中 国 移 动 通 信 企 业 标 准

QB-XX-XXX-XXXX

中国移动一卡通业务安全技术规范--密钥与算法要求（企业端管理系统部分）

Key and Algorithm Specification for China Mobile E-Card Pass

版本号： 1.0.0

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中国移动通信集团公司　　发布

目　录

前　言

本标准是对一卡通企业端管理系统所使用密钥及相关算法提出全面要求，是一卡通企业端管理系统密码体系设计所需要遵从的纲领性技术文件。

本标准主要包括以下几方面内容：一卡通系统安全要求、一卡通系统密钥定义、密钥要求、密钥算法要求、会话密钥生成以及MAC/TAC计算等。

本标准是一卡通业务系列标准之一，该系列标准的结构、名称或预计的名称如下：

序号	标准编号	标准名称
[1]	QB-D-111-2009	《中国移动一卡通业务规范》V1.0
[2]		《中国移动一卡通业务总体技术要求》V1.0
[3]		《中国移动一卡通业务设备规范--一卡通业务系统部分》V1.0
[4]		《中国移动一卡通业务设备规范--一卡通企业端管理系统部分》V1.0
[5]		《中国移动一卡通业务设备规范--SIM 卡应用部分》V1.0
[6]		《中国移动一卡通业务设备规范--SAM 卡部分》V1.0
[7]		《中国移动一卡通业务终端设备规范--发卡终端部分》V1.0
[8]		《中国移动一卡通业务终端设备规范--门禁终端部分》V1.0
[9]		《中国移动一卡通业务终端设备规范--考勤终端部分》V1.0
[10]		《中国移动一卡通业务终端设备规范--消费终端部分》V1.0
[11]		《中国移动一卡通业务终端设备规范--充值终端部分》V1.0
[12]		《中国移动一卡通业务接口规范—业务系统与企业端管理系统接口分册》V1.0
[13]		《中国移动一卡通业务接口规范--SIM 卡与业务系统接口分册》V1.0
[14]		《中国移动一卡通业务接口规范--SIM 卡与发卡终端接口分册》V1.0
[15]		《中国移动一卡通业务接口规范--SIM 卡与门禁终端接口分册》V1.0
[16]		《中国移动一卡通业务接口规范--SIM 卡与考勤终端接口分册》V1.0
[17]		《中国移动一卡通业务接口规范--SIM 卡与消费终端接口分册》V1.0
[18]		《中国移动一卡通业务接口规范--SIM 卡与充值终端

接口分册》V1.0
[19] 《中国移动一卡通业务安全技术规范-总体要求》
[20] 《中国移动一卡通业务安全技术规范-密钥与算法要求》
[21] 《中国移动一卡通业务安全技术规范-密钥安全管理要求（一卡通业务系统）》
[22] 《中国移动一卡通业务安全技术规范-密钥安全管理要求（一卡通企业端管理系统）》
[23] 《中国移动一卡通业务安全技术规范-一卡通业务系统加密机设备要求》
[24] 《中国移动一卡通业务安全技术规范-密钥母卡设备要求》

本标准的附录A~E为标准性附录。

本标准由中移　　号文件印发。

本标准由中国移动通信集团数据部提出，集团公司技术部归口。

本标准起草单位：中国移动通信研究院

本标准主要起草人：任晓明、郭漫雪、乐祖晖、李亚强、罗烽

1 范围

本标准规定了中国移动一卡通系统所使用业务密钥的类型，各密钥生成、分发、存储及更新等生命周期管理，以及所使用的密码算法，用于一卡通业务流程安全保障，供中国移动内部和厂商共同使用；适用于GSM/GPRS/3G网络环境。

2 规范性引用文件

下列文件中的条款通过本标准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标准，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标准。

表1-1

[1]	QB-D-111-2009	《中国移动企业一卡通业务规范》	中国移动通信有限公司
[2]		《中国移动企业一卡通业务总体技术要求》	中国移动通信有限公司
[3]		《中国移动一卡通业务安全技术规范-总体要求》	中国移动通信有限公司
[4]	QB-F-009-2009	《中国移动手机支付业务-密钥安全管理总体技术要求》	中国移动通信有限公司

3 术语、定义和缩略语

下列术语、定义和缩略语适用于本标准：

表1-2

词语	解释
MAC	Message Authentication Code，消息验证码
TAC	Transaction Authentication Code，交易验证码

4 密钥类型定义

4.1 一卡通应用密钥

一卡通应用密钥说明如下表所示：

密钥分类	密钥类型	用途	相关设备
企业管理密钥	企业主控密钥	用于如下功能的权限验证和密钥加密： l 用于自身的更新； l 用于其它应用卡中密钥的装载与更新； l 更新个人化信息 ***说明：业务平台和 SIM 卡之间的权限验证是通过在指令中携带由该密钥计算的 MAC 来实现的，MAC 的计算数据应包括指令所涉及的关键信息***	SIM 卡（主卡）；密钥母卡
	企业空中传输密钥	用于加密企业通过空中传递的敏感信息 ***说明：业务平台和 SIM 卡之间通过空中传递的信息可以通过该密钥进行端到端的加密***	SIM 卡；业务模块；密钥母卡
	企业空中报文 MAC 密钥	用于生成企业通过空中传递敏感信息的 MAC ***说明：业务平台和 SIM 卡之间通过空中传递的信息可以通过该密钥进行端到端的信息验证***	SIM 卡；业务模块；密钥母卡
身份识别类密钥	身份识别应用密钥	用于门禁、考勤等身份识别类应用刷卡过程的认证	SIM 卡（身份识别卡）；门禁/考勤终端/SAM 卡；密钥母卡
联机消费密钥	联机交易鉴权密钥	对联机交易的鉴权	SIM 卡（联机消费卡）；业务模块；密钥母卡
	联机交易 TAC 密钥	用于生成联机交易的 TAC	
脱机消费密钥	消费密钥	用于 POS 刷卡过程的认证	SIM 卡（脱机消费卡）；消费 PSAM 卡；密钥母卡
	充值密钥	用于充值	SIM 卡（脱机消费卡）；业务模块；密钥母卡
	脱机交易 TAC 密钥	用于生成消费相关交易的 TAC	SIM 卡（脱机消费卡）；业务模块；密钥母卡

4.2 SAM 卡密钥

SAM 卡密钥如下表所示：

	密钥类型	说明
SAM 卡密钥	SAM 卡卡片主控密钥	SAM 卡的卡片主控密钥，用于如下操作过程中的权限控制： 1、 创建卡片 MF 区域的文件 2、 更新自身、卡片维护密钥 3、 装载卡片维护密钥和应用主控密钥
	SAM 卡卡片维护密钥	SAM 卡的卡片维护密钥，用于如下操作过程中的权限控制： 1、更新卡片文件信息

	SAM 卡应用主控密钥	SAM 卡的应用主控密钥，用于如下操作过程中的权限控制： 1、 装载应用维护密钥、应用密钥 2、 更新应用主控密钥、应用维护密钥和应用密钥
	SAM 卡应用维护密钥	SAM 卡的应用主控密钥，用于如下操作过程中的权限控制： 1、 用于更新应用文件信息 2、 应用解锁

5 密钥要求

5.1 密钥层次结构设计

5.1.1 一卡通应用密钥

5.1.1.1 企业管理密钥

企业密钥包括如下类型：

- 企业管理密钥
  - 企业主控密钥
  - 企业空中传输密钥
  - 企业空中报文 MAC 密钥

如果企业使用移动提供的初始密钥，不进行二次洗卡，则相应的密钥层次，采用四级结构，说明如下：

- 四级结构：根密钥->省密钥->企业级密钥->卡片子密钥，其中企业端管理系统相关密钥如下：
  - 企业级密钥：移动为各企业分配的初始企业管理根密钥
  - 卡片子密钥：每个卡片上的子密钥
- 分散参数：
  - 子密钥分散参数：应用序列号（3-16 位）+密钥版本号

企业二次洗卡后，自己管理应用密钥，则采用二级结构，说明如下：

- 二级结构：企业根密钥->卡片子密钥
- 子密钥分散参数：应用序列号（3-16 位）+密钥版本号

各级密钥的分布情况如下表所示：

	企业管理密钥
企业根密钥	密钥母卡

卡片子密钥	SIM 卡主控子应用

5.1.1.2 企业应用密钥

企业应用密钥包括如下类型：

- 身份识别类密钥
  - 身份识别应用密钥
- 联机消费密钥
  - 联机交易鉴权密钥
  - 联机交易 TAC 密钥
- 脱机消费密钥
  - 消费密钥
  - 充值密钥
  - 脱机交易 TAC 密钥

如果企业使用移动提供的初始密钥，不进行二次洗卡，则相应的密钥层次，采用五级结构，说明如下：

- 五级结构：根密钥->省密钥->企业级密钥->应用级密钥->卡片子密钥，其中企业端管理系统相关密钥如下：
  - 企业级密钥：移动为各企业分配的各类应用的初始根密钥
  - 应用级密钥：每个应用实例的根密钥
  - 卡片子密钥：针对不同应用实例分散出的卡片子密钥
- 分散参数：
  - 应用级密钥分散参数：子应用索引号（标识不同的应用实例）+密钥版本号
  - 卡片子密钥分散参数：应用序列号（3-16 位）+密钥版本号

企业二次洗卡后，自己管理应用密钥，则采用三级结构，说明如下：

- 三级结构：企业级密钥->应用级密钥->卡片子密钥
- 分散参数：
  - 一级分散参数：子应用索引号+密钥版本号
  - 二级分散参数：应用序列号（3-16 位）+密钥版本号

企业端管理系统中各级密钥的分布情况如下表所示：

	身份识别应用密钥	**联机消费密钥**	**脱机消费密钥**		
			消费密钥	充值密钥	脱机交易 TAC 密钥
企业级密钥	密钥母卡	密钥母卡、一卡通企业端管理系统	密钥母卡、脱机消费 SAM 卡	密钥母卡、一卡通企业端管理系统	密钥母卡、一卡通企业端管理系统
应用级密钥	门禁/考勤终端/SAM 卡	N/A	N/A	N/A	N/A

卡片子密钥	SIM 卡中的身份识别子应用（门禁、考勤）	SIM 卡中的联机消费子应用	SIM 卡中的脱机消费子应用

5.1.2 SAM 卡密钥

SAM 卡密钥由中国移动管理并预置在母卡相关卡片内，具体包括如下三类：

- SAM 卡卡片主控密钥
- SAM 卡卡片维护密钥
- SAM 卡应用主控密钥
- SAM 卡应用维护密钥

SAM 卡密钥，采用三级管理结构，说明如下：

- 三级结构：根密钥->省密钥->企业级密钥->卡片密钥
- 分散参数：
  - 一级分散参数：省编码+密钥版本号
  - 二级分散参数：企业 ID+密钥版本号
  - 三级分散参数：省级密钥到卡片子密钥的分散规则参见附录-F，包括对如下子密钥的分散规则的具体要求：
    - SAM 卡卡片主控密钥
    - SAM 卡卡片维护密钥
    - SAM 卡应用主控密钥
    - SAM 卡应用维护密钥

各级密钥的分布情况如下表所示：

	母卡相关密钥
企业级密钥	母卡（SAM 卡卡片维护、应用主控、应用维护密钥）
卡片密钥	SAM 卡

5.1.3 密钥分散参数的获取方式

在一卡通系统的各类交易过程中密钥分散参数的获取方式如下表所示：

密钥分散参数	**获取方式**
企业 ID	在系统交互过程中直接传递
子应用索引号	在系统交互过程中直接传递
一卡通应用序列号	在系统交互过程中从卡片中（SIM 卡、IC 卡）直接获取

5.2 密钥生成与分发

各类密钥的生成与分发说明如下：

密钥类型	生成与分发要求
初始密钥： l 企业主控密钥 l 企业空中传输密钥 l 企业空中报文 MAC 密钥 l 身份识别应用密钥 l 联机交易鉴权密钥 l 联机交易 TAC 密钥 l 消费密钥 l 充值密钥 l 脱机交易 TAC 密钥	对于各类初始密钥： l 企业根密钥：由一卡通业务系统从根密钥分散生成并注入密钥母卡，提供给企业 l 卡片子密钥： n 初始企业主控子密钥：由一卡通业务系统生成并在应用管理密钥的保护下写入用户卡 n 其它子密钥：由一卡通业务系统生成并写入 l 终端密钥：对于不二次洗卡的企业，则由发卡模块将应用根密钥分发到终端/PSAM 卡中
企业应用密钥（更新密钥）： l 企业主控密钥 l 企业空中传输密钥 l 企业空中报文 MAC 密钥 l 身份识别应用密钥 l 联机交易鉴权密钥 l 联机交易 TAC 密钥 l 消费密钥 l 充值密钥 l 脱机交易 TAC 密钥	l 企业根密钥：更新的企业密钥均由密钥母卡生成 l 卡片子密钥： n 企业主控子密钥：在初始企业主控子密钥的保护下将新的企业主控子密钥写入用户卡 n 其它子密钥：由密钥母卡生成并在新的企业主控子密钥的保护下写入用户卡 l 终端密钥：对于二次洗卡的企业，则由发卡模块将更新的应用根密钥分发到终端/PSAM 卡中

5.3 密钥存储

一卡通各应用密钥存储位置如下表所示：

密钥	密钥母卡	企业端管理系统	(U)SIM	终端(PSAM)
企业主控密钥	企业主控密钥（企业级）	N/A	企业主控子密钥	N/A
企业空中传输密钥	企业级空中传输密钥	一卡通应用根密钥 （不包含消费密钥和身份识别应用密钥）	企业空中传输子密钥	N/A
企业空中报文 MAC 密钥	企业级空中报文 MAC 密钥		企业空中报文 MAC 子密钥	N/A
身份识别应用密钥	企业级身份识别应用密钥		身份识别应用子密钥	企业级身份识别应用密钥（身份门禁/考勤等）

联机交易鉴权密钥	企业级联机交易鉴权密钥		联机交易鉴权子密钥	N/A
联机交易 TAC 密钥	企业级联机交易 TAC 密钥		联机交易 TAC 子密钥	N/A
消费密钥	企业级消费密钥		消费子密钥	企业级消费密钥
充值密钥	企业级充值密钥		充值子密钥	N/A
脱机交易 TAC 密钥	企业级脱机交易 TAC 密钥		脱机交易 TAC 子密钥	N/A

5.4 密钥更新

- 用户卡密钥更新：
  - **企业自行写入**：由企业端管理系统的发卡模块通过写卡器将更新密钥写入卡片中。
  - **空中写入（不二次洗卡）**：企业端管理系统的发卡子模块通过中国移动一卡通业务系统的空中通道将更新密钥写入卡片中。
  - **空中写入（二次洗卡）**：二次洗卡操作不能通过空中方式，但二次洗卡之后，如需密钥更新，则可以由企业端管理系统的发卡子模块通过中国移动一卡通业务系统的空中通道将更新密钥写入卡片中。
- 终端密钥更新：
  - 由企业端管理系统的发卡子模块通过终端/PSAM 卡读写机具（采用工作母卡）将更新密钥写入终端或 PSAM 卡中。
- 服务器密钥更新：

  由一卡通管理系统的密钥管理模块生成新密钥，更新到系统中。

6 密钥属性及相关要求

各密钥的使用都有一定的限制，必须满足密钥属性的要求。

密钥属性包括密钥长度、标识、密钥算法标识以及密钥版本等。

6.1 密钥长度

以上密钥均为 128bit 密钥。

6.2 密钥标识

密钥标识或密钥类型，长度为 1 个字节。

6.2.1 （U）SIM 卡中的密钥标识

各密钥标识长度为1字节，一卡通应用、每个子应用各自独立管理密钥，各密钥的初始版本号均为0x01。

密钥类型	密钥标识
企业主控密钥	0x01
企业空中传输密钥	0x02
企业空中报文 MAC 密钥	0x03
身份识别应用密钥	0x01
联机交易鉴权密钥	0x01
联机交易 TAC 密钥	0x02
消费密钥	0x01
充值密钥	0x02
脱机交易 TAC 密钥	0x03

6.2.2 母卡中的密钥标识

母卡、母卡认证卡、工作母卡中的密钥标识定义如下表所示，各密钥初始密钥版本号均为 0x01。

密钥类型	（U）SIM 卡	密钥母卡		母卡认证卡	工作母卡
		初始密钥	新密钥		
企业主控密钥	0x01	0x30	0xA0/0xAA	--	--
企业空中传输密钥	0x02	0x31	0xA1	--	--
企业空中报文 MAC 密钥	0x03	0x32	0xA2	--	--
身份识别密钥	0x01	0x40	0xB0	--	0x40 *只存一个应用密钥*
联机交易鉴权密钥	0x01	0x50	0xC0	--	--
联机交易 TAC 密钥	0x02	0x51	0xC1	--	--
脱机消费密钥	0x01	0x60	0xD0	--	--
充值密钥	0x02	0x61	0xD1	--	--
脱机交易 TAC 密钥	0x03	0x62	0xD2	--	--
终端初始密钥	--	0x80	--	--	0x80 *只存一个初始密钥*
SAM 卡卡片维护密钥	-	0x91	0x97	-	-
SAM 卡应用主控密钥	-	0x94	0x98	-	-
SAM 卡应用维护密钥	-	0x95	0x99	-	-

说明：

1、 **企业不能替换和删除的密钥**：上表中绿色底色的密钥，为中国移动初始化母卡过程中写入，企业不能删除和替换，包括人如下几类：
   a) 企业应用密钥（初始密钥）
   b) SAM卡卡片维护/应用主控/应用维护密钥：对于移动发行的SAM卡，移动通过密钥母卡向企业提供SAM卡卡片维护/SAM卡应用主控/SAM卡应用维护密钥，企业采用以上密钥可以向卡内写入其它密钥及其它信息，而SAM卡的卡片主控密钥由一卡通业务平台管理，不向企业提供
2、 **新的应用密钥**：采用密钥母卡生成新的应用密钥后，需要采用新的密钥标识（如上表中新密钥对应的标识所示），再次生成新密钥后，则覆盖上一次新密钥以及标识（企业主控密钥除外）。对于企业主控密钥，需要保存上一次生成的密钥及标识（更新卡片中的企业主控密钥需要原企业主控密钥的保护）。
3、 **终端初始密钥**：密钥母卡中只能保存一个终端初始密钥，工作母卡中只允许保存一个终端初始密钥和一个终端应用密钥（工作母卡不能识别多个终端初始密钥和多个终端应用密钥）。
4、 SAM**卡密钥**：在密钥母卡中预置了SAM卡卡片维护密钥、应用主控密钥、应用维护密钥，企业可以直接采用该密钥向SAM卡中写入应用主密钥（如消费密钥）及其它信息。

6.2.3 SAM 卡中的应用密钥标识

SAM 卡中的应用密钥标识（类型）定义如下表所示，其中初始版本号均为 0x01：

密钥类型	（U）SIM 卡	SAM 卡
身份识别密钥	0x01	0x03
脱机消费密钥	0x01	0x03
通用 DES 计算密钥	--	0x04

6.3 算法标识

密钥算法标识指定了密钥所支持的加密算法，长度为1字节。密算法标识约定如下：

表1-3 密钥算法标识

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	0	0	0—3DES
0	0	0	0	0	0	0	1	1—DES
X	X	X	X	X	X	X	X	2~255—保留

6.4 密钥版本

密钥版本指定某种类型密钥的标识，长度为 1 字节，范围 0x01-0xFF。所有密钥的版本

初始值为 0x01。

6.5 密钥索引

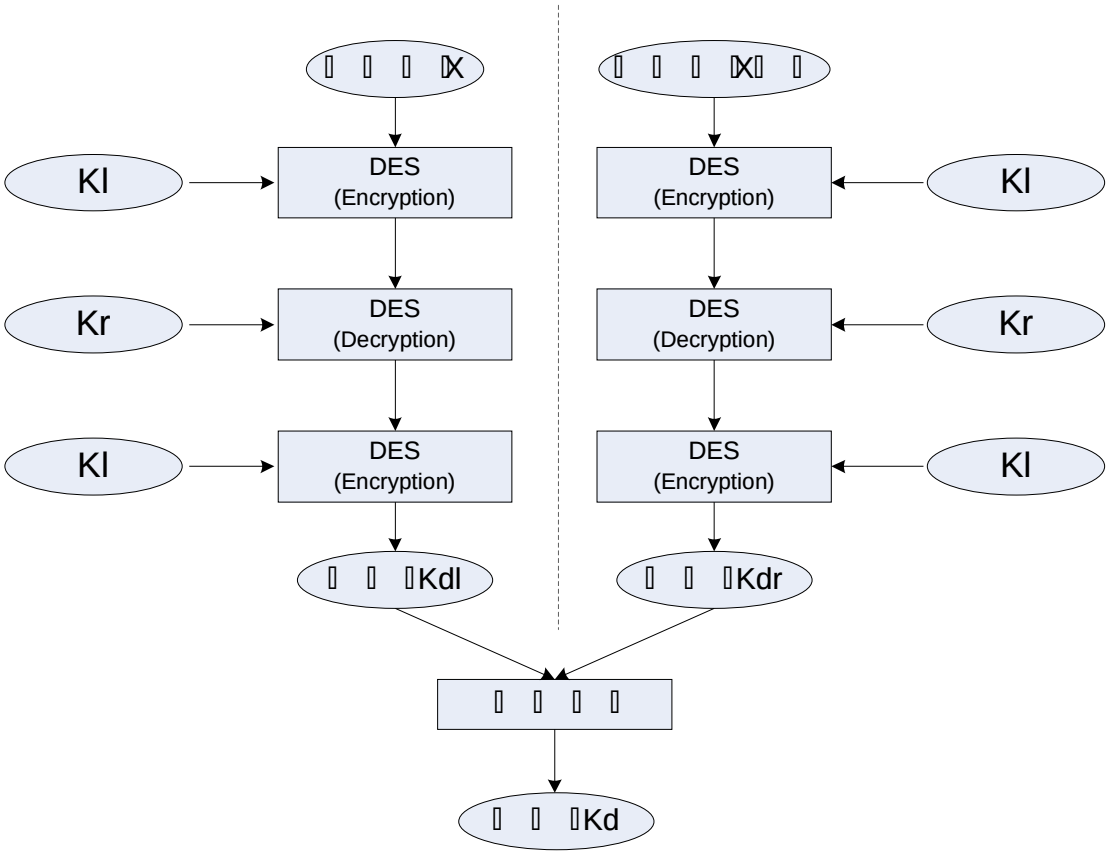
密钥索引，长度为 1 字节，范围 0x01-0xFF。所有密钥的索引初始值为 0x01。

7 编制历史

版本号	更新时间	主要内容或重大修改
1.0.0	2009-12-29	评审稿
1.0.0	2010-01-18	报批稿

附录 A 密钥分散算法

分散参数 X 不足 8 字节，则先补 0x80，如不足 8 字节则再补 0x00 至 8 字节。如分散参数超过 8 字节，则取最右 8 字节。



Kl = □ □ □ □ □ □ □ □　　Kdl = □ □ □ □ □ □

Kr = □ □ □ □ □ □ □ □　　Kdr = □ □ □ □ □ □

Kd = □ □ □

图 A-1 分散算法

附录 B 会话密钥的生成

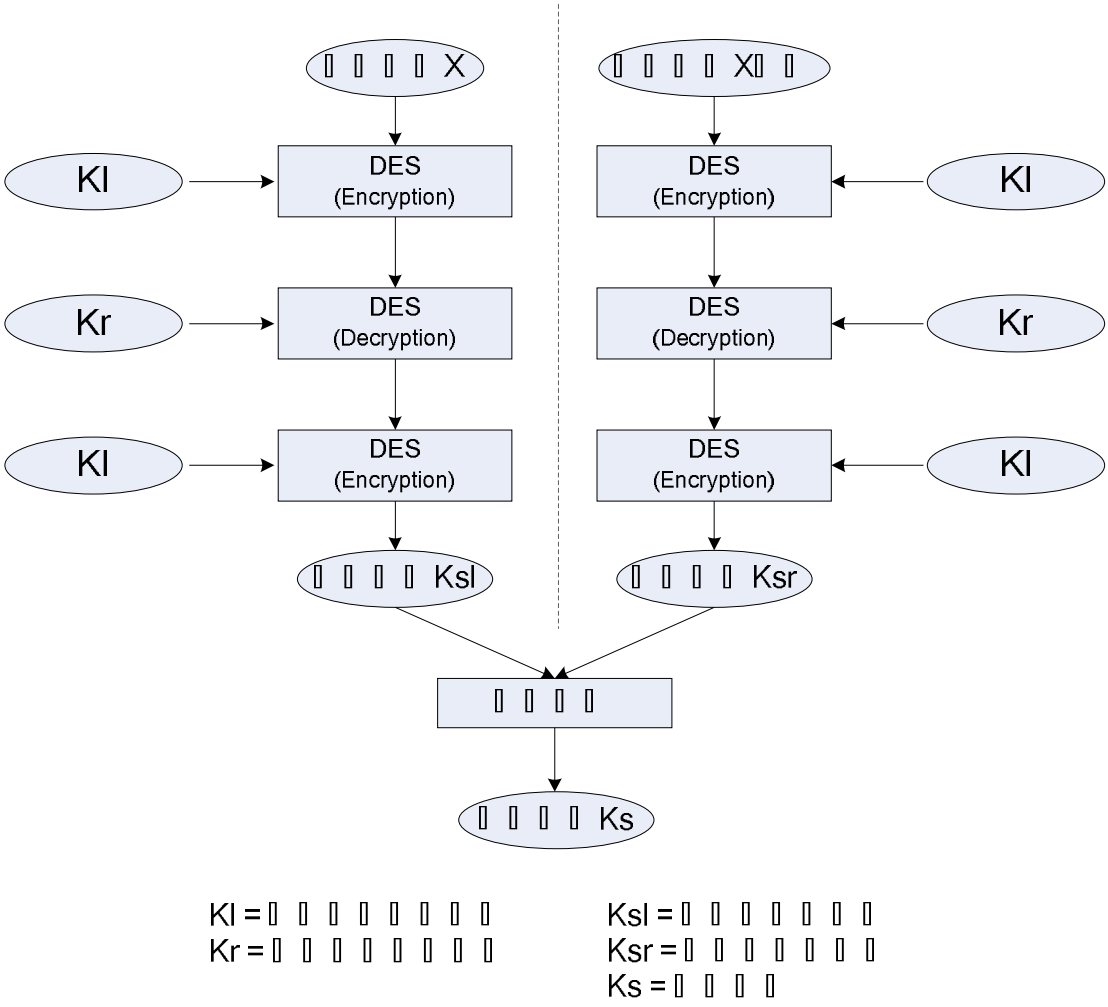
会话密钥是在交易的过程中用可变数据产生的双倍长密钥。会话密钥产生后只能在某过程/交易中使用一次。

图 B-1 描述了现场脱机支付进行消费交易时产生会话密钥的机制。这方法也用于不同交易类型的会话密钥的产生，但输入的数据取决于不同的交易类型。

会话密钥的分散参数的选取有两种情况：

1、对于只有一方提供了随机数的情况下，分散参数为：4 字节随机数+"0x80 00 00 00"

2、对于通信双方都提供了随机数的情况下，则分散参数为：（4 字节随机数 1）||（4 字节随机数 2）



图B-1 3DES会话密钥的分散算法

附录 C MAC/TAC 的计算

MAC/TAC 的产生使用以下算法：

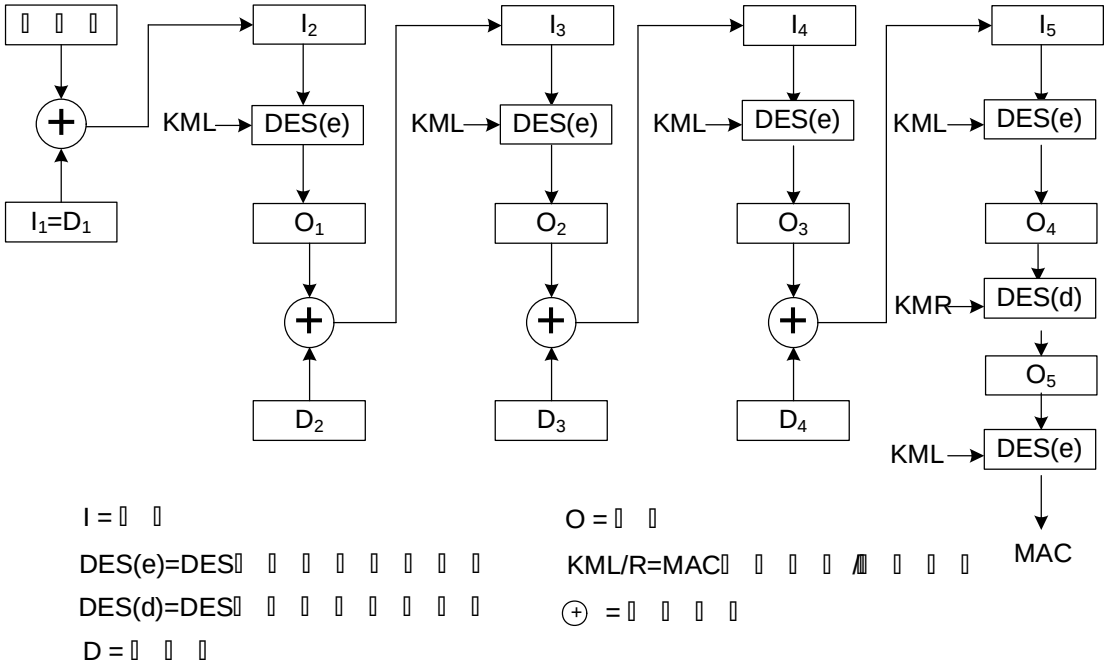
第一步：将一个 8 个字节长的初始值（Initial Vector）设定为 16 进制的'0x 00 00 00 00 00 00 00 00'。

第二步：将所有的输入数据按指定顺序连接成一个数据块。

第三步：将连接成的数据块分割为 8 字节长的数据块组，标识为 D1，D2，D3，D4 等等。分割到最后，余下的字节组成一个长度小于等于 8 字节的最后一块数据块。

第四步：如果最后一个数据块长度为 8 字节，则在此数据块后附加一个 8 字节长的数据块，附加的数据块为：16 进制的'0x 80 00 00 00 00 00 00 00'。如果最后一个数据块长度小于 8 字节，则该数据块的最后填补一个值为 16 进制 '0x80'的字节。如果填补之后的数据块长度等于 8 字节，则跳至第五步。如果填补之后的数据块长度仍小于 8 字节，则在数据块后填补 16 进制'0x00'的字节至数据块长度为 8 字节。

第五步：MAC 的产生是通过上述方法产生的数据块组，由会话密钥进行加密运算。MAC 算法见下图所示。



第六步：最终值的左4字节为MAC。

附录 D 加解密算法

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。

本节所述的加解密算法适用于 SIM 卡与其它设备之间的安全报文传送。

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，加密过程密钥按照附录 B 中描述的方式产生。

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)，L_D 长度为 1 个字节
- 明文数据
- 填充字符（参考本节“数据加密计算”中的说明）

然后整个数据块使用本节“数据加密计算”中描述的数据加密技术进行加密。

3 数据加密计算

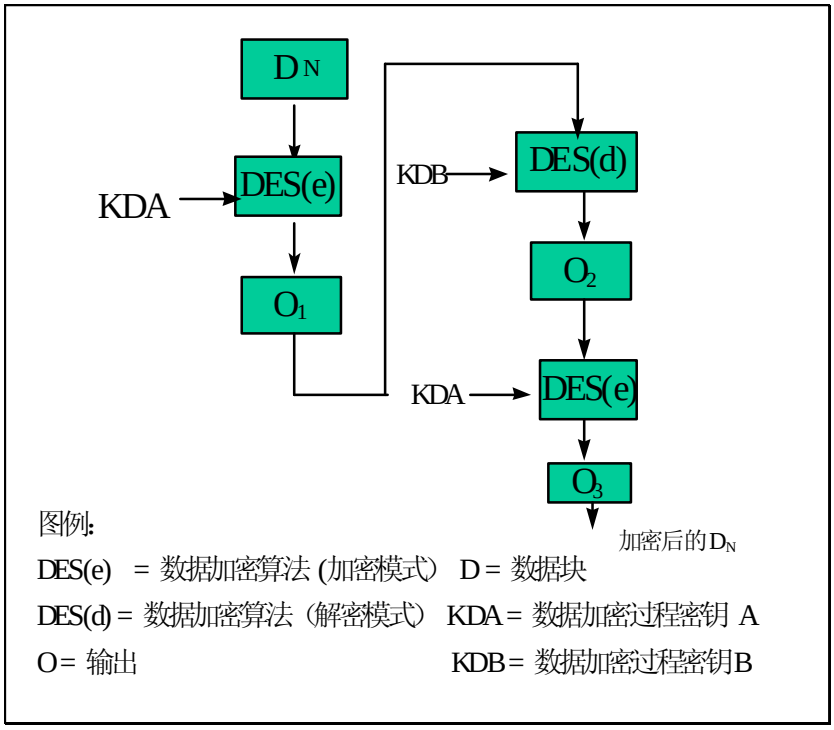
数据加密技术如下所述：

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 16 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 16 进制数字’0’直到长度达到 8 字节。

第四步：每一个数据块使用如下图所示的算法加密。

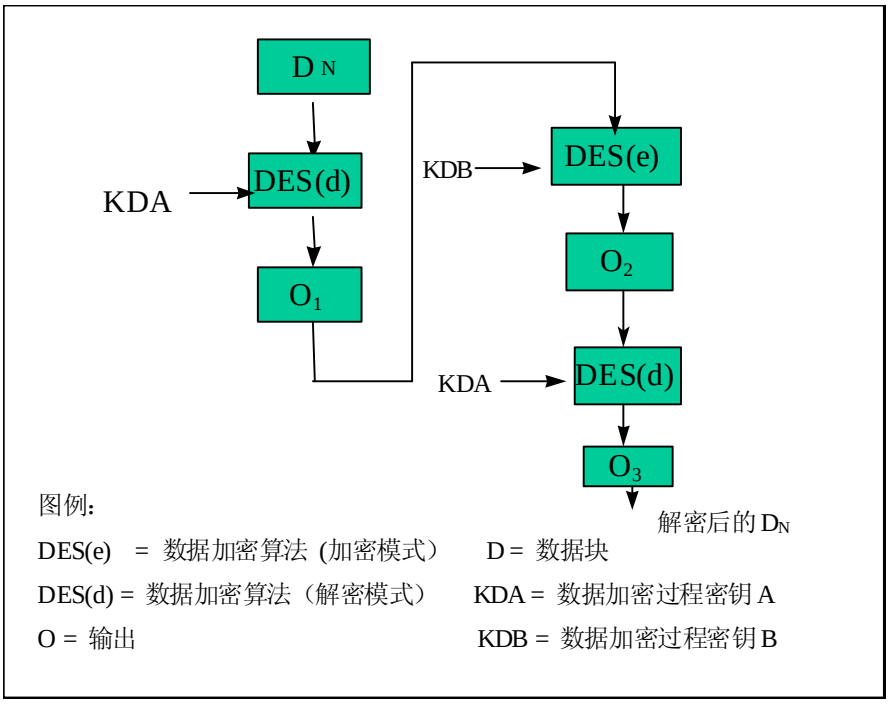


第五步：计算结束后，所有加密后的数据块依照原顺序连接在一起。

4 数据解密计算

数据解密的技术如下：

第一步：将密文数据块分解成 8 字节长的数据块，标号为 D1，D2，D3，D4 等等。每个数据块使用如下图所示的算法解密。



第二步：计算结束后，所有解密后的数据块依照顺序链接在一起。数据块由 L_D、明文数据、填充字符（如果在加密过程中进行填充的话）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。

附录 E （U）SIM 卡安全报文传送要求

本节对（U）SIM 卡的 APDU 安全指令进行介绍，具体的算法参考其它章节。

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 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。卡中的 FCI 表明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。

b4	b3	b2	b1	说　明
0	0	x	x	不需要安全报文
0	1	x	x	需要安全报文

2 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(Lc)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：

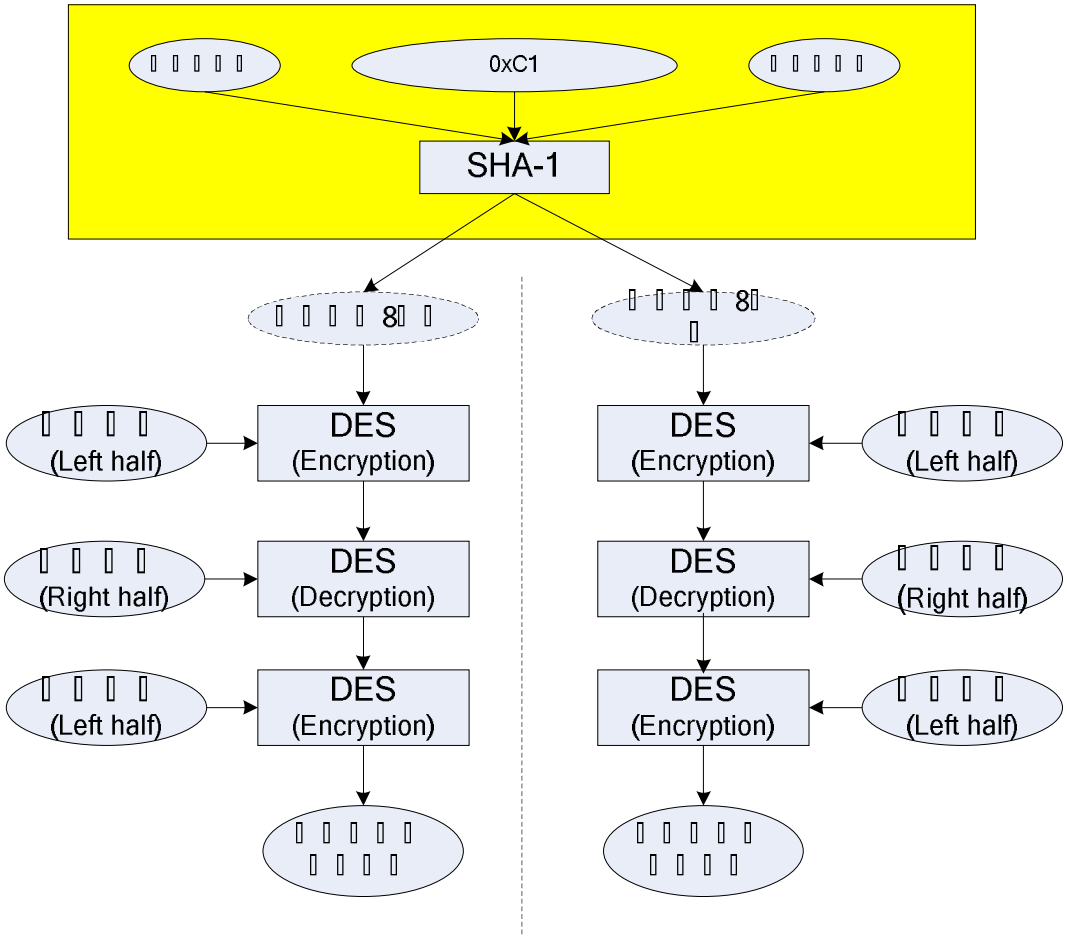
CLA	INS	P1	P2	Lc	命令数据	MAC	Le

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。

附录 F SAM 卡子密钥的分散规则

1 SAM 卡卡片维护密钥

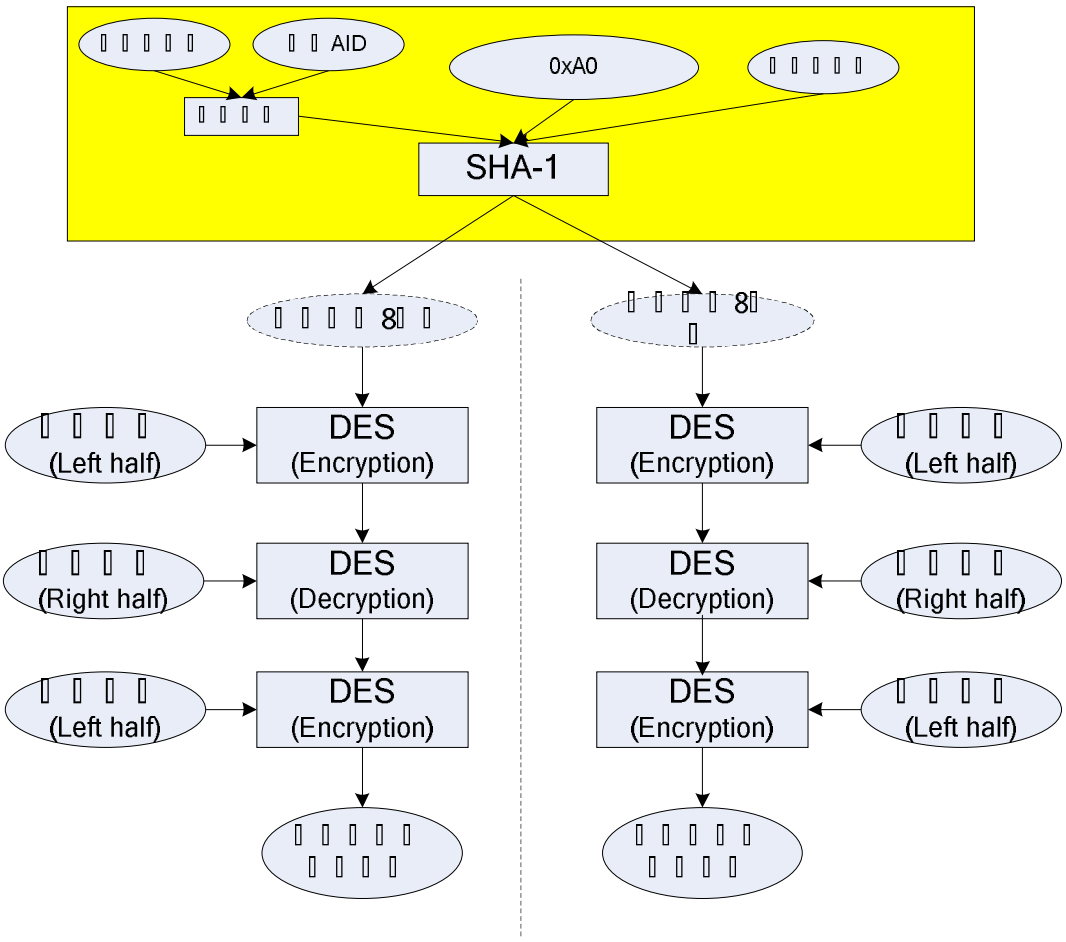
SAM卡卡片维护子密钥的分散规则如下图所示：



产生16字节双倍长卡片维护密钥左半部的输入分散参数为SHA-1(卡片序列号||0xC0||密钥版本号)散列结果值的左8个字节；产生卡片维护密钥右半部的输入分散参数为SHA-1(卡片序列号||0xC0||密钥版本号)散列结果值的右8个字节。

2 SAM 卡应用主控密钥

SAM卡应用主控子密钥的分散规则如下图所示：

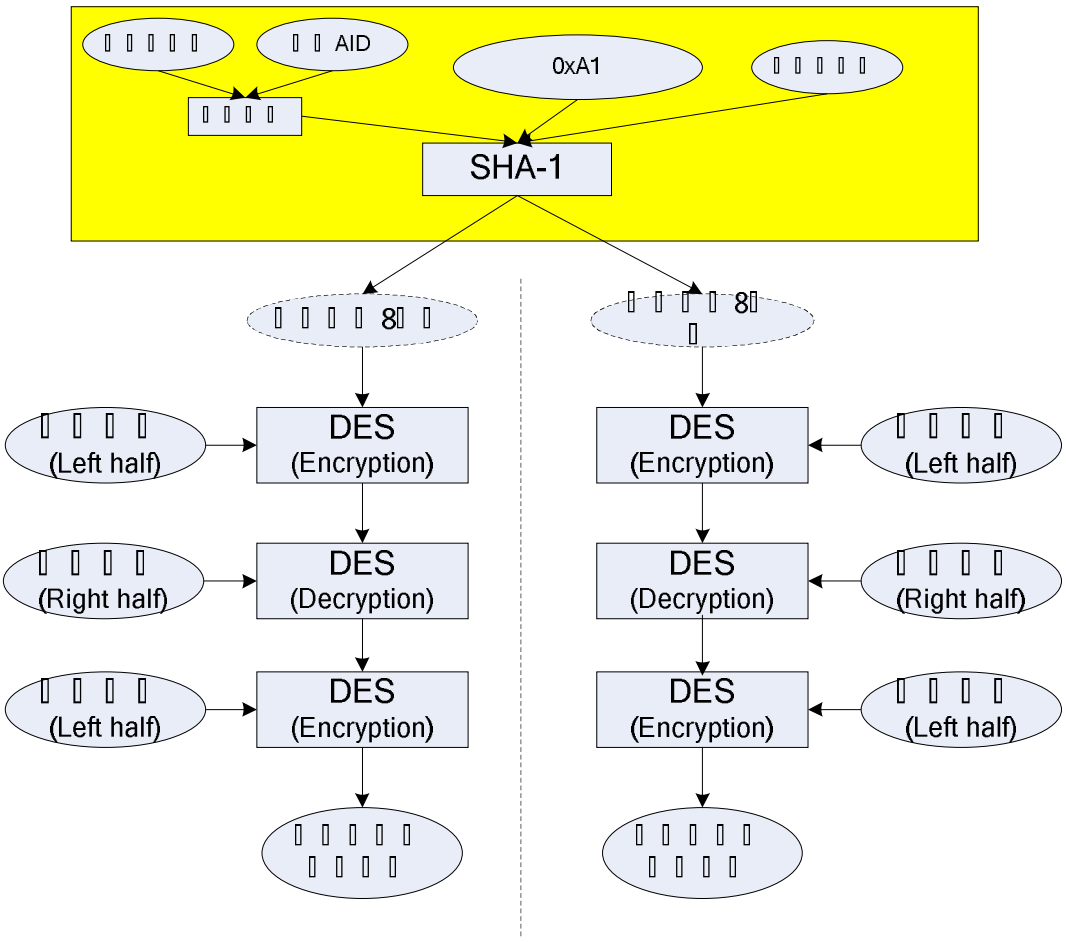


产生16字节双倍长应用主控密钥左半部的输入分散参数为SHA-1(（卡片序列号⊕应用AID)||0xA0||密钥版本号)散列结果值的左8个字节；产生应用主控密钥右半部的输入分散参数为SHA-1(（卡片序列号⊕应用AID)||0xA0||密钥版本号)散列结果值的右8个字节。

以上卡片序列号与AID异或操作中，卡片序列号需要左补0至与AID等长。

3 SAM 卡应用维护密钥

SAM卡应用维护子密钥的分散规则如下图所示：



产生16字节双倍长应用维护密钥左半部的输入分散参数为SHA-1(（卡片序列号⊕应用AID)||0xA1||版本号)散列结果值的左8个字节；产生应用维护密钥右半部的输入分散参数为SHA-1(（卡片序列号⊕应用AID)||0xA1||版本号)散列结果值的右8个字节。

以上卡片序列号与AID异或操作中，卡片序列号需要左补0至与AID等长。

附录 G 密钥使用详解

	会话密钥计算	MAC 初始向量	MAC 算法	TAC 初始向量	TAC 算法	加密算法
企业主控密钥	**A**	**C**	**E**			**F**
消费密钥	**A**	**C**	**E**			**F**
充值密钥	**A**	**C**	**E**			**F**
联机交易 TAC 密钥 脱机交易 TAC 密钥	**B**			**C**	**E**	**F**
身份识别应用密钥 联机交易鉴权密钥	**A**	**C**	**E**			**F**
企业空中传输密钥 企业空中报文 MAC 密钥	**A**	**C**	**E**			**F**
SAM 卡应用主控密钥 SAM 卡卡片维护密钥 SAM 卡应用维护密钥	**B**	**D**	**E**			**F**

说明：

A：双倍长会话密钥，本文档，附录 B

B：直接使用子密钥，不生成会话密钥

C：8 个字节长的初始值设定为 16 进制的’0x 00 00 00 00 00 00 00 00’

D：8 个字节长的初始值设定为 4 字节随机数后缀以’ 0x 00 00 00 00’

E：双倍长 3DES 算法，本文档，附录 C

F：本文档，附录 D

附录 H 省编码

需要说明的是：以下省编码为十进制代码。在根密钥分散为省密钥过程中，需要转换为 16 进制（如：下表中重庆的省代码为 31，对应的 16 进制编码为 0x1F）。在其它编码（如企业 ID、应用序列号等）中无须转换。

省区市	代码	省区市	代码
北京	01	河南	16
天津	02	湖北	17
河北	03	湖南	18
山西	04	广东	19
内蒙古	05	广西	20
辽宁	06	海南	21
吉林	07	四川	22
黑龙江	08	贵州	23
上海	09	云南	24
江苏	10	西藏	25
浙江	11	陕西	26
安徽	12	甘肃	27
福建	13	青海	28
江西	14	宁夏	29
山东	15	新疆	30
		重庆	31