范围（上限、下限）在其相应的专用标准中规定。

发卡方公开密钥的指数的长度与 IC 卡公开密钥的指数长度由发卡方决定。

数字签名算法中的公开密钥算法的标志码为十六进制数字“01”。

10 认可的算法

10.1 对称加密算法

a) 国外算法：DES\3DES 算法 算法定义参见 ISO 16609-2004、ISO/IEC 10116。
b) 国产算法：SM1、SM4，SM4 算法定义见 GM/T 0002。

10.2 非对称加密算法

a) 国外算法：RSA 算法。
b) 国产算法：SM2 ，算法定义见 GM/T 0003。

10.3 安全哈希算法

a) 国外算法：SHA-1 算法，算法定义参见 GB/T 18238.3。
b) 国产算法：SM3 算法，算法定义见 GM/T 0004。

11 系统安全

11.1 系统安全基本要求

根据中国人民银行《非金融机构支付服务业务系统检测认证管理规定》，市政交通一卡通系统应用安全要求应符合 GB/T 22239-2008 《信息系统安全等级保护基本要求》第三级的基本要求。

系统应用安全包括：鉴别和访问控制、操作的审计、数据安全、网络与计算的安全、业务连续性要求等。

11.2 鉴别和访问控制

系统应具备鉴别及访问控制功能，鉴别与访问控制应符合GB/T 22239-2008中应用安全的第三级要求。

11.2.1 鉴别

a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别。
b) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。
c) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。
d) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。
e) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

11.2.2 访问控制

a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问。
b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。
c) 应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限。
d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。
e) 应具有对重要信息资源设置敏感标记的功能。
f) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

11.3 操作的审计

系统应具备操作的审计功能，操作的审计应符合GB/T 22239-2008中应用安全的第三级要求。

a) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。
e) 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录。
f) 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。

g) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

11.4 数据安全

a) 应保证原始交易记录完整、正确发送到一卡通中心计算机处理系统。
b) 防止交易数据被窃取或篡改。
c) 对联机交互报文关键信息采用加密及数字签名方式传输。
d) 对数据库及日志内的关键信息采用加密方式存储。
e) 一卡通中心计算机处理系统验证交易记录的合法性。
f) 一卡通中心计算机处理系统之间传输的交换数据包应有校验码，接收方对发送方数据包的校验码进行验证。
g) 通过对数据的审计及时发现异常卡及异常数据并进行处理。

11.5 网络与计算环境的安全

符合GB/T 22239-2008中网络安全的第三级要求。

根据应用业务特点及服务对象需求，基于系统面临的网络安全风险，采取相应的安全保护措施。

11.5.1 网络结构安全

a) 应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要。
b) 应保证网络各个部分的带宽满足业务高峰期需要。
c) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径。
d) 应绘制与当前运行情况相符的网络拓扑结构图。
e) 应根据系统和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。
f) 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段。
g) 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

11.5.2 访问控制安全

a) 应在网络边界部署访问控制设备，启用访问控制功能。
b) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。
c) 应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制。
d) 应在会话处于非活跃一定时间或会话结束后终止网络连接。
e) 应限制网络最大流量数及网络连接数。
f) 重要网段应采取技术手段防止地址欺骗。
g) 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。
h) 应限制具有拨号访问权限的用户数量。

11.5.3 计算环境

a) 符合 GB 50174-2008 的安全要求；
b) 保护系统的完整性和可用性。如资源和局域网管理、补丁管理、防病毒等。
c) 实现系统的鉴别与访问控制功能。

d) 实现计算环境的审计功能。
e) 实现计算环境的监控和报警。

11.6 系统备份要求

a) 系统应具备完善的备份机制,灾难发生时，保证系统数据的及时恢复以及业务的连续。
b) 一卡通中心计算机核心系统及核心网络系统设备采用双机热备。
c) 建立同城异地备份系统，灾难发生时，实现一卡通系统数据层、应用层、网络层的异地接管。
d) 须在本地及异地灾备系统进行数据同步及备份。
e) 灾备系统业务处理能力满足生产系统业务处理需求。

附 录 A
（规范性附录）
MAC 计算

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 4 个字节随机数，后补 4 字节的 16 进制数字’0’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

—— 所有在市政交通卡应用规范中定义的数据。

—— 在命令的数据域中(如果存在)包含明文或加密的数据。(例：如果要更

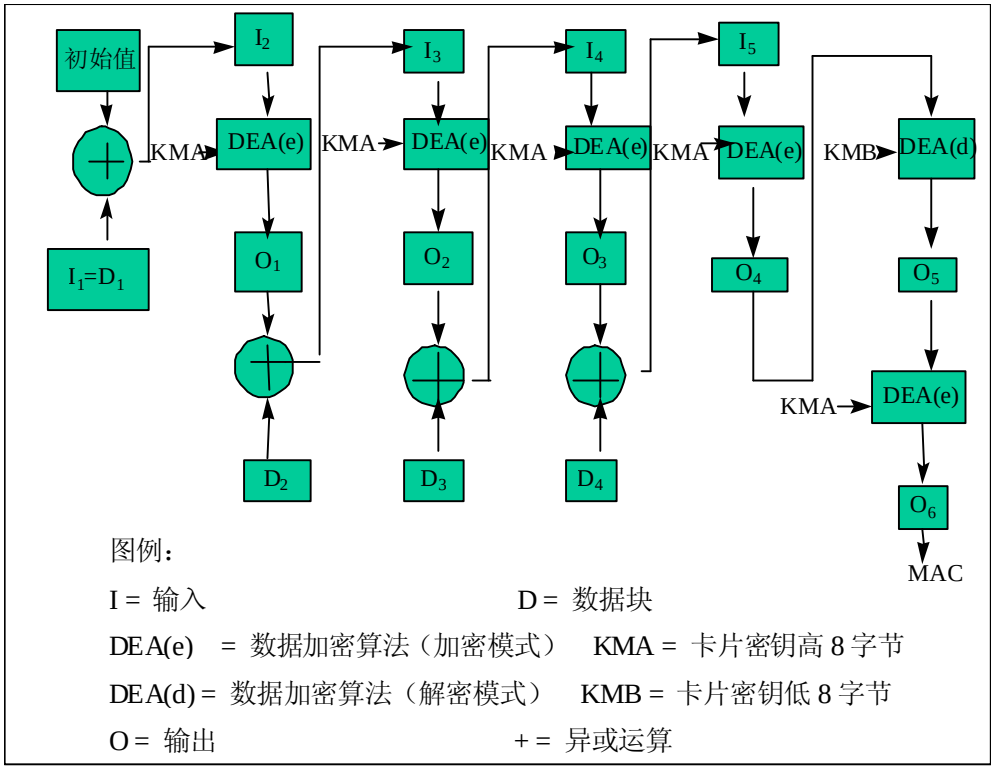
改个人密码，加密后的个人密码数据块放在命令数据域中传输)

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 16 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 16 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 16 进制数字’0’直到长度达到 8 字节。

第五步：对这些数据块使用卡片维护密钥进行计算 (MAC 的产生如图附录 A 中所示)，(根据第二步产生的数据块的长度，计算过程有可能多于或少于四步)。



图附录 A　双长度 DEA Key 的 MAC 算法

第六步：最终得到是从计算结果左侧取得的 4 字节长度的 MAC。