中国移动通信
CHINA MOBILE

中 国 移 动 通 信 企 业 标 准

QB-Y-031.13-2013

NGBOSS2-CRM(V4.5)(U)SIM卡写卡技术规范支撑分册

Technology Specification of On-Demand Personalization of (U)SIM Card

版本号：2.1.0

2013-8-21 发布　　2013-8-21 实施

中国移动通信集团公司　　发布

目　　录

前　言

本标准规定了中国移动SIM卡、USIM卡现场写卡的业务特征、网络架构、业务流程、关键技术、设备要求等内容，是中国移动通信集团开展SIM卡和USIM卡现场写卡业务开发、测试、运营的依据。本标准适用于中国移动SIM卡、USIM卡现场写卡，适用于中国移动自有营业厅及非自有营业厅现场写卡，并支持通过PC或智能终端等实现现场写卡。

本标准适用于中国移动GSM、GPRS、3G、LTE网络环境。

本标准是现场写卡系列标准之一，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-Y-031.13-2013	NGBOSS2-CRM(V4.5) (U)SIM卡写卡技术规范支撑分册
[2]	QB-Y-031.14-2013	NGBOSS2-CRM(V4.5) (U)SIM卡写卡业务规范支撑分册

本标准的附录A、B、C、D为资料性附录，附录E、F为标准性附录。

本标准由中移技〔2013〕172号印发。

本标准由中国移动通信集团业务支撑部提出，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：张颖、任晓明、杨超、王健、罗红、朱本浩

1　范围

本标准规定了SIM卡、USIM卡现场写卡的业务特征、系统架构、业务流程、关键技术要求、设备要求、系统要求等内容，是中国移动通信集团公司开展现场写卡业务的依据。本标准适用于SIM卡、USIM卡的现场写卡。现场写卡业务可覆盖自有营业厅现场写卡、非自有营业厅现场写卡，非自有营业厅现场写卡可覆盖代理渠道现场写卡、校园营销类现场写卡等。

中国移动的SIM卡和USIM卡供应商应根据本标准要求提供SIM卡、USIM卡，系统提供商应根据本标准要求提供现场写卡业务设备或系统。

用于现场写卡的SIM卡应符合GSM11.11、GSM11.14等标准的要求，其文件系统配置应符合《中国移动SIM卡技术规范》的要求。用于现场写卡的USIM卡应符合ETSI TS 102.221、3GPP TS 31.111 、3GPP TS 31.102等标准的要求。

为满足LTE USIM卡集中管理和跨省写卡相关需求，并根据省公司反馈在现网升级过程中发现的一些需求及问题，2.1.0版本对《NGBOSS2-CRM(V4.5) (U)SIM卡写卡技术规范支撑分册》V2.0.0的进行了升级和扩充。

1. 针对现网对跨省写卡的需求，跨省密钥 （K2）如采用对称方式对集团及各省公司的密钥管理提出很高的要求，而且存在密钥泄露的风险；
2. 各省公司在密钥使用方面存在较大差异，为实现多组密钥的管理和使用要求，需对密钥使用过程中的加密机规格及加密机密钥调用方式提出标准和明确要求；
3. 现场写卡业务定义的多组密钥，包括K1、KEK、K2等，需要对其提出明确的管理要求，包括密钥生成、密钥传输等关键环节。

根据上述需求及问题，本标准修订跨省 USIM 卡写卡的相关密钥及业务处理流程，增加省级写卡使用的加密机技术要求，修订跨省写卡相关的密钥管理要求等，主要修订内容包括：

1. 重新定义K2密钥为非对称密钥，每省1对，用于保护跨省传输的预置数据；修订与跨省传输相关的各网元接口等技术点；
2. 对加密机的功能、技术指标等提出明确要求；针对加密机的API进行了增补和优化；
3. 增加密钥导入导出相关要求，增加密钥传输卡操作的指令流程及技术要求，并针对各类密钥的技术要求进行补充及修订。另增加对密钥管理流程的说明，参见《中国移动(U)SIM卡发卡密钥管理方案(电信应用部分)》。

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2-1　规范性引用文件

序号	标准编号	标准名称	发布单位
[1]	ISO/IEC 7816-1 (1998)	3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface"	ISO/IEC
[2	ISO/IEC 7816-4 (1995)	"Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange"	ISO/IEC
[3]	ISO/IEC 7816-5 (1994)	"Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers"	ISO/IEC
[4]	ISO/IEC 7816-6 (1996)	"Identification cards -- Integrated circuit(s) cards with contacts -- Part 6: Interindustry data elements"	ISO/IEC
[5]	ISO/IEC 8825(1990)	"Information technology; Open Systems Interconnection; Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)"	ISO/IEC
[6]	GSM 11.11	Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (V8.3.0: 2000-08)	ETSI
[7]	GSM 11.14	Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (V8.3.0: 2000-08)	ETSI
[8]	ETSI TS 102.221	Smart Cards; UICC-Terminal interface;Physical and logical Characteristics	ETSI
[9]	3GPP TS 31.111	" USIM Application Toolkit (USAT)".	3GPP
[10]	3GPP TS 31.102	"Characteristics of the USIM application"	3GPP
[11]	QB-E-005-2004	SIM 卡远程写卡业务规范(V1 0 0)	中国移动通信集团公司
[13]	QB-E-001-2012	中国移动防克隆 SIM 卡技术规范(V2.0.0)	中国移动通信集团公司
[14]	QB-E-065-2011	中国移动 SIM 卡技术规范(V1.0.0)	中国移动通信集团公司
[15]	QB-E-023-2011	中国移动 LTE USIM 卡技术规范(V1.0.0)	中国移动通信集团公司

[16]	QB-Y-037.5-2012	NGBOSS2-CRM(V4.0)智能终端版 CRM 分册(V1.0.0)	中国移动通信集团公司
[17]	QB-Y-037.2-2012	NGBOSS2-CRM(V4.0)渠道协同支撑分册	中国移动通信集团公司

3 术语、定义和缩略语

3.1 术语、定义

下列术语和定义适用于本标准：

表3-1 术语与定义

词语	解释
现场写卡业务	现场写卡业务指在自有营业厅、非自有营业厅（例如代理渠道、校园等）现场向用户卡内写入个人化数据，并与其他系统（例如 CRM、BOSS 等）配合实现号码开通等功能的业务。
个人化数据	与用户身份相关、需要写入用户卡中的特定数据集合，通常用于网络鉴权的参数和个人数据，SIM 个人化数据包括 ICCID、IMSI、Ki，SMSP、PIN1、PUK1、PIN2、PUK2 以及伪 Ki、索引随机数；USIM 个人化数据包括 ICCID、IMSI、OPc，K，SMSP、PIN1、PUK1、PIN2、PUK2。伪 Ki、索引随机数的定义具体参见《中国移动防克隆 SIM 卡技术规范》V2.0.0。
预置数据	特指在工厂生产卡片时写入的部分个人化数据。对于 SIM 卡，预置数据包括 Ki、伪 Ki、索引随机数，对于 USIM 卡，预置数据包括 K、OPc。
实时写卡数据	特指通过现场写卡业务实时写入的除预置数据外的其他个人化数据，包括 ICCID、IMSI、SMSP、PIN1、PIN2、PUK1、PUK2 等。
实卡	已完成全部个人化数据写入的 SIM 卡、USIM 卡。
空卡	未进行任何个人化数据项写入的 SIM 卡、USIM 卡。
预置空卡	已在工厂生产阶段写入预置数据的 SIM 卡、USIM 卡。
统一写卡组件	指适用于特定 SIM 卡、USIM 卡等用户卡校验、写卡等操作的，独立封装的，供客户端调用的软件模块，本标准中主要用于完成预置空卡的校验、写卡等操作。
写卡资源库	指现场写卡业务中管理数据资源的系统或模块，数据资源包括空卡序列号及预置数据、实时写卡数据等。相应功能的实现各省公司可视情况在现场写卡系统中实现，也可在 CRM 系统中实现。本标准仅为流程描述方便，将其单独列出。
空卡序列号	即空卡标识文件，为方便空卡的管理，卡片生产时在 SIM 卡和 USIM 卡中建立的特定标识文件，用以标识该空卡的供应商、类别、出厂时间、序列号、卡功能标识等信息。
预置卡密钥	需提前预置在预置空卡中，用于对写卡数据报文的加解密，

	并用于生成写卡报文 MAC 计算的会话密钥。
智能终端	是指具有独立的操作系统，可以由用户自行安装软件等第三方服务商提供的程序，通过此类程序可对终端的功能进行扩充，并可以通过移动通讯网络实现无线网络接入的一类终端的总称，例如 PAD 等。
SIM 个人化数据生成系统	负责生成 SIM 个人化数据的系统或模块。在现场写卡业务中,SIM 个人化数据生成系统生成 SIM 卡预置空卡的预置数据及预置空卡的实时写卡数据，另外需生成空卡序列号、预置卡密钥、预置数据的对应文件。
一卡多号卡	本标准中的一卡多号卡是指在 SIM/USIM 卡内存储 2 个或 2 个以上的个人化数据。
本省写卡	用户在归属省使用现场写卡业务。
跨省写卡	用户在漫游省使用现场写卡业务。

3.2 缩略语

表 3-2 缩略语

词语	解释
SIM	用户识别模块
USIM	通用用户识别模块
ICCID	IC卡片识别号
APDU	应用协议数据单元
IMSI	移动用户识别号
Ki	用户认证密钥
K	用户认证密钥
OP	鉴权参数
OPc	由OP和K分散得到的密钥
HLR	归属地寄存器
BOSS	业务支撑系统
SMSP	短消息中心
MAC	消息验证码
ATR	复位应答
CRM	用户关系管理
OPS	现场写卡
DCN	数据通信网

4 业务概述

现场写卡业务支持自有营业厅现场写卡、非自有营业厅现场写卡。

自有营业厅现场写卡，是由移动营业员通过可靠、高速的内网接入现场写卡系统等系统，使用营业终端（PC 机或智能终端等）和读卡器实施读写卡业务，完成现场写卡、现场开通等相关操作。

非自有营业厅现场写卡，包括代理渠道现场写卡及校园营销类现场写卡，由代理商或者移动营业人员通过安全可靠的方式接入 Internet 网络并接入现场写卡系统等内网系统，使用营业终端（PC 机或智能终端等）和读卡器实施写卡业务，完成现场写卡、现场开通等相关操作。其中校园营销类现场写卡多数发生在特定时间（如校园开学、营销活动等）、特定场合（如针对 VIP 用户或公司用户进行上门服务）实时的现场写卡业务。

5 网络架构

5.1 组网结构

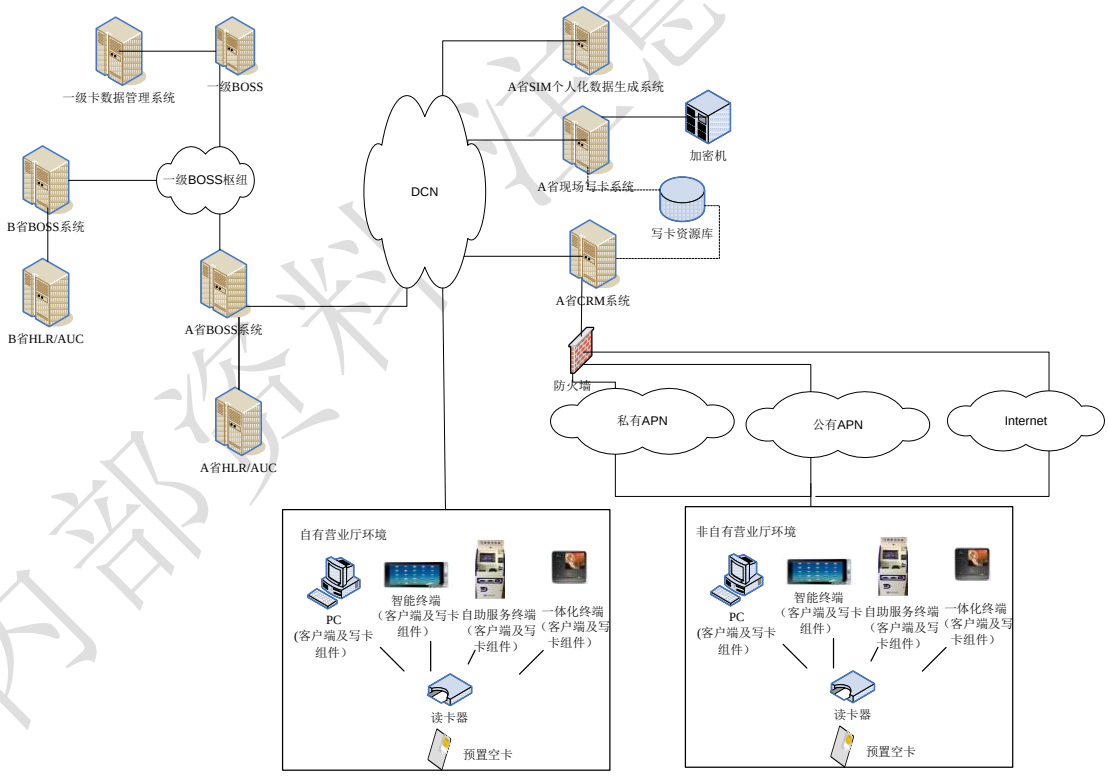


图 5-1 组网结构图

5.2 各网元描述

5.2.1 预置空卡

预置空卡包括 SIM、USIM 等不同卡类型。预置空卡将写入实时写卡数据。

5.2.2 读卡器

读卡器与卡片进行交互，完成读取卡内信息及实时写卡数据的写入等功能。

5.2.3 统一写卡组件

统一写卡组件与客户端进行交互，并可通过读卡器与卡片进行交互，完成卡内信息的读取及实时写卡数据的写入等功能。

5.2.4 客户端

客户端是 PC 机或自助服务终端上的采用浏览器方式的写卡界面，或者是部署在智能终端（例如 PAD）上的应用软件，通常与 CRM 系统连接。在现场写卡业务中，客户端软件为现场写卡业务提供操作界面，并与统一写卡组件及 CRM 进行交互，配合实现卡片信息获取及实时写卡数据的写入等功能。

5.2.5 现场写卡系统

现场写卡系统是现场写卡业务的主要设备，负责受理现场写卡指令的打包及写卡结果的报文解释工作，控制实时写卡数据写入、安全管理，组件管理，基础数据管理等功能。该系统在原远程写卡系统上进行升级，分省建设。

5.2.6 加密机

为了保证现场写卡的数据安全，各省公司应配备加密机。加密机与现场写卡系统交互，提供现场写卡业务的密钥存储及加解密功能。

5.2.7 SIM 个人化数据生成系统

SIM 个人化数据生成系统负责生成 SIM 个人化数据。在现场写卡业务中，SIM 个人化数据生成系统生成 SIM 卡预置空卡的预置数据及预置空卡的实时写卡数据，另外需生成空卡序列号、预置卡密钥、预置数据的对应文件。

SIM 个人化数据生成系统可独立建设，根据各省情况，也可与现场写卡系统或 CRM 系统进行合设。

注：在一级卡数据管理系统未建设完成之前，SIM 个人化数据生成系统可代为生成 USIM 卡个人化数据，及 K、OPc 与空卡序列号、预置卡密钥的对应文件。在一级卡数据管理系统建设完成后，SIM 个人化数据生成系统要实现与一级卡数据管理系统之间的 USIM 卡个人化数据的迁移。

5.2.8 CRM 系统

CRM 系统是提供给营业员或者合作代理渠道使用，负责给用户进行发卡和补换卡的业务系统。用户客户端从现场写卡系统获取写卡相关数据，通过写卡组件完成用户卡数据的写入，通过 BOSS 完成 HLR 用户鉴权数据的写入。

5.2.9 BOSS 系统

BOSS 系统负责处理从 CRM 传递的客户鉴权信息，完成 HLR 的操作，以及与一级 BOSS 进行跨省数据交换、实现 USIM 卡个人化数据转发等功能。

5.2.10 一级 BOSS 系统/网状网

在现场写卡业务中，一级 BOSS 系统，即升级后的网状网，是跨省写卡业务数据及 USIM 卡数据接口枢纽。一级 BOSS 系统负责与省 BOSS 系统进行跨省数据的交换及负责一级卡数据管理系统与省 BOSS 系统进行的 USIM 卡数据的转发。

5.2.11 一级卡数据管理系统

在现场写卡业务中，一级卡数据管理系统为各省公司 USIM 制卡提供数据生成服务。该系统为规划新建设备。

5.3 组网要求

现场写卡系统通过省公司内部 DCN 网实现与 CRM 系统的连接。

CRM 系统通过省公司内部 DCN 网实现与省 BOSS 系统的连接。

省 BOSS 系统通过 DCN 网或者专线与 HLR 连接。

省 BOSS 系统通过专线或者承载网连接一级 BOSS 枢纽，实现与一级 BOSS 连接。

一级卡数据管理系统通过专线实现与一级 BOSS 连接。

自有营业厅办理环境的 PC、智能终端、自助服务终端等设备通过省公司内部 DCN 网实现与 CRM 系统的连接。

非自有营业厅办理环境的 PC、智能终端设备、自助服务终端可通过公有 APN 或专用 APN 或 Internet 方式接入 CRM 系统，具体接入要求参见《NGBOSS2-CRM(V4.5)智能终端版 CRM 分册》。

6　系统结构

6.1　系统结构图

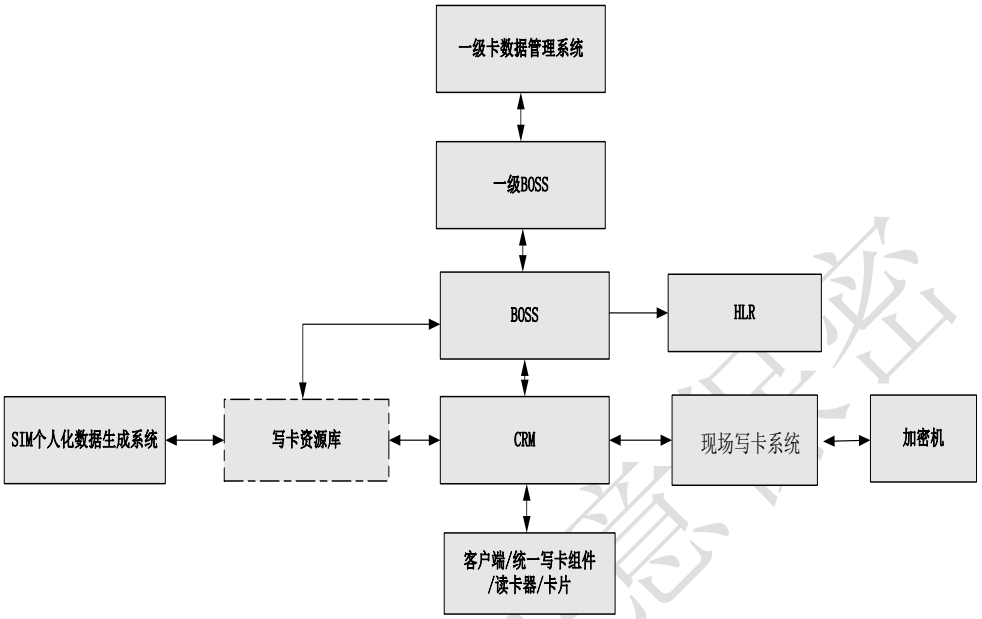


图 6-1　系统结构图

6.2　系统功能概述

个人化数据生成阶段：SIM 个人化数据生成系统将 SIM 个人化数据导入写卡资源库中；一级卡数据管理系统将 USIM 个人化数据通过一级 BOSS、BOSS 导入到写卡资源库中；写卡资源库需将导入结果反馈 SIM 个人化数据生成系统及一级卡数据管理系统。

写卡阶段：由客户端发起写卡请求，CRM 系统从写卡资源库获取个人化数据，并将个人化数据发送到现场写卡系统，现场写卡系统通过加密机将个人化数据进行加密后返回 CRM，由 CRM 下发到客户端，最终写入卡内，并将写卡结果回传。

开通阶段：确认写卡成功后，CRM 系统通知 BOSS 进行开通操作，由 BOSS 通知 HLR 进行开通。

7　业务流程

7.1　卡数据生成流程

7.1.1　SIM 数据生成流程

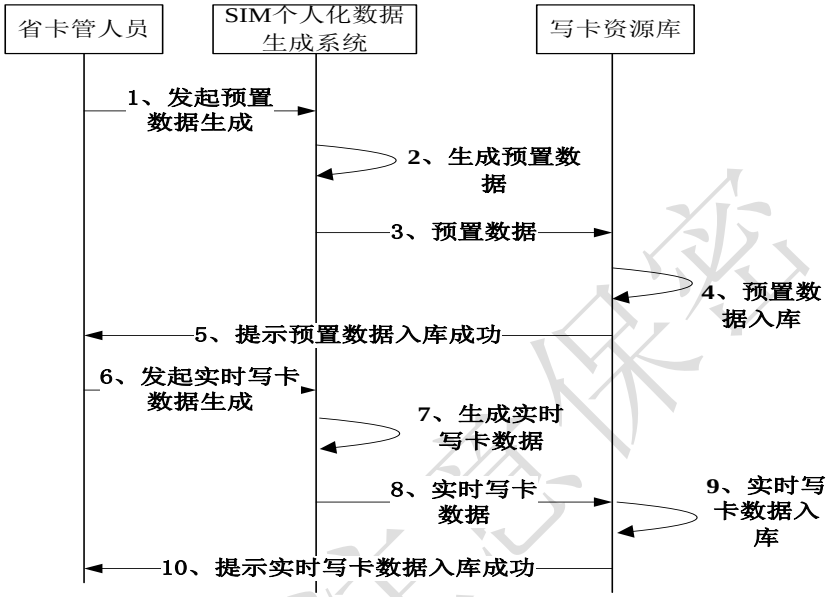


图 7-1　SIM 数据生成流程图

流程描述：

1. 省卡管人员通过 SIM 个人化数据生成系统发起预置数据生成操作。
2. SIM 个人化数据生成系统根据卡管人员的输入条件，生成预置数据、空卡序列号、预置卡密钥。
3. SIM 个人化数据生成系统将空卡序列号、经 KEK 加密后的预置数据传给写卡资源库。
4. 写卡资源库将空卡序列号、经 KEK 加密后的预置数据导入到数据库中。
5. 写卡资源库提示省卡管人员预置数据已经成功导入到数据库。
6. 省卡管人员通过 SIM 个人化数据生成系统发起实时写卡数据生成请求。
7. SIM 个人化数据生成系统根据卡管人员的输入要求，生成实时写卡数据。
8. SIM 个人化数据生成系统将实时写卡数据传给写卡资源库。
9. 写卡资源库将实时写卡数据导入到数据库中。
10. 写卡资源库提示省卡管人员实时写卡数据已经成功导入到数据库。

注 1：预置数据导入写卡资源库前，需确认发给卡商的制卡文件（由预置数据、空卡序列号、预置卡密钥组成）接收成功，保证写卡数据的一致性。

注 2：SIM 数据生成可以采用批量生成方式。

7.1.2 USIM卡数据生成流程

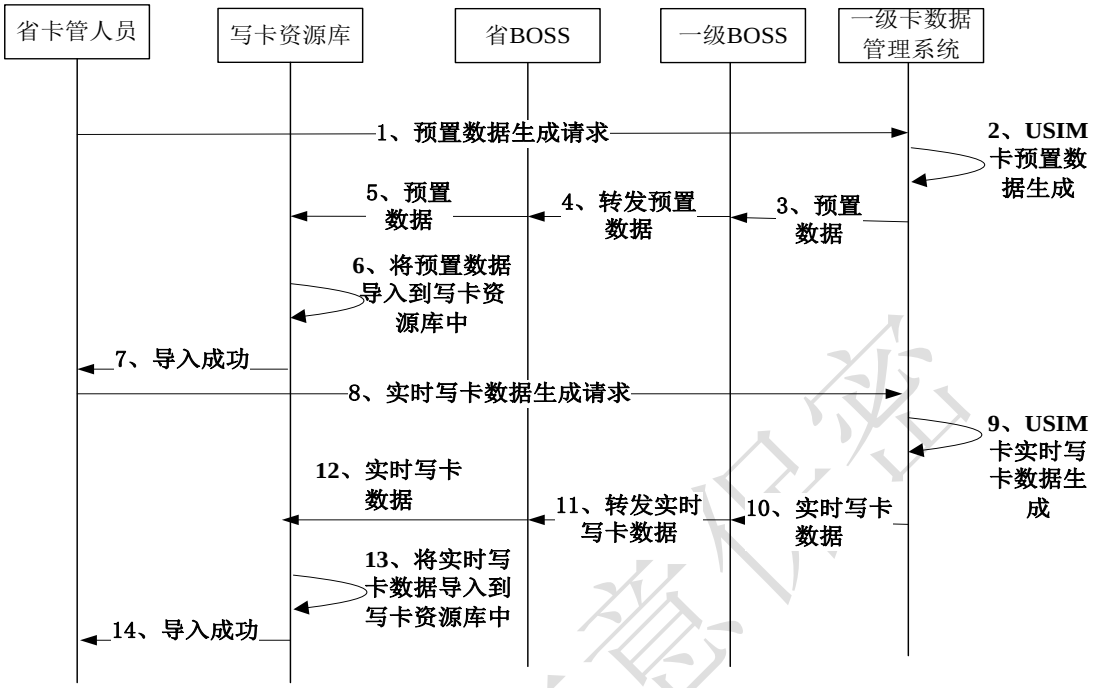


图 7-2 USIM 数据生成流程图

流程描述：

1. 省卡管人员通过一级卡数据管理系统发起 USIM 卡预置数据生成请求，该请求包括省份，制卡数量，数据申请时间等。
2. 一级卡数据管理系统根据省公司数据生成的申请要求，生成省公司所需的预置数据、空卡序列号、预置卡密钥。
3. 一级卡数据管理系统将生成的空卡序列号、经 KEK 加密后的预置数据传给一级 BOSS 系统。
4. 一级 BOSS 系统将空卡序列号、经 KEK 加密后的预置数据透传给省 BOSS 系统。
5. 省 BOSS 系统将空卡序列号、经 KEK 加密后的预置数据传给写卡资源库，
6. 写卡资源库将空卡序列号、经 KEK 加密后的预置数据导入到写卡资源库中。
7. 写卡资源库提示省卡管人员预置数据已经成功导入到数据库。
8. 省卡管人员通过一级卡数据管理系统发起 USIM 卡实时写卡数据生成请求。
9. 一级卡数据管理系统根据省公司数据生成的申请要求，生成省公司所需的实时写卡数据。
10. 一级卡数据管理系统将生成的实时写卡数据文件传给一级 BOSS 系统。
11. 一级 BOSS 系统将实时写卡数据文件透传给省 BOSS 系统。
12. 省 BOSS 系统将实时写卡数据文件传给写卡资源库，实时写卡数据文件格式参见一级卡数据管理系统相关接口规范。

13. 写卡资源库将实时写卡数据文件中的实时写卡数据导入到写卡资源库数据库中。

14. 写卡资源库提示省卡管人员实时写卡数据已经成功导入到数据库。

注 1：预置数据导入写卡资源库前，需确认发给卡商的制卡文件（由预置数据、空卡序列号、预置卡密钥组成）接收成功，保证写卡数据的一致性。

注 2：一级卡数据生成系统在规划建设中，以上流程为拟定流程，具体根据一级卡数据生成系统相关规范实施。在一级卡数据管理系统未建设完成之前，SIM 个人化数据生成系统可代为生成 USIM 卡个人化数据。

注 3：USIM 数据生成可以采用批量生成方式。

7.2 写卡流程

现场写卡分为本省写卡和跨省写卡两部份。写卡过程主要包括获取空卡序列号、新旧空卡识别、卡片信息获取、空卡及卡类识别，写卡数据获取，写卡数据写入，开通等七个步骤。

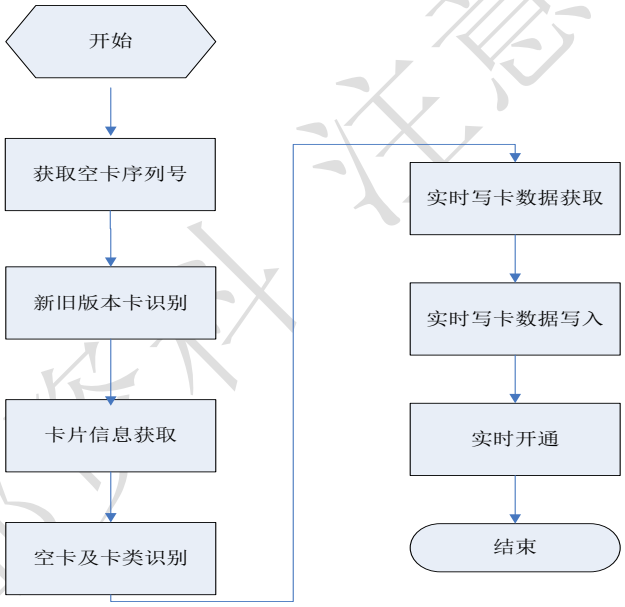


图 7-3 写卡流程图

1. 客户端调用统一写卡组件获取空卡序列号用于进行新旧版本卡片的识别。

2. 新旧版本空卡识别是指识别卡片的新旧版本，在本标准发布前各省已经发行的空卡采用 16 位空卡序列号，将此类卡片称为旧版本空卡，本标准发布后，各省发行新的用于现场写卡的空卡采用 20 位空卡序列号，预置个人化数据、预置卡密钥等，并能够完成自解密和自写卡功能，将此类卡片称为新版本空卡，即预置空卡。新旧版本空卡识别是通过空卡序列号的长度来识别的。

3. 卡片信息获取是指统一写卡组件在写卡之前，通过向预置空卡发送卡片信息指令，获取卡片的一些基本信息。基本信息包括卡片的空卡序列号，卡内的 ICCID 数据等。

4. 空卡及卡类识别是根据卡片空卡序列号及 ICCID 等信息确定卡片是否为空卡，及卡片的类型，如单号/多号， SIM/USIM 等。

5. 实时写卡数据获取是指 CRM 从写卡资源库获取实时写卡数据并发给现场写卡系统进行报文组装。写卡资源库根据各省情况的不同，可由现场写卡系统实现或者是由 CRM 系统实现。写卡资源库的数据来自两部份，一部份来源于 SIM 个人化数据生成系统，这部份数据主要是指 SIM 卡数据，另一部份来源于一级卡数据管理系统，这部份数据主要是指 USIM 卡数据。

6. 写卡数据写入是指客户端软件调用统一写卡组件，将实时写卡数据写入预置空卡。

7. 实时开通包括两部份操作，一部份是指 BOSS 系统实时地将鉴权数据（IMSI，KI/（K，OPC））导入到 HLR 并激活的过程。另一部份是指 CRM 系统或 BOSS 系统建立客户档案并建立客户号码及客户卡基本信息关系。

7.2.1 本省写卡流程

本省写卡包括本省新开户写卡及本省补换卡写卡两种情况，补换卡写卡和新开户写卡的写卡流程基本一致。两者的不同之处在于补换卡写卡要求在写卡之前需要对用户的号码及身份信息进行验证核对，具体验证核对要求根据集团或各省公司相关部门规定由 CRM 实施。

本省写卡流程如下图示。

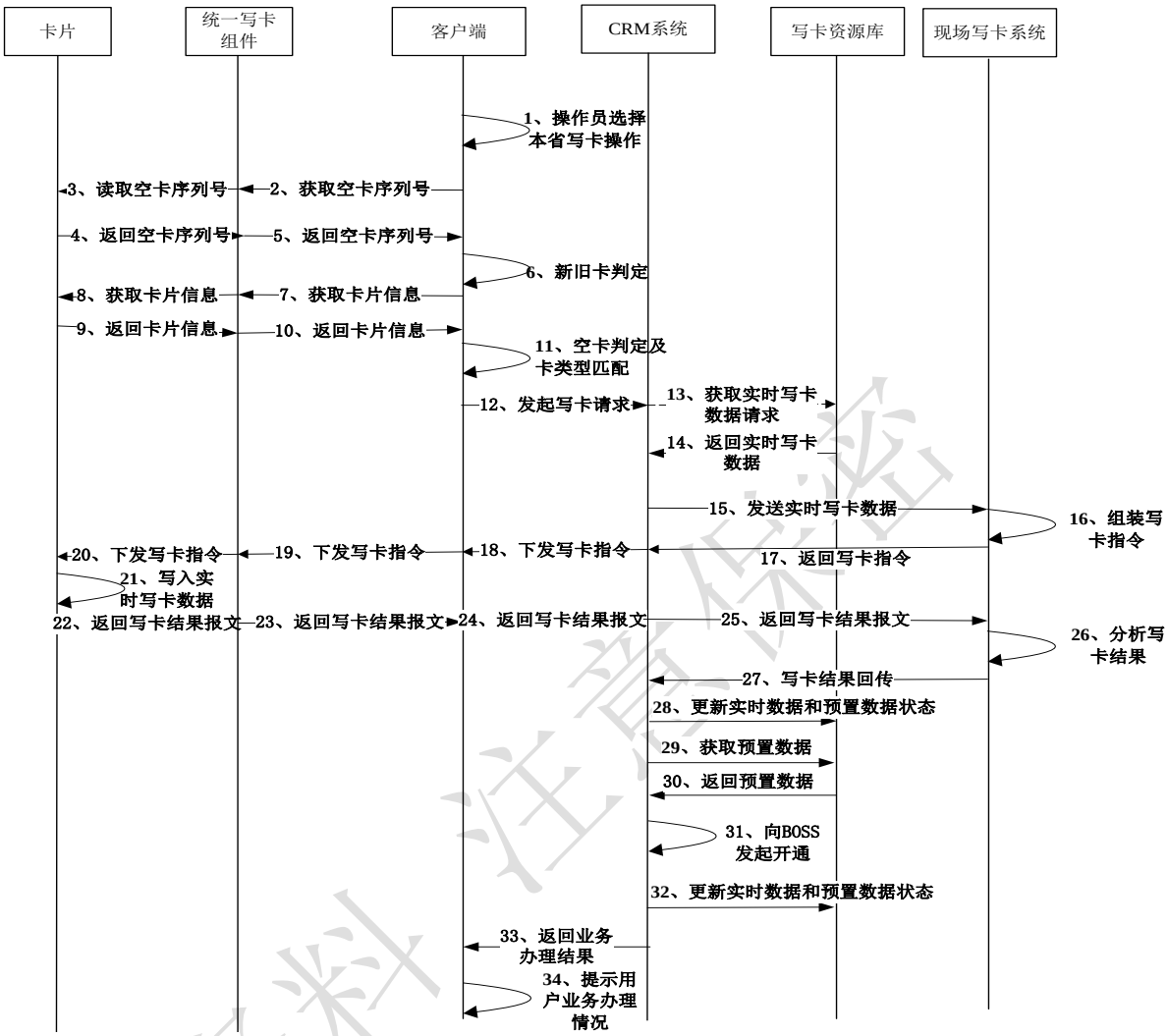


图 7-4　本省写卡流程图

流程详细说明如下：

1. 操作人员通过客户端选择本省写卡操作，操作人员把空卡插入读卡器；
2. 客户端调用统一写卡组件获取卡片空卡序列号。
3. 统一写卡组件读取卡片的空卡序列号文件。
4. 卡片向统一写卡组件返回空卡序列号文件。
5. 统一写卡组件向客户端返回卡片的空卡序列号。
6. 客户端验证所插空卡的新旧版卡，如是旧版本空卡，则走原有远程写卡流程，如是新版本空卡（预置空卡），则继续后续流程。
7. 客户端调用统一写卡组件获取卡片信息（包括卡片空卡序列号，卡内 ICCID 文件内容等），具体参见统一写卡组件相关的函数定义。
8. 统一写卡组件向卡片下发卡片信息获取报文，获取卡片的基本信息（包括卡片空卡序列号，卡内 ICCID 文件内容等）。

9. 卡片向统一写卡组件返回卡片的基本信息（包括卡片空卡序列号，卡内 ICCID 文件内容等）。
10. 统一写卡组件向客户端返回卡片的基本信息(包括卡片空卡序列号,卡内 ICCID 文件内容等）。
11. 客户端通过卡片信息判断卡片是否为空卡，并获取卡片的类型信息（多号卡，单号卡，SIM、USIM 等）。如为非空卡，提示错误，流程终止。
12. 客户端调用 CRM 接口发起写卡请求。写卡请求中包括（卡片空卡序列号，卡内 ICCID 文件内容，手机号码，卡片的类型等）。
13. CRM 系统根据卡片信息及手机号码等从写卡资源库中获取匹配的实时写卡数据。如果未找到匹配资源，则直接返回错误。
14. 写卡资源库向 CRM 系统返回实时写卡数据，并更新实时写卡数据和对应的预置数据状态，具体要求参见 7.4 节。
15. CRM 系统调用接口向现场写卡系统发起获取写卡指令请求。
16. 现场写卡系统通过加密机加密实时写卡数据，并组装写卡指令。
17. 现场写卡系统将组装后的写卡指令返回 CRM 系统。
18. CRM 系统将写卡指令透传给客户端。
19. 客户端将写卡指令发送到统一写卡组件。
20. 统一写卡组件将写卡指令发送到卡片。
21. 卡片收到写卡指令后，解密写卡指令的数据，并校验 MAC，写入实时写卡数据。
22. 卡片向统一写卡组件返回写卡结果报文。
23. 统一写卡组件向客户端返回写卡结果报文。
24. 业务办理客户端将写卡结果报文返回 CRM 系统。
25. CRM 系统将写卡结果报文返回现场写卡系统。
26. 现场写卡系统对写卡结果报文进行验证，并分析写卡结果。
27. 现场写卡系统向 CRM 系统返回写卡成功或失败结果及原因。
28. CRM 系统根据写卡结果更新写卡资源库相应的实时写卡数据和预置数据的状态。
29. 如果写卡成功则 CRM 系统向写卡资源库获取预置数据。否则 CRM 系统直接跳到第 33 步返回业务办理失败。
30. 写卡资源库向 CRM 系统返回预置数据。
31. CRM 调用接口与 BOSS 系统的接口，完成开通。
32. CRM 系统根据开通结果更新写卡资源库相应的预置数据、实时写卡数据的状态。
33. CRM 系统将业务办理结果返回给客户端。
34. 客户端通知操作员业务办理结果。

注：对于一卡多号卡，如果是分步写入，每写入一个号码均要及时更新预置数据及实时写卡数据状态。

7.2.2 跨省写卡流程

跨省写卡主要完成跨省补换卡操作，在写卡之前需要对用户的号码及身份信息进行验证核对，具体验证核对要求根据集团或各省公司相关部门规定由 CRM 实施。

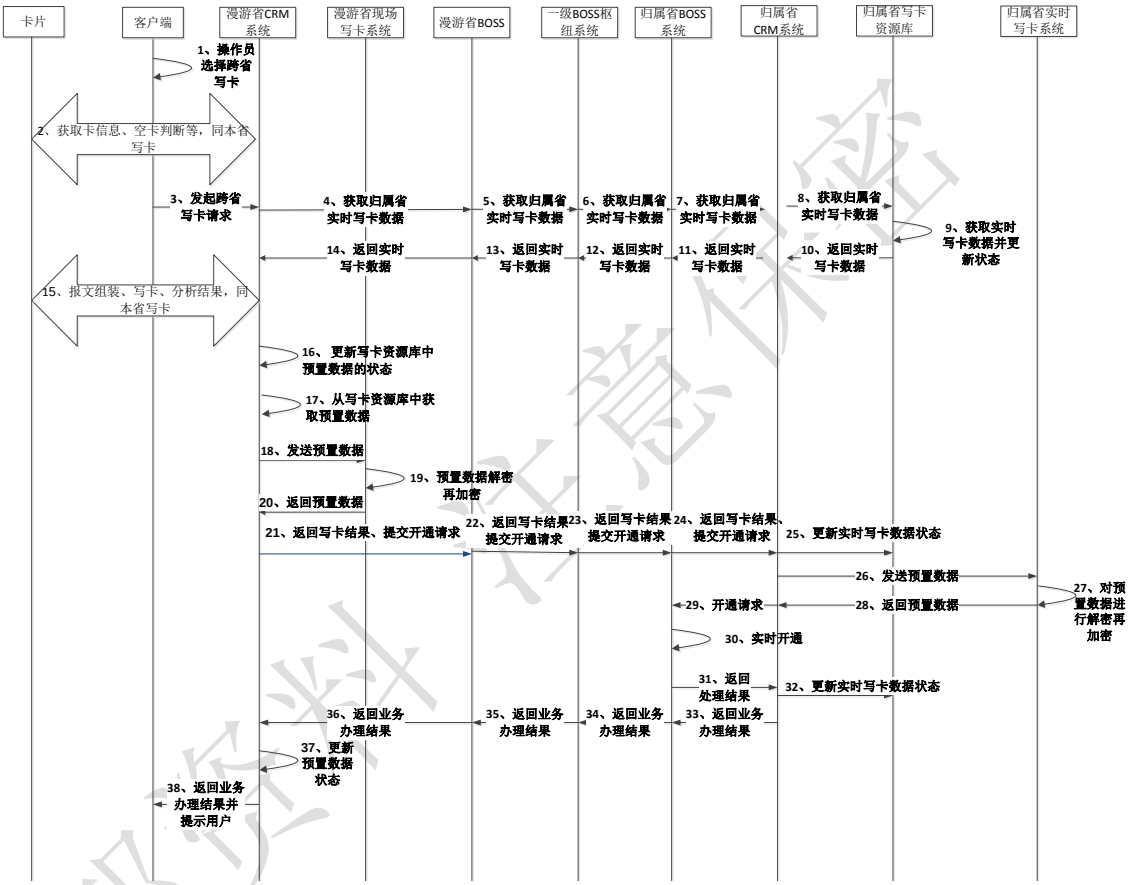


图 7-5　跨省写卡流程

流程详细说明如下：

1. 漫游省操作人员通过客户端选择跨省写卡操作，操作人员把空卡插入读卡器；
2. 漫游省客户端进行空卡判断识别、卡片信息获取等操作，同本省写卡第 2~11 步；
3. 漫游省客户端向漫游省 CRM 系统向起跨省写卡请求；
4. 漫游省 CRM 系统向漫游省 BOSS 系统发送申请归属省实时写卡数据请求；
5. 漫游省 BOSS 向一级 BOSS 枢纽发送申请归属省实时写卡数据请求；
6. 一级 BOSS 枢纽向归属省 BOSS 系统发送申请实时写卡数据请求；
7. 归属省 BOSS 系统向归属省 CRM 发送申请实时写卡数据请求；
8. 归属省 CRM 系统向归属省写卡资源库获取实时写卡数据。

9. 归属省写卡资源库根据客户手机号码的号段及卡信息等从写卡资源库中获取实时写卡数据并更新实时写卡数据状态，状态更新具体要求参见 7.4 节。
10. 归属省写卡资源库将实时写卡数据发送给归属省 CRM 系统；
11. 归属省 CRM 系统将实时写卡数据发送给归属省 BOSS 系统。
12. 归属省 BOSS 系统将实时写卡数据发给一级 BOSS 枢纽。
13. 一级 BOSS 枢纽将实时写卡数据发给漫游省 BOSS 系统；
14. 漫游省 BOSS 系统将实时写卡数据发给漫游省 CRM 系统。
15. 漫游省 CRM 系统获取实时写卡数据后，完成报文组装、写卡、结果校验等流程，同本省写卡。
16. 漫游省 CRM 系统更新漫游省写卡资源库中预置数据的状态。
17. 漫游省 CRM 系统从漫游省写卡资源库中获取预置数据。
18. 漫游省 CRM 系统将预置数据传给漫游省现场写卡系统。
19. 漫游省现场写卡系统调用加密机将预置数据利用漫游省的预置数据加密密钥（KEK）和归属省的跨省传输密钥（K2pub）进行转加密。
20. 漫游省现场写卡系统将加密后的预置数据返回给漫游省 CRM 系统。
21. 漫游省 CRM 系统将写卡结果及开通请求（包括预置数据）发送给漫游省 BOSS。
22. 漫游省 BOSS 通过一级 BOSS 枢纽转发写卡结果及开通请求（包括预置数据）。
23. 一级 BOSS 枢纽向归属省 BOSS 发送写卡结果及开通请求（包括预置数据）。
24. 归属省 BOSS 转发写卡结果及开通请求（包括预置数据）至归属省 CRM 系统。
25. 归属省 CRM 发送更新实时写卡数据状态请求到写卡资源库。
26. 归属省 CRM 将预置数据传给现场写卡系统进行转加密。
27. 归属省现场写卡系统接收到加密数据后，利用内置的归属省跨省传输密钥（K2pri）和归属省的预置数据加密密钥（KEK）对预置数据进行转加密。
28. 归属省现场写卡系统将加密后的预置数据返回给归属省 CRM 系统。
29. 归属省 CRM 向归属省 BOSS 系统发起开通操作。
30. 归属省 BOSS 系统进行开通。
31. 归属省 BOSS 系统将开通结果返回给归属省 CRM 系统。
32. 归属省 CRM 系统根据开通结果向归属省写卡资源库发起更新实时写卡数据状态请求。
33. 归属省 CRM 系统将开通结果返回给归属省 BOSS 系统。
34. 归属省 BOSS 将开通结果返回到一级 BOSS 枢纽。
35. 一级 BOSS 枢纽将开通结果转发到漫游省 BOSS。
36. 漫游省 BOSS 将开通结果转发到漫游省 CRM。

37. 漫游省 CRM 通知漫游省写卡资源库更新预置数据状态。

38. 漫游省 CRM 通知客户端业务办理结果并提示用户。

7.3 空卡标识及统一写卡组件管理

空卡标识和统一写卡组件必须首先在现场写卡系统中注册，然后才能投入使用。

7.3.1 空卡标识注册

空卡标识信息，如供应商等，应首先注册，然后才能投入使用。

如果采用空卡标识文件对空卡进行识别，则需在现场写卡系统中登记空卡的类别代码 L1L2。本标准颁布后的卡还需要登记卡类型标识字 T1T2T3T4。

如果采用 ATR 对空卡进行识别，则需在现场写卡系统中登记空卡的 ATR，同时记录其对应的类别代码 L1L2。

注：自本标准颁布之日起，所有新发行的 SIM 卡和 USIM 卡均应采用空卡序列号来标识卡的类别。

7.3.2 统一写卡组件管理

统一写卡组件管理包括统一写卡组件在现场写卡系统中的注册并上传 CRM 系统和写卡时自动下载到客户端两个步骤。

注册并上传流程如下：

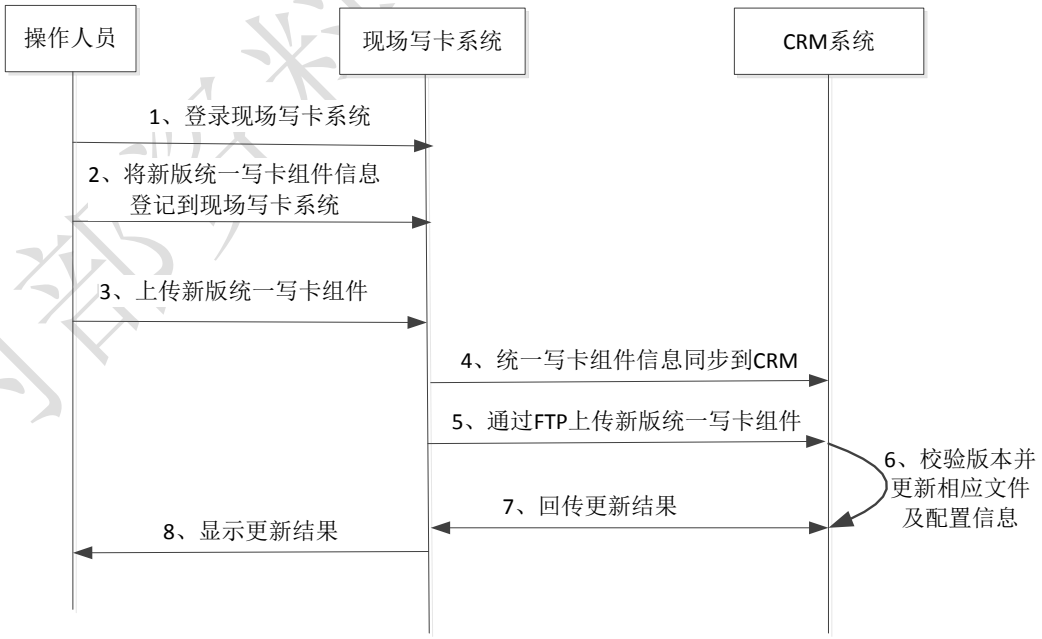


图 7-6 统一写卡组件上传流程图

流程说明：

1. 管理员登录现场写卡系统；

2. 管理员将新版统一写卡组件信息录入到现场写卡系统。

3. 管理员上传最新版统一写卡组件。确定上传后由现场写卡系统进行必要的版本号等校验。

4. 统一写卡组件成功上传现场写卡系统后，管理员通过现场写卡系统界面将同步新版统一写卡组件请求提交至 CRM 系统。

5. 现场写卡系统通过 ftp 方式上传组件文件。为了方便 CRM 系统进行版本校验，上传的组件名称增加版本号，版本号信息共三位，以数字表示，例：OPSClient1.0.2.dll。

6. CRM 系统收到组件文件,进行版本校验后,删除组件文件名中的版本信息并进行保存，例：OPSClient.dll，并更新相应的配置信息。

7. CRM 系统向现场写卡系统回传更新结果。

8. 现场写卡系统向管理员显示更新结果。

自动下载流程如下：

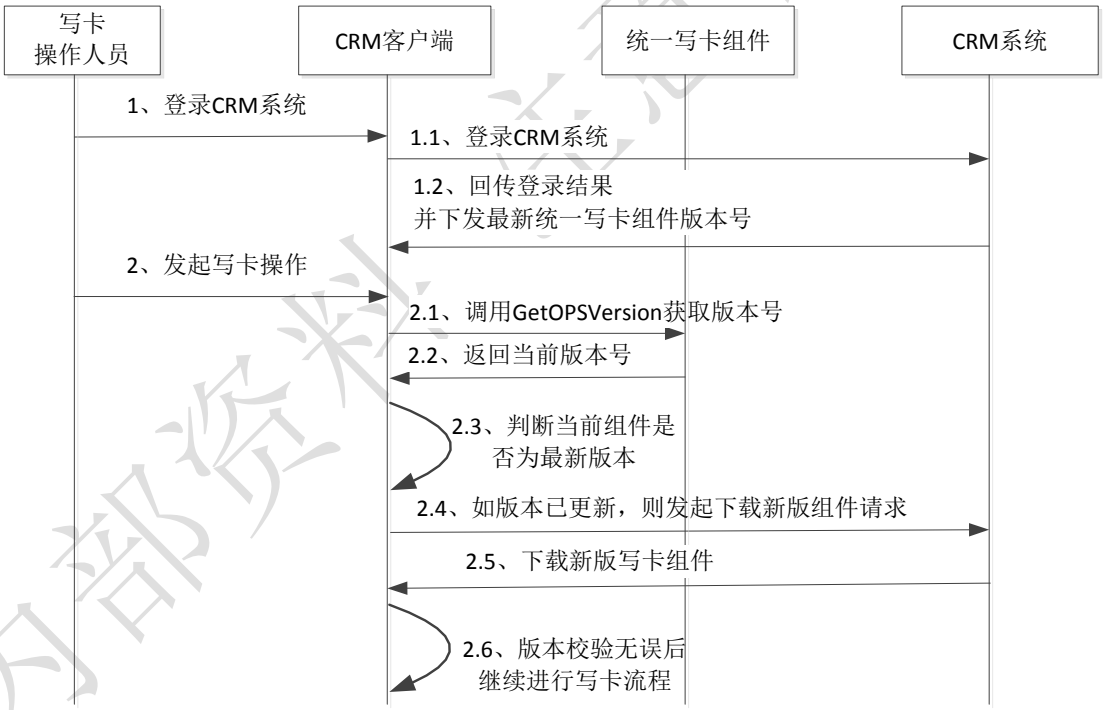


图 7-7　统一写卡组件自动下载流程图

流程说明：

1. 写卡操作员登录 CRM 系统；CRM 系统返回 CRM 客户端登陆结果并下发最新统一写卡组件版本号。

2. 写卡操作员通过 CRM 客户端发起写卡操作，CRM 客户端调用统一写卡组件 GetOPSVersion 获取当前组件版本号。

3. CRM 客户端根据 CRM 系统下发的版本号和从组件获取的版本号判断是否需要更新统一写卡组件，如需更新则从 CRM 系统服务器下载组件文件。

4. 版本校验无误后，CRM 客户端继续调用统一写卡组件其他接口完成写卡流程。

7.4 个人化数据的状态迁移

在现场写卡过程中，写卡资源库中的每套实时写卡数据、预置数据可以有如下状态。

表 7-1 数据状态说明

状态值	状态说明
0	未使用：个人化数据可被现场写卡业务使用；未启动写卡及开通操作。
1	中间态：个人化数据已被使用，正在实施写卡操作。
2	已使用：个人化数据已被成功完成写卡，正在实施开通操作。
3	已开通：个人化数据已被成功完成写卡，并已经成功开通。
4	回收状态.
-1	写卡失败，个人化数据已被使用。
-2	开通失败，个人化数据已被使用。

状态迁移图如下：

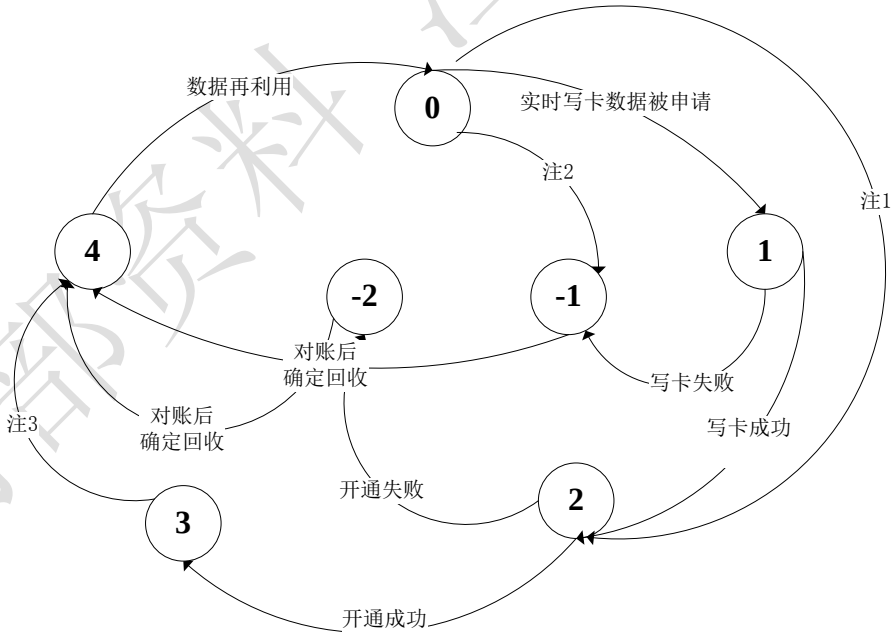


图 7-8 个人化数据状态迁移图

注 1：0->2,跨省写卡中，当归属省实时写卡数据写卡成功后，漫游省预置数据状态可由 0 直接更新为 2，参考跨省写卡流程；

注 2：0->-1,跨省写卡中，当归属省实时写卡数据写卡失败后，漫游省预置数据状态可由 0 直接更新为-1，参考跨省写卡流程；

注 3：3->4,当对账过程中，发现状态为 3 的数据并未正常开通，则将状态迁移至 4。参见对账章节。

说明：

1. 写卡资源库在数据被申请阶段应自动完成数据状态更新：

   a) 本省写卡中，实时写卡数据被申请时，写卡资源库自动将实时写卡数据及预置数据状态由 0 更新为 1。

   b) 跨省写卡中，归属省实时写卡数据被申请时，归属省写卡资源库自动将实时写卡数据状态由 0 更新为 1。

2. 写卡过程的不同阶段需根据 CRM 系统的返回结果，应实时更新写卡资源库中预置数据和实时写卡数据的状态：

   a) 本省写卡中，写卡过程不同阶段应实时且同步更新写卡资源库中预置数据和实时写卡数据的状态，例如，当某条实时写卡数据写卡成功/失败，状态由 1 至 2/-1，则所写卡片的预置数据状态也同步由 1 至 2/-1。

   b) 跨省写卡中，分别实时更新预置数据及实时写卡数据状态，参考漫游省写卡流程。例如归属省实时写卡数据写卡成功/失败后，归属省写卡资源库应及时更新实时写卡数据状态由 1 更新为 2/-1,将漫游省预置数据状态由 0 更新为 2/-1。

3. 对于实时写卡数据：

   1) 如果状态为-1、-2，在进行与 BOSS 对账后，确定未开通状态，则更新为状态 4，需定期删除此实时写卡数据，并对 IMSI 资源进行回收重利用。

   2) 在进行与 BOSS 对账后，状态为 3 的数据，则需定期删除。

4. 对于预置数据：

   1) 在进行与 BOSS 对账后，状态不为 0，则需定期删除，确保不会被再次使用。

7.5 实时开通

实时开通包括两部份工作，一部份是指 BOSS 系统实时地将鉴权数据（IMSI，KI/（K，OPC））导入到 HLR 并激活的过程。另一部份是指 CRM 系统或 BOSS 系统建立客户档案并建立客户号码及卡基本信息关系。

成功完成现场写卡后，现场写卡系统自动应将 IMSI、Ki（对于 SIM 卡）或 IMSI、OPC、K（对于 USIM 卡）等鉴权数据导入省 CRM，由省 CRM 发起将鉴权数据传给 BOSS 系统，由 BOSS 系统导入 HLR/AUC，实施开通。

7.6 对帐（数据同步）

写卡资源库的个人化数据应与省 BOSS 保持同步，即两个系统应定期进行对帐操作，并以 BOSS 侧个人化数据的状态为同步基准。

对帐逻辑如下：

1. 若 BOSS 中某套实时写卡数据及预置数据已成功开通，而写卡资源库中状态不

为 3，则认为写卡成功且开通成功，写卡资源库应将其迁移至状态 3。

2. 若 BOSS 中某套实时写卡数据及预置数据尚未成功开通，而写卡资源库中状态 -1 或-2 或 3，则认为写卡失败或开通失败，写卡资源库应将状态移至状态 4。

建议对帐周期不超过 24 小时。

7.7 一卡多号卡写卡

一卡多号卡是指在一张 SIM 或 USIM 卡上存储 2 个或 2 个以上电话号码对应的个人化数据，并可以通过卡菜单切换激活号码。

现场写卡业务应支持一卡多号写卡能力，即在一张 SIM 卡或 USIM 卡上写入两个或多个码号对应的个人化数据。

现场写卡业务的一卡多号功能应满足：

1. 允许主号码及各个副号码分属省内不同的归属地。
2. 允许一次性写入全部号码，也允许对于每个号码分别依次写入，但应首先写入主号码。卡内已写入数据的区域不允许重新写入。一次传入的实时写卡数据的数量不应多于卡内未写卡的区域数量。否则卡片报错。
3. 需要一个空卡序列号对应两个或多个 Ki。在制卡数据中需要定义出哪个 KI 用于主号，哪个 KI 用于副号码（具体由各省的卡数据管理系统定义）。在写卡时最早写入的为主号码，最后写入的为副号码。卡片可以根据写入的顺序或 TAG 的顺序，确定预置 Ki 和写卡数据的对应关系。
4. CRM 客户端需根据卡片返回信息对一卡多号卡所能支持的最大写入号码数量和当前已写入号码的数量进行判断，以便写卡时判断可写入号码数量。具体参见 8.3.3.1 节的表 8-9。如果是分步写卡，则每次写入号码前，CRM 均需获取卡片信息并进行判断。

7.8 查询统计

各省根据本省业务运营管理需求确定查询统计功能的具体要求，应包括不限于以下基本功能：

1. 支持对写卡日志进行记录的功能；
2. 支持对写卡次数、成功次数、失败次数、写卡业务类型等基本项进行查询统计功能；
3. 支持统计报表的个性化定制，可根据各省实际需要生成个性化报表；
4. 提供报表访问和展示界面；

查询统计功能还可包括对地区、县市、营业厅/代办点操作员、厂商、卡类型等信息的查询统计。

8　关键技术要求

8.1　空卡序列号

对于可用于现场写卡业务的 SIM 卡或 USIM 卡，应在空卡中预置空卡序列号，记录该卡的归属省、供应商、类别等信息。

制空卡时应预置空卡序列号，将作为空卡的唯一标识，且不可更改。

SIM 卡空卡序列号内容（空卡序列号）由 SIM 个人化数据生成系统负责管理和生成。

USIM 卡空卡序列号内容（空卡序列号）由一级卡数据管理系统负责管理和生成。

8.1.1　文件定义

该文件位于主文件路径（3F00）下。

表 8-1　空卡序列号

<table>
<tr><td colspan="2">文件标识符　　’2F02’</td><td colspan="2">透明文件</td><td>必选</td></tr>
<tr><td colspan="3">文件容量 10 个字节</td><td colspan="2">更新频率　低</td></tr>
<tr><td colspan="5">访问条件：
READ　　ALW
UPDATE　　NEVER
INVALIDATE　　ADM
REHABILITATE　　ADM</td></tr>
<tr><td>字节</td><td>描述</td><td>M/O</td><td colspan="2">长度</td></tr>
<tr><td>1</td><td>P1P2,省代码</td><td>M</td><td colspan="2">1</td></tr>
<tr><td>2</td><td>Y1Y2,制卡年号</td><td>M</td><td colspan="2">1</td></tr>
<tr><td>3</td><td>M1M2,保留</td><td>M</td><td colspan="2">1</td></tr>
<tr><td>4</td><td>L1L2,卡类代码</td><td>M</td><td colspan="2">1</td></tr>
<tr><td>5-6</td><td>T1T2T3T4
卡类型标识字</td><td>M/O (注 1)</td><td colspan="2">2</td></tr>
<tr><td>7－10</td><td>C X1-X7,
卡商 空卡序列号</td><td>M</td><td colspan="2">4</td></tr>
</table>

注 1：对于本标准发布前发行的 SIM 卡，该字段为可选。对于本标准颁布后新发行的所有 SIM 卡、USIM 卡，该字段为必选

8.1.2　编码格式

文件格式：P1P2Y1Y2M1M2L1L2T1T2T3T4CX1X2X3X4X5X6X7。

P1P2 为省代码，参见附录 C。BCD 编码（00-99）。

如 P1P2=13 时，该字节格式为：

表 8-2　P1P2 举例

0	0	0	1	0	0	1	1

bit 0　　bit 7

其中 bit 7 靠近后续字节（即 Y1Y2）。下同。

Y1Y2 为生产时间的年号（后两位）。BCD 编码，00-99。

M1M2 为保留字，01-29 为集团公司保留，30-69 由省公司自行使用，70-99 由 SIM 卡供应商自行使用，未使用时为 00。BCD 编码，00-99。

L1L2 为类别代码，各省公司自行定义业务卡类别代码，00 保留。ASCII 码，0x00 - 0xFF。

T1T2T3T4 为卡类型标识字，ASCII 码，0x0000 - 0xFFFF。

T1-T4 字节编码：

表 8-3　T1T2 字段编码

T1T2	bit0	bit1	bit2	bit3	Bit4	Bit5	bit6	bit7

表 8-4　T3T4 字段编码

T3T4	bit8	bit9	bit10	bit11	bit12	bit13	bit14	bit15

bit0：扩展标识。0—T3T4 后无扩展更多标识字节；1——标识位 bit1-bit15 已经全部使用，T3T4 后已扩展其他标识字段。目前 bit0=0。

表8-5　bit1字段取值

bit1	说明
0	预置空卡
1	非预置空卡

表8-6　bit2字段取值

bit2	说明
0	单号卡
1	一卡多号卡

表8-7　bit3bit4字段取值

bit3bit4	说明
00	SIM 卡
01	USIM 卡
其他	保留

bit5: SWP 卡，　1 为 SWP 卡，0 为非 SWP 卡

bit6 ：M2M 卡， 1 为 M2M 卡，0 为非 M2M 卡

bit7-bit15：保留，均置 0。

C 为 SIM 卡供应商的代码，参见附录 A。ASCII 码，0x0 - 0xF。

X1-X7 为空卡序列号，BCD 编码，0000000－9999999。各省公司自行管理。

8.1.3 空卡标识唯一性

空卡序列号的内容，也就是空卡标识应具有全局唯一性。各省公司应建立其与 ICCID 的一一对应关系。

对于一卡多号卡，空卡标识只与主号码的 ICCID 对应。

为便于客户服务和运营管理，推荐将空卡标识（全部或部分内容）打印在 Plug-in 小卡上。由省公司最终决策。

8.2 获取空卡识别信息

在实施现场写卡之前，需首先获得该卡的类型、供应商等空卡识别信息。本标准颁布后，所有 SIM 卡和 USIM 卡均应从空卡序列号中获取空卡识别信息。

8.2.1 空卡判断

在进行现场写卡业务前须判断当前插入卡片是否为空卡、是否为多号卡，以确定是否还可以写入新号码。

对于单号卡，现场写卡统一写卡组件读取待写卡 ICCID，如果是“FFFFFFFFFFFFFFFFFFFF”或“00000000000000000000”，则认为该卡是空卡。否则，则认为该卡不是空卡。

对于“一卡多号”卡，以主号码 ICCID 是否为空卡 ICCID 作为判定该卡是否为空卡的依据，如主号码 ICCID 为空则认为是该卡是空卡。是否可以继续写入号码则须判断主号码及各副号码当前状态，具体规则请参见第 7.7 节“一卡多号卡写卡”。

8.3 统一写卡组件

8.3.1 功能

现场写卡系统统一写卡组件集成在系统客户端中，由 CRM 系统提供用户界面，调用统一写卡组件接口完成相应的功能。

本标准发布起，启用统一写卡组件，由卡商维护的原私有组件将不再增加及升级，仅用于各省公司库存旧版空卡的现场写卡。

1. 读取卡片信息

现场写卡系统进行现场写卡业务前须获取卡片信息，如空卡序列号、卡片 ICCID 值等，统一写卡组件提供接口供 CRM 获取卡片信息。

2. 实时写卡数据写入

CRM 从现场写卡系统获取写卡报文后，通过调用统一写卡组件的接口完成实时写卡数据的写入。

8.3.2 命名方式

本标准要求现场写卡业务支持不同的写卡终端，统一写卡组件根据不同的写卡终端有不同的实现版本。

各实现版本统一写卡组件文件名为 OPSClient.XXX，其中 XXX 根据不同操作系统确定，如 Windows 系统为 dll，Linux 平台为 so 等。Android 平台统一写卡组件命名方式为 libOPSClient.so。

8.3.3 下行报文格式

8.3.3.1 获取卡片信息

由统一写卡组件组装获取卡片信息的报文。

统一写卡组件首先模拟手机开机过程中的 STK/USAT 启动流程，发送 TerminalProfile 指令，通过 0 次或多次 Fetch 指令完成与卡片的主动式命令交互，直到卡片没有 STK/USAT 主动式命令返回，具体流程参见 GSM11.14，然后发送获取卡片信息的报文。

下行报文和返回数据均不使用加密和校验。

1. 报文格式

表 8-8 下行报文格式

标识		长度(字节)	值	说明
TPDU_Header		可变	短消息头	TP-UDHI 为 1
UDL		1		后续数据长度
安全应用数据	UDHL	1	0x02	信息标识长度
	IEIb	1	0x70	安全头标识
	IEIDLb	1	0x00	信息长度
	CPL	2		后续数据长度,从 CHL 到最后
	CHL	1	0x0D	安全报文头长度，从 SPI 到 PCNTR
	SPI	2	0x00 0x00	无加密，无校验，无计数器
	KIc	1	0x00	不使用加密
	KID	1	0x00	不使用校验
	TAR	3	B000F1	获取卡片信息

	CNTR	5	0X00 00 00 00 00	RFU
	PCNTR	1	0x00	RFU
命令数据	命令类型	1	HEX	0x0A，获取卡片信息
	命令长度	1	HEX	0x00,无后续命令长度

2. 卡片处理流程

卡片在得到该条下行报文后，读取空卡序列号、ICCID 值，并响应 91xx，以显示文本（DisplayText）的命令，在文本内容字段（TextString）内返回卡片空卡序列号、卡片 ICCID 值，该指令流程结束；

Displaytext 的 DCS 字段编码格式使用 0x04。

数据项缺失视为获取卡片信息命令失败。

3. 返回数据格式

TLV(tag-length-value)，length 为 HEX（1 字节长度），具体的返回数据的格式，参见 GSM 11.11 相关文件及本标准 8.1 节空卡序列号说明。

表 8-9 返回数据格式

数据项	tag	类型	Mandatory/ Optional	数据长度（字节）	举例和说明
ICCID	08	HEX	M	10	080A98680021436587092143 注：为兼容一卡多号卡，本 Tag 可出现多次，第一个为主号码 ICCID,第二个为副号码 ICCID,依次类推。此处 ICCID 为卡片文件存储格式。
CardSN	0E	HEX	M	10	0E0A01120101012345670000

8.3.3.2 写卡

写卡的下行报文由现场写卡系统进行组装。

统一写卡组件首先模拟手机开机过程中的 STK/USAT 启动流程，发送 TerminalProfile 指令，通过 0 次或多次 Fetch 指令完成与卡片的主动式命令交互，直到卡片没有 STK/USAT 主动式命令返回，具体流程参见 GSM11.14，然后将下行写卡报文发送至卡片。

下行报文使用加密和校验，返回数据使用校验。

1. 报文格式

下行报文说明如下，其中加密内容为 CNTR,PCNTR,CC（MAC）,命令数据及填充字节。

表 8-10 第一条下行报文

标识	长度（字节）	值	说明

TPDU_Header		可变	短消息头	TP-UDHI 为 1
UDL		1		后续数据长度
安全应用数据	UDHL	1	0x07	信息标识长度
	IEIa	1	0x00	级联标识
	IEIDLa	1	0x03	级联信息长度
	IEDa	3	0xXX XX 01	批次、短信总数、短信索引
	IEIb	1	0x70	安全头标识
	IEIDLb	1	0x00	信息长度
	CPL	2		后续数据长度,从 CHL 到最后
	CHL	1	0x11	安全报文头长度，从 SPI 到 CC
	SPI	2	0x06 0x00	只使用第一字节 bit1,bit2,bit3。
	KIc	1	0x05	3DES CBC
	KID	1	0x05	3DES CBC
	TAR	3	0xB000F2	写卡
	CNTR	5	0x00 00 00 00 00	计数器固定值,卡片不对计数器进行合法性判断
	PCNTR	1	0xXX	参见 GSM03.48
	CC	4		使用 MAC，参见 12.2.3
命令数据	Secured Data	X	XX	参见“命令数据格式”定义和注 1

如指令需多条短信，第二条及以后各条下行报文格式如下，其中加密内容为命令数据。

表 8-11　第二条及以后各条下行报文格式

标识		长度（字节）	值	说明
TPDU_Header		可变	短消息头	TP-UDHI 为 1
UDL		1		后续数据长度
安全应用数	UDHL	1	0x05	信息标识长度

据	IEIa	1	0x00	级联标识
	IEIDLa	1	0x03	级联信息长度
	IEDa	3	0xXX XX 02	批次、短信总数、短信索引
命令数据	Secured Data	X	XX	参见“命令数据格式”定义和注 1

表 8-12 命令数据格式

标识		长度（字节）	值	说明
命令数据	命令类型	1	0x XX	0x0B：写卡
	随机数	8	Hex	用于卡片返回写卡结果时计算 MAC 使用
	写卡后续数据长度	1	0x XX	0－255 后续写卡数据长度
	写卡后续数据	X	参见 8-13	参见注 1

注 1：

1) CNTR 固定为全 0x0000000000（RFU），下行报文计数器不变化。

2) 写卡报文最长 3 条 Envelope。

3) 写卡数据中对于 PIN1、PIN2、PUK1、PUK2 数据项，只更新其值，不对卡内 PIN 及 PUK 的状态、剩余次数做改变，缺省状态下，PIN1 为 Disable/3 次剩余。卡内 PIN、PUK 出厂状态及剩余验证次数设置请参照全个人化卡片。

4) EF ACC(6F78)文件根据传入的 IMSI 进行更新，具体要求参见《应急通信用户优先接入技术要求》V1.0.0。

5) 写卡数据格式：TLV(tag-length-value)，length 为 HEX（1 字节长度），具体的更新数据的格式，参见 GSM 11.11 相关文件。卡片执行该指令时，需按字段分别依次写入。

表 8-13 写卡数据 TLV 格式

数据项	tag	类型	Mandatory/Optional	数据长度（字节）	例子
ICCID	01	HEX	M	10	010A98680021436587092143 注：此处 ICCID 为卡片文件存储格式。
IMSI	02	HEX	M	9	0209084906001111212299

					注：此处 IMSI 为卡片文件存储格式。
SMSP	03	HEX	M	8	030891683108706505F0
PIN1	04	HEX	M	8	040831323334FFFFFFFF
PIN2	05	HEX	M	8	050835363738FFFFFFFF
PUK1	06	HEX	M	8	06083735383336333633
PUK2	07	HEX	M	8	07083735383336333633

上表中报文数据均为明文，实际下发卡片的报文用预置卡密钥进行加密。

注:

一卡多号如果采用一次写入方式：写卡数据项有多套，默认以第一套写卡数据为主号，第二套及以后写卡数据为辅号。TAG 按成对顺序出现，如<ICCID1><IMSI1>…<ICCID2><IMSI2>…

一卡多号如果采用多次写入方式：默认第一个写入的数据为主号，第二个写入的数据为辅号。

卡片应能根据卡内文件的内容，判断是否已写入相应的主号和辅号。为了保证写卡的完整性，在多号卡写卡过程，无论是主号或是辅号写卡出现失败时都按写卡错误处理。具体的出错代码按具体的写入数据来定（参见表 8-14 的返回数据格式）。

2. 卡片处理流程

卡片在得到该条下行报文并执行结束后，响应 91xx，以显示文本（DisplayText）的命令，在文本内容字段（TextString）内返回 1 字节的结果代码加 MAC 值，该指令流程结束。Displaytext 的 DCS 字段使用 0x04。

如果 MAC 认证错，卡片直接返回 9000。统一写卡组件将 9000 直接返回给服务器。

3. 返回数据格式

表 8-14　返回数据格式

	结果代码	含义
写卡结果	0x30	写卡成功
	0x31	写卡指令接收不完整
	0x32	写卡指令中的 3DES 解密错误
	0x33	出现不支持的 Tag 值
	0x4X（1<=X<=D）	Tag=0x0X 的写卡数据校验失败 例如： 0x41：代表 ICCID 校验失败（Tag 01-0C 的写卡数据只校验长度）

		…. .
	0x5X(1<=X<=D)	Tag=0x0X 的写卡数据写入时发生错误 例如： 0x51：代表 ICCID 写入时发生错误
	其他	保留
MAC	写卡结果代码 MAC 值，参见 12.2.3 节，其中原始数据此处包含写卡结果和下行写卡报文中的随机数字段。	

8.4 预置空卡要求

预置空卡的要求如下：

1. 所有 SIM/USIM 卡须按 8.1 节规定预置空卡序列号。
2. SIM/USIM 卡出厂时须写入预置数据，对于 SIM 卡，预置数据包括 Ki、伪 Ki、索引随机数，对于 USIM 卡，预置数据包括 K、OPc。
3. SIM/USIM 卡出厂时须写入预置卡密钥 K1，参见 12.1 节。
4. 写卡过程中，由现场写卡系统对个人化数据的长度和值做逻辑判断；卡片只需判断相应个人化数据的长度，无需判断写入的个人化数据的值。
5. 卡片收到下行报文后，读、写卡片实现流程要求如下图所示：

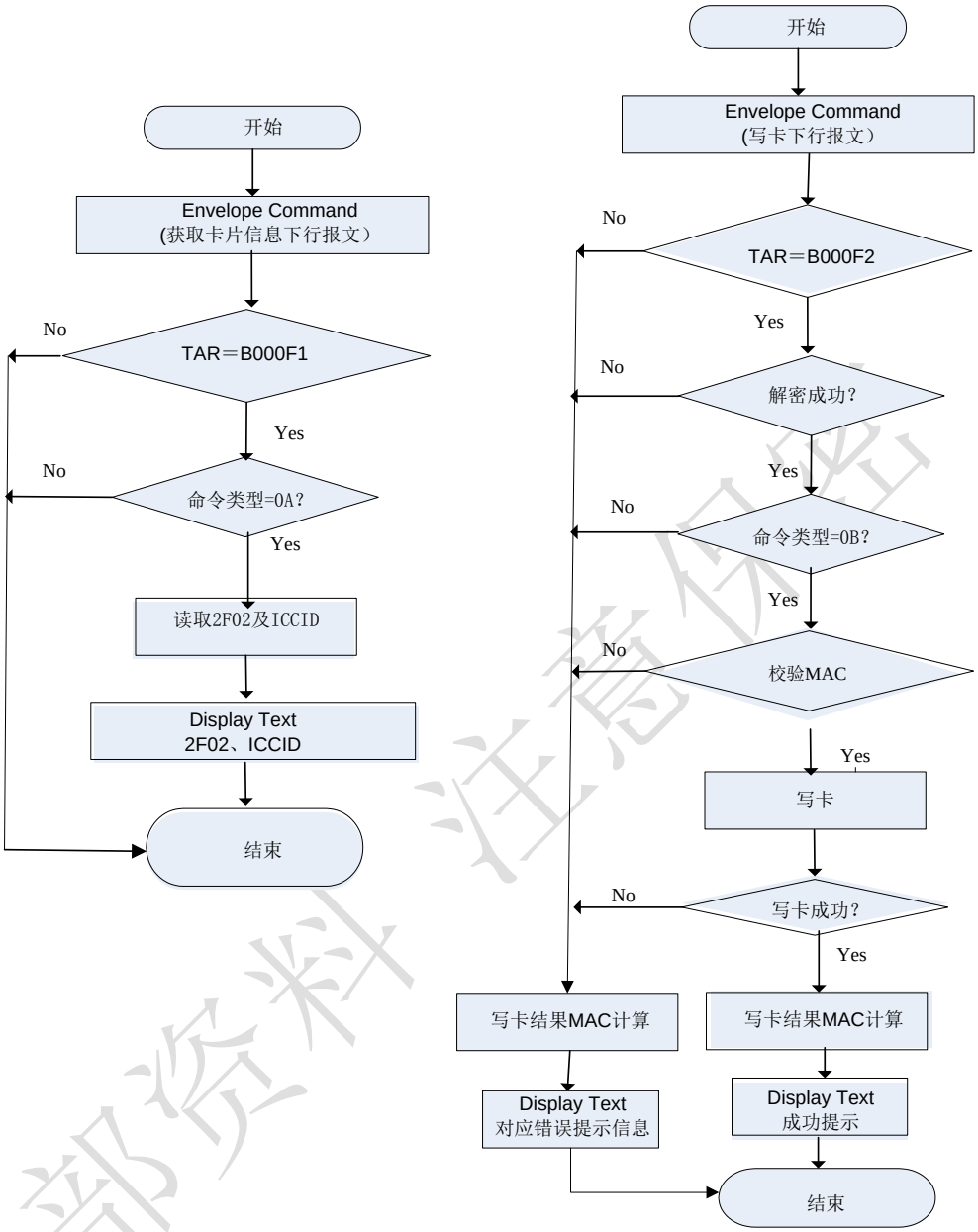


图 8-1　卡片处理流程图

6. 上下行报文数据加密及解密

为保证实时写卡数据的安全，在传输过程中需对数据进行加密，卡片收到下行写卡报文后须先进行解密，解密算法及密钥使用参见第 12 章安全性要求。

写卡结果返回须增加 MAC 值。

8.5 一卡多号卡

一卡多号卡写卡规则请参见第 7.7 节说明，卡片实际生效的 PIN1、PIN2、PUK1、PUK2 均为主号相对应的数据，写副号码时丢弃传入的相应数据项。

8.6 读卡器控制组件要求

8.6.1 读卡器控制组件调用方式

读卡器控制组件调用方式如下图所示：

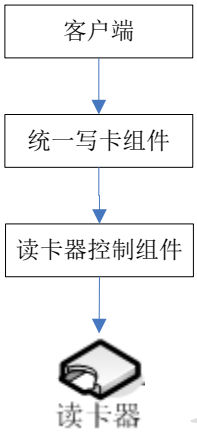


图8-2 读卡器控制组件调用图

8.6.2 读卡器控制组件命名规则

读卡器控制组件根据不同的操作系统平台有不同的实现版本。各实现版本读卡器控制组件命名为 OPSLibReader.XXX，其中 XXX 根据不同操作系统确定，如 Windows 系统为 dll，Linux 系统为 so，Android 系统的读卡器控制组件命名为 libOPSLibReader.so。

8.6.3 统一写卡组件与读卡器控制组件接口

接口包括五个函数，具体定义如下：

8.6.3.1 连接读卡器

int OpenCardReader([in] int ReaderType, [in] char * DeviceID, [in] char * Password);

功能说明：

通过该函数连接读卡器。

参数说明：

ReaderType:读卡器类型，其值为1：USB读卡器（CM-READER协议）；2：蓝牙读卡器；3：串口读卡器；4：内置读卡器（内置读卡器是指读卡器与电脑或读卡器与平板集成在一起，不论内部是何种连接方式，比如智能终端一体机）。

DeviceID:

- ReaderType 为 1 时取值如下：

  WINDOWS: PCSC读卡器名称

Linux: PCSC读卡器名称

Android:USB读卡器VID+PID的16进制字符串，如VID为23D8，PID为0185，则值为23D80185

- ReaderType 为 2 时为蓝牙读卡器 MAC 地址的 16 进制字符串,

  如读卡器MAC地址为11:22:33:44:55:66，则值为112233445566。

- ReaderType 为 3 时取值如下：

  WINDOWS: 串口名称，如COM1

  Linux: 终端主机自带的串口，如/dev/ttyS0

  USB卡(线)转换的串口，如/dev/ttyUSB0

  Android: 终端主机自带的串口，如/dev/ttyS0

  USB卡(线)转换的串口，如/dev/ttyUSB0

- ReaderType 为 4 时取值如下：可以设置为固定值，也可以不配置。

Password:使用蓝牙读卡器时，该参数为连接蓝牙读卡器的验证码，其他读卡器时此值默认为空。该字段为预留字段。

返回值说明：

0：函数执行成功；

非 0：函数执行失败；

8.6.3.2 卡片上电

int CardPowerOn([out] char * Atr);

功能说明：

通过该函数给卡片上电。

参数说明：

Atr:输出卡片的 ATR。

返回值说明：

0：函数执行成功；

非 0：函数执行失败；

8.6.3.3 发送 APDU 指令

int SendApduCommand ([in] int CmdInLength, [in] char * CommandIn, [out] int *CmdOutLength, [out] char *CommandOut);

功能说明：

通过该函数向卡片发送指令。

参数说明：

CmdInLength:输入的 APDU 指令的长度，以字节为单位。

CommandIn：输入的 APDU 指令，16 进制形式的字符串。

CmdOutLength:卡片返回的实际数据的长度，以字节为单位。

CommandOut: 卡片返回的实际数据，16 进制形式的字符串，数据格式：数据+2 字节的状态字。

如：读取 2FE2 文件

CmdInLength：5

CommandIn：A0B000000A

CmdOutLength：12

CommandOut： 986800000021436587099000

返回值说明：

0：函数执行成功；

非 0：函数执行失败；

8.6.3.4 卡片下电

int CardPowerOff ()

功能说明：

通过该函数给卡片下电。

返回值说明：

0：函数执行成功；

- 非 0：函数执行失败；

8.6.3.5 关闭读卡器

int CloseCardReader( );

功能说明：

通过该函数关闭读卡器。

返回值说明：

0：函数执行成功；

非 0：函数执行失败；

注：以上函数的错误代码表如下：

表 8-15　错误代码

错误代码	含义
0	执行成功
1001	未找到读卡器
1002	连接读卡器失败
1003	卡片上电失败
1004	APDU 指令发送失败
1005	卡片下电失败

8.6.4　读卡器通信协议要求

由于目前对于所有的操作系统没有统一的读写卡器标准，为了降低读写卡器的开发复杂度，对于目前不支持 PC/SC 协议的读写卡器，统一使用中国移动的现场写卡读卡器通信协议，简称 CM-READER 协议。

表 8-16　读卡器支持协议

读写卡器类型	操作系统	支持协议
蓝牙读卡器	Android/Windows/Linux	CM-READER 协议
USB 读卡器	Android	CM-READER 协议
USB 读卡器	Windows/Linux	PC/SC 协议
串口读卡器	Android/Windows/Linux	CM-READER 协议

读卡器控制组件和读卡器的通信协议（CM-READER 协议）如下：

1.下行报文

方向：从读卡器控制组件到读卡器，报文格式：包头+长度+命令类型+数据包+ BCC 校验

包头：4 字节，固定为 FFFF5555。

长度：2 字节，包括命令类型+数据包的总长度，数据传输采用大端模式。

命令类型：1 字节，见下表：

表 8-17　命令类型

命令类型	含义

30	连接读卡器
31	获取读卡器状态
32	卡片上电
33	发送 APDU 指令
34	卡片下电
35	断开读卡器连接

BCC 校验：对数据进行异或校验，长度+命令类型+数据包。

2.上行报文

方向：从读卡器到读卡器控制组件，报文格式：包头+长度+命令类型+数据包+ BCC 校验

包头：4 字节，固定为 FFFF6666。

长度：2 字节，包括命令类型+数据包的总长度，数据传输采用大端模式。

命令类型：1 字节，见下表：

表 8-18　命令类型

命令类型	含义
30	连接读卡器
31	获取读卡器状态
32	卡片上电
33	发送 APDU 指令
34	卡片下电
35	断开读卡器连接

BCC 校验：对数据进行异或校验，长度+命令类型+数据包

8.6.4.1 连接读卡器

表 8-19　下行报文

长度		命令类型	数据包
00	01	30	无

表 8-20　上行报文

长度	命令类型	数据包

00	02	30	Data

Data 定义：

00-读卡器准备就绪；

其他-失败。

8.6.4.2 获取读卡器状态

下行报文如下：

表 8-21　下行报文

长度		命令类型	数据包
00	02	31	Data0

Data0 定义:

01-获取卡槽状态

02-获取电池状态

03-FF:保留

1)　Data0 为 01 时，上行报文如下：

表 8-22　上行报文

长度		命令类型	数据包		
00	04	31	Data0	Data1	Data2

Data0：下行命令数据中的 Data0。

Data1:卡槽状态，1 字节，每一位（bit）表示卡槽状态，0 无此卡槽，1 有卡槽，详见下表。

表 8-23　Data1 说明

7	6	5	4	3	2	1	0	说明
							1	非接触
						1		卡槽 1
					1			卡槽 2
				1				卡槽 3
			1					卡槽 4

		1						卡槽 5
	1							卡槽 6
1								卡槽 7

Data2：卡状态，1 字节，每一位（bit）表示卡状态，0 无卡，1 有卡，详见下表。

表 8-24　Data2 说明

7	6	5	4	3	2	1	0	说明
							1	非接触卡
						1		卡 1
					1			卡 2
				1				卡 3
			1					卡 4
		1						卡 5
	1							卡 6
1								卡 7

2)　　Data0 为 02 时，上行报文如下：

表 8-25　上行报文格式

长度		命令类型	数据包	
00	03	31	Data0	Data1

Data0：下行命令数据中的 Data0。

Data1：

00：没有电池

01—09：电量值，01 表示电量低，09 表示电量满。

8.6.4.3 卡片上电

下行报文如下：

表 8-26　下行报文格式

长度		命令类型	数据包
00	02	32	Data

Data 定义：

00 非接触上电

01 卡槽 1 上电

02 卡槽 2 上电

……

07-卡槽 7 上电

上行报文如下：

表 8-27　上行报文格式

长度		命令类型	数据包
00	02+ATR 长度	32	Data0+ATR

Data0 定义：

- 00-卡片上电成功，成功时返回卡片 ATR

  其他-失败

8.6.4.4 发送 APDU 指令

下行报文如下：

表 8-28　下行报文格式

长度		命令类型	数据包	
00	02+APDU 长度	33	Data0	APDU

Data0：1 字节，表示卡槽号 。

APDU：APDU 指令。

上行报文如下：

表 8-29　上行报文格式

长度		命令类型	数据包	
00	02+RPDU 长度	33	Data0	RPDU

Data0：1 字节，表示卡槽号 。

RPDU:卡片返回的数据，最后 2 字节为 SW1，SW2。

8.6.4.5 卡片下电

下行报文如下：

表 8-30　下行报文格式

长度		命令类型	数据包
00	02	34	Data

Data 定义：

00 非接触下电

01 卡槽 1 下电

02 卡槽 2 下电

……

07-卡槽 7 下电

上行报文如下：

表 8-31　上行报文格式

长度		命令类型	数据包
00	02	34	Data

Data 定义：

00-卡片下电成功

其他-失败

8.6.4.6 断开读卡器连接

下行报文如下：

表 8-32　下行报文格式

长度		命令类型	数据包
00	01	35	无

上行报文如下：

表 8-33　上行报文格式

长度		命令类型	数据包
00	01	35	无

9 设备要求

9.1 现场写卡系统

现场写卡系统是现场写卡业务的主要设备，需配备加密机，提供密钥的安全存储功能，对写卡数据进行加解密，具体参见 12 章。主要负责：

1. 对实时写卡数据进行报文打包并控制数据写入。
2. 对写卡结果进行解析并验证。
3. 跨省写卡中对预置数据进行转加密。

该系统分省建设。

9.2 写卡资源库

现场写卡业务中管理数据资源的子系统或模块，数据资源包括（不限于）实时写卡数据、空卡序列号与预置数据的对应关系等。相应功能的实现各省公司可视情况在现场写卡系统中实现，也可在 CRM 系统中实现。

写卡资源库须保证数据的安全存储，实时对个人化数据进行状态迁移。对于预置数据，使用后应及时删除；对于实时写卡数据，根据使用及状态情况，可对 IMSI 资源进行删除或回收利用。

9.3 SIM 个人化数据生成系统

SIM 个人化数据生成系统负责批量生成 SIM 卡个人化数据，在一级卡数据生成系统建设投入使用前，可代为生成 USIM 卡个人化数据。生成的个人化数据包括实时写卡数据、预置数据、空卡序列号、预置卡密钥等。

1. 生成空卡序列号、预置数据、预置卡密钥组成的制卡文件，发送给卡商用于制卡，制卡文件中各数据项顺序为：空卡序列号、预置数据、预置卡密钥（SIM：2F02、Ki、K1；USIM：2F02、K、OPc、K1），其中预置数据和预置卡密钥应为加密数据。
2. 将预置数据经 KEK 加密，并与空卡序列号批量导入到写卡资源库，预置数据与空卡序列号成功导入到写卡资源库后，SIM 个人化数据生成系统应及时删除预置数据、空卡序列号、预置卡密钥。
3. 将实时写卡数据批量导入到写卡资源库，实时写卡数据成功导入到写卡资源库后 SIM 个人化数据生成系统应及时删除实时写卡数据。
4. 需要保证数据的一致性，发给厂家的制卡文件，待厂家确认接收成功后，再将加密的预置数据、空卡序列号导入写卡资源库，写卡资源库确认导入成功后，SIM 个人化数据生成系统再将相应数据删除；同样，待写卡资源库确认导入实时写卡数据成功后，SIM 个人化数据生成系统再将相应数据删除。

SIM个人化数据生成系统生成的Ki应符合“《中国移动防克隆SIM卡技术规范2.0.0》安全方案所要求的增强型 Ki。提供省公司密钥及 KEK 密钥的安全存储功能，具体参见 12 章。

该系统可以与省 BOSS 合设，也可以与现场写卡系统合设，分省建设。

9.4 一级卡数据生成系统

一级卡数据生成管理系统负责生成 USIM 卡个人化数据，并以安全的方式通过一级 BOSS 枢纽传递到省 BOSS，最后导入写卡资源库，处理方式同 SIM 个人化数据生成系统。

该系统集团统一规划建设，为 USIM 卡资源管理和生产提供有效的技术支撑。该系统正式建成投入使用前，USIM 卡数据生成方式参照现网 SIM 卡数据生成方案和流程，由发卡省自行生成 USIM 卡数据（如 K、OPc 等）并确保发卡数据的安全。

9.5 省 CRM

在现场写卡业务中，省 CRM 主要负责：

1. 写卡前客户资料的验证及号码查询等业务；
2. 与写卡资源库交互，获取实时写卡数据及预置数据；
3. 与现场写卡系统交互，将实时写卡数据进行加密组包及写卡结果解析；
4. 通过与 BOSS 交互实施号码开通；
5. 协助完成跨省写卡。

9.6 省 BOSS

在现场写卡业务中，省 BOSS 主要负责：

1. 管理用户通信账户及其个人用户资料；
2. 实施业务开通；
3. USIM 个人化数据申请时提供中转功能；
4. 跨省写卡业务中提供数据中转功能。

9.7 现场写卡终端/客户端

现场写卡终端通常为 PC 机、也可以是笔记本电脑、智能终端（例如 PAD）等，含客户端和统一写卡组件。需支持如下功能：

1. 操作员完成写卡前必要的 CRM 系统操作流程后，确认写卡后由 CRM 客户端调用现场写卡统一组件，驱动读卡器实现到 SIM 卡、USIM 卡等用户卡的数据读出/写入。
2. 现场写卡终端需支持 USB 读卡器、蓝牙读卡器或串口读卡器中的至少一种。
3. 客户端应配有设置读卡器的参数的功能，在蓝牙或串口读卡器第一次使用时，用户要先进行配置才能进行现场写卡操作。如果当前有系统中配置有多个蓝牙读卡器或串口读卡器，操作员必须配置一个当前有效的读卡器。读卡器参数配置信息保存在相应的配置文件中。
4. 客户端的合法性及安全性应由 CRM 系统进行确认。

9.8 预置空卡

预置空卡是现场写卡业务中待写入实时写卡数据的 SIM 或 USIM 卡，具体要求参见第 8.4 节预置空卡要求。

9.9 读卡器

读卡器的硬件要求如下：

1. 符合中华人民共和国国家标准—集成电路(IC)卡读写机通用规范(GB/T18239-2000）；符合 ISO/IEC7816 协议或符合 EMV 规范，Level 1；
2. 能够适应环境温度范围：-10～50oC；
3. 能够适应相对湿度范围：20%～90%；
4. 与电信智能卡通讯要求支持 PPS，通讯速率达到 400kbps 以上（支持 TA1 0x11/0x12/0x13/0x94/0x38/0x95/0x18/0x96 等）；
5. 支持符合 ISO/IEC7816 协议的 CPU 电信智能卡(T=0、T=1 协议),并能通过升级驱动方式保证在不换读卡器的情况下对未来通信协议的支持；
6. 支持 5V、3V 和 1.8V 智能卡；
7. 支持处理 8Pin 机制；
8. 防短路和过热保护；
9. 保证 10 万次电信智能卡的插拔次数；
10. 平均无故障时间（MTBF）大于 5000 小时 13）；
11. 符合 RoHS 标准；

9.9.1 蓝牙读卡器

9.9.1.1 命名规则

蓝牙读卡器命名规则如下：

CMRDXXY，共 7 个字符，由数字（0-9）和字母（A-Z）组成，其中：

- CMRD:读卡器前缀，固定写法，中国移动读卡器缩写。
- XX:读卡器厂商代码，该厂商代码由中国移动统一规划。
- Y:读卡器版本或型号，厂家自定义 。

9.9.1.2 蓝牙读卡器标识规则

蓝牙读卡器标识分为 2 部分，包括蓝牙读卡器名称和 MAC 地址后 6 位，该标识用于：

1. 蓝牙读卡器设备标签，需标注在读卡器设备表面。
2. 客户端界面显示，用于操作员对读卡器进行选择。

标识规则如下：

CMRDXXYZZZZZZ，共 13 个字符，由数字（0-9）和字母（A-Z）组成，其中：

- CMRD:读卡器前缀，固定写法，中国移动读卡器缩写。
- XX:读卡器厂商代码，该厂商代码由中国移动统一规划。
- Y:读卡器版本或型号，厂家自定义　。
- ZZZZZZ:蓝牙读卡器 MAC 地址后六位。

例：蓝牙读卡器名称为 CMRDEP0，MAC 地址为 11:22:33:44:55:66，则蓝牙读卡器标识为：CMRDEP0445566。

9.9.1.3 蓝牙验证码

为提高设备安全性，要求蓝牙读卡器与终端（PC 或移动设备）连接时，必须设置连接验证密码，该连接验证密码为 6 位数字，由蓝牙读卡器厂商在蓝牙读卡器出厂时提前设置，该密码在出厂后可以重新设置。

9.9.2　串口读卡器

用于现场写卡业务的串口读卡器统一要求波特率为 115200bps、停止位 1 位，数据位 8 位，采用偶校验。

9.9.3　USB 读卡器

无特殊要求。

9.10 现场写卡系统加密机

现场写卡系统加密机是经过国家密码主管部门（国密局）认证的专用硬件设备，用于 K1、KEK、K2 等各类密钥的管理操作（生成、更新、导入等），并向现场写卡系统提供基于各类密钥的密码运算服务（包括：加解密、MAC 计算、签名/验签等）。

现场写卡系统需要配备 2 台加密机（负载均衡模式），用于向现场写卡系统提供高可用、高吞吐量的密码运算服务。对现场写卡系统加密机的功能、技术指标等要求见附录-E，接口要求、接口调用流程见 10.5 节。

10　接口要求

10.1 接口结构图及接口说明

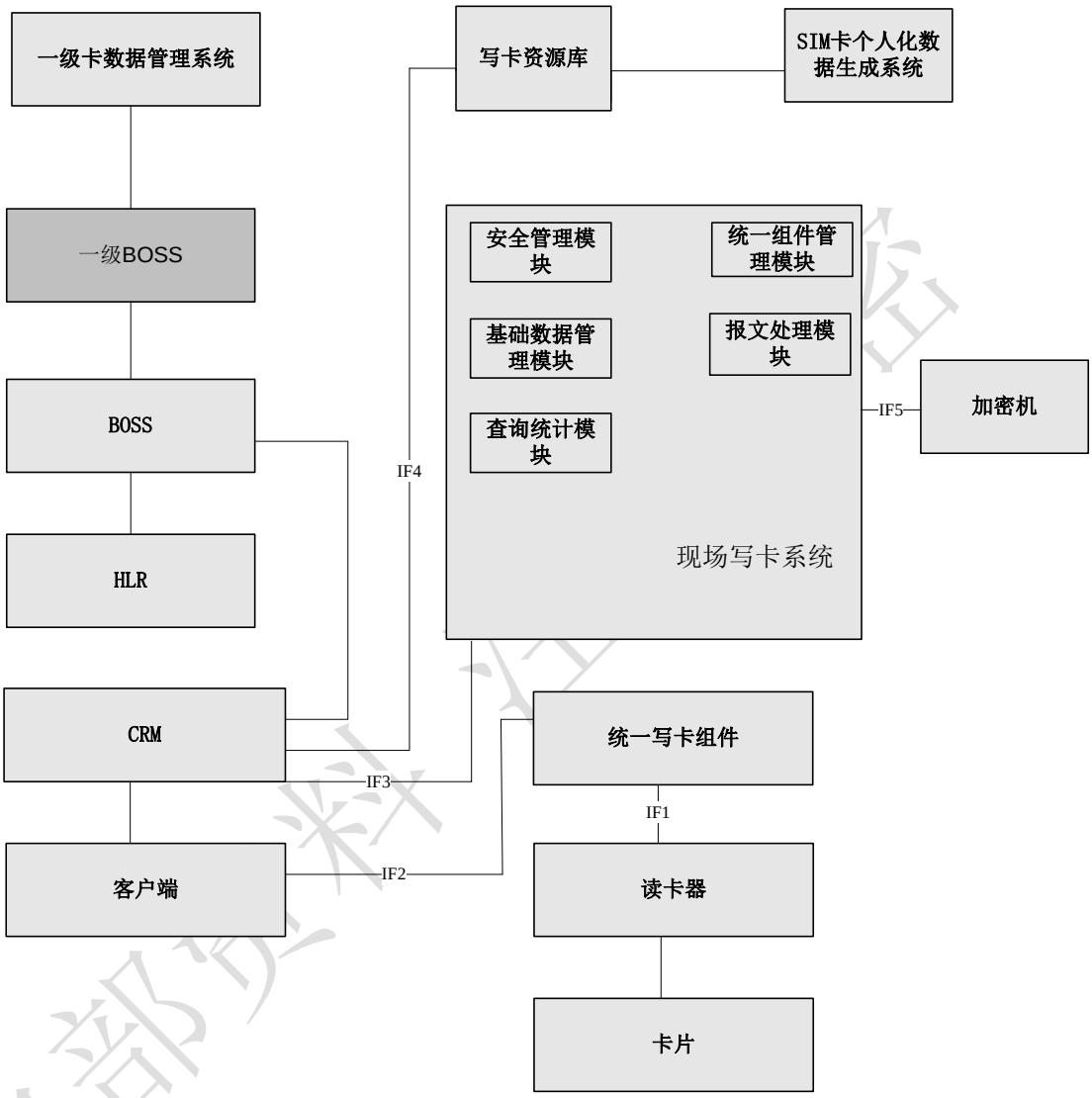


图 10-1　接口结构图

本标准的接口结构图中主要介绍与现场写卡系统直接相关的网元接口，其他涉及的一级卡数据管理系统与一级 BOSS 互操作、一级 BOSS 与省 BOSS 互操作、省 BOSS 与 HLR 开通等逻辑和流程，CRM 系统和客户端的互操作等应遵循中国移动相关规范或由省公司补充规定。

现场写卡系统主要由安全管理模块，基础数据管理模块，报文处理模块，查询统计模块及统一组件管理模块组成。

现场写卡系统的主要功能包括：

1. 安全管理模块功能包括现场写卡配备的加密机应对所有密钥的集中管理、统一加解密处理；

2. 报文处理模块功能包括对写卡报文的打包及写卡结果报文处理；

3. 基础数据管理包括现场写卡业务的卡业务相关数据的集中管理，包括卡商，卡类型等数据的管理；

4. 查询统计模块包括对写卡情况的查询统计功能，日志的查询统计功能。提供按卡商，卡类型，时间等不同维度的查询和统计功能；

5. 统一组件管理模块包括统一组件的上传，版本管理功能。

接口说明如下：

1） 读卡器控制组件与统一写卡组件之间的接口（IF1）

该接口的具体指令参见 8.6 节的相关定义。

表 10-1 读卡器控制组件与统一写卡组件之间的接口描述

参考点	接口类名	接口类描述
IF1	操作类	1. 连接读卡器 2. 卡片上电 3. 发送 APDU 指令 4. 卡片下电 5. 关闭读卡器

2） 统一写卡组件与客户端之间的接口（IF2）

该接口的具体指令参见 10.2 节的相关定义。

表 10-2 统一写卡组件与客户端之间的接口描述

参考点	接口类名	接口类描述
IF2	操作类	1. 获取版本信息 2. 读空卡序列号 3. 读取卡片信息 4. 实时写卡数据写入 5. 获取错误信息 6. 获取读卡器信息

3） CRM 与现场写卡系统之间的接口（IF3）

该接口的具体指令参见 10.4 节的相关定义。

表 10-3 CRM 与现场写卡系统之间的接口描述

参考点	接口类名	接口类描述
IF3	操作类	1. 实时写卡数据加密及报文组装 2. 漫游省预置数据解密并加密

		3. 归属省预置数据解密并加密 4. 写卡结果回传及校验

4) CRM 与写卡资源库之间的接口（IF4）

该接口的具体指令参见 10.3 节的相关定义。

表 10-4 CRM 与写卡资源库之间的接口描述

参考点	接口类名	接口类描述
IF4	操作类	1. 申请实时写卡数据 2. 申请预置数据 3. 实时写卡数据状态更新 4. 预置数据状态更新

5) 现场写卡系统与加密机之间的接口（IF5）

该接口的具体指令参见 10.5 节的相关定义。

表 10-5 现场写卡系统与加密机之间的接口描述

参考点	接口类名	接口类描述
IF5	操作类	1. MAC 值计算 2. 数据加密 3. 数据转加密 4. 签名 5. 签名验证 6. 公钥导入 7. 公私钥对生成

10.2 统一写卡组件与客户端间接口

动态库中导出接口函数原型声明统一用_stdcall标准调用约定，不使用默认调用约定方式，如：

extern “C” _declspec(dllexport) bool _stdcall GetOPSVersion (char *Version)

说明如下：

1. 本标准只规定必要的接口函数。各省公司可进行扩充。
2. 编码方式：如无明确说明，char*类参数将采用16进制数字的ASCII字符串表示，即每个字节表示为2个‘0’-‘9’、‘A’-‘F’字符，如0x1A（即10进制数26）

表示为字符串“1A”（ASCII码为0x31 0x41）。

3. 本标准规定统一写卡组件为与CRM间接口适用于不同平台（包括Windows、安卓、Linux等）的实现版本。各省在具体实施时可在本标准的基础上进行适当的封装。例如假设CRM客户端在Windows平台下用JAVAScript+HTML实现可用ActiveX OCX控件的方式对统一写卡组件DLL进行封装，该封装工作可由CRM承建方实现。

10.2.1 获取版本信息

int GetOPSVersion ([out] char * Version)

功能说明：

通过该函数获取统一写卡组件的版本信息。

参数说明：

Version：函数返回，统一写卡组件版本信息。

返回值说明：

0：函数执行成功

非0：函数执行失败

10.2.2 读空卡序列号

int GetCardSN ([out] char * CardSN)

功能说明：

该函数用于读取卡片空卡序列号，该函数支持本标准发布前和发布后的所有现场写卡系统空卡。第 10.2.3 节函数 GetCardInfo 虽亦能读取空卡序列号，但只支持本标准发布后生产的空卡。因此 CRM 客户端可通过调用 GetCardSN 判断是否为本标准发布后生产的空卡。

参数说明：

CardSN：空卡序列号，如卡片符合中国移动《SIM卡远程写卡业务规范》v1.0.0版本，则长度为16位，如卡片符合中国移动《现场写卡技术规范》，则长度为20位。

返回值说明：

0：函数执行成功

非 0：函数执行失败

10.2.3 读取卡片信息

int GetCardInfo ([out] char * CardInfo)

功能说明：

该函数用于读取卡片信息，卡片信息包含卡片ICCID、卡片空卡序列号

参数说明：

CardInfo：该参数包含卡片ICCID、卡片空卡序列号。格式为TLV格式，具体参见第8.3.3节。其中卡片ICCID如果为一卡多号卡，可出现多次。具体请参见第7.7一卡多号卡写卡及第8.2.1节空卡判断。

返回值说明：

0：函数执行成功

非0：函数执行失败

10.2.4 实时写卡数据写入

int WriteCard ([in] char * IssueData，[out] char* Result)

功能说明：

该函数用于实时写卡数据写入。函数返回值为 0 时表示统一写卡组件向卡片发送写卡数据成功并得到卡片响应。写卡是否成功须根据 Result 判断。

参数说明：

IssueData: 现场写卡系统生成的写卡下行报文，如多条报文，用“|”分隔。

Result：卡片返回结果，格式参见第 8.3.3.2 节中第 3 部分“返回数据格式”说明。CRM 向现场写卡系统回传写卡结果时须传带 MAC 值的完整结果。

返回值说明：

0：函数执行成功

非 0：函数执行失败

10.2.5 获取错误信息

int GetOPSErrorMsg ([in] int ErrorCode，[out] char *ErrorMsg)

功能说明：

该函数用于获取错误信息，统一写卡组件将返回最近一次函数调用的错误信息。

参数说明：

ErrorCode：该参数为统一写卡组件最近一次接口调用的错误代码，如最近一次执行成功则该参数返回0。

ErrorMsg：该参数为统一写卡组件最近一次接口调用的错误描述，如最近一次执行成功则该参数返回字符串“NoError”。

返回值说明：

0：函数执行成功

非0：函数执行失败

10.2.6 获取读卡器信息

int ConfigReader([in] int ReaderType,[in] char* DeviceID, [in]char*

Password)

功能说明：

通过该函数连接读卡器。

参数说明：

ReaderType ： 1、USB口读卡器（CM-READER协议）；2、蓝牙读卡器；3、串口读卡器；4、内置读卡器

DeviceID:

- ReaderType 为 1 时取值如下：

  WINDOWS: PCSC读卡器名称

  Linux: PCSC读卡器名称

  Android:USB读卡器VID+PID的16进制字符串，如VID为23D8，PID为0185，则值为23D80185

- ReaderType 为 2 时为蓝牙读卡器 MAC 地址的 16 进制字符串,如读卡器 MAC 地址为 11:22:33:44:55:66，则值为 112233445566。

- ReaderType 为 3 时取值如下：

  WINDOWS: 串口名称，如COM1

  Linux: 终端主机自带的串口，如/dev/ttyS0

  USB卡(线)转换的串口，如/dev/ttyUSB0

  Android: 终端主机自带的串口，如/dev/ttyS0

  USB卡(线)转换的串口，如/dev/ttyUSB0

- ReaderType 为 4 时取值如下：可以设置为固定值，也可以不配置

Password: 蓝牙读卡器连接密码，该字段为预留字段。

返回值：

0成功

-1 失败

调用流程示意图如下:

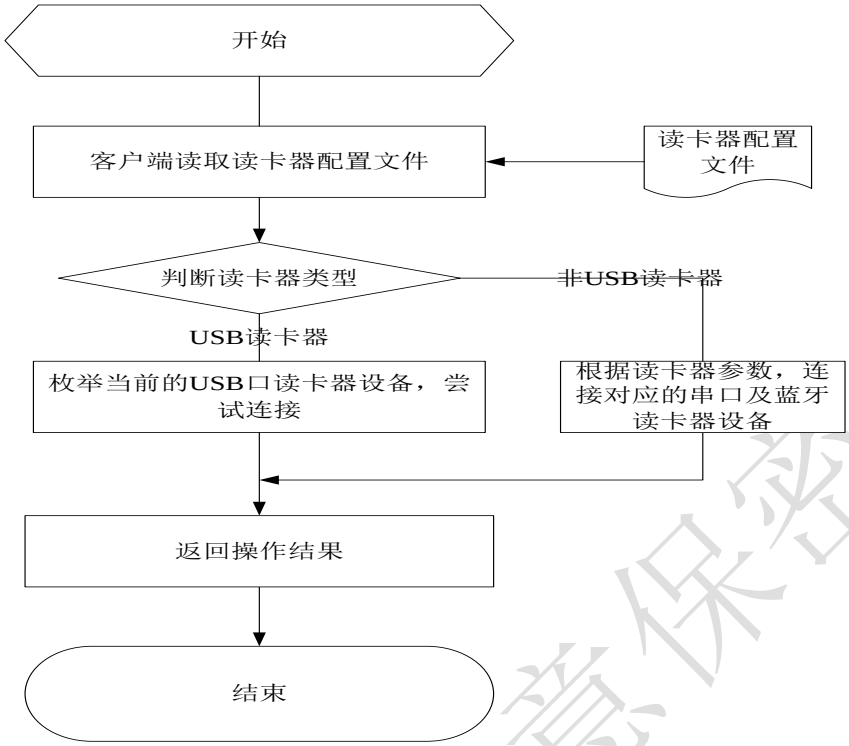


图 10-1　读卡器调用流程图

调用流程描述：

1. 在加载统一写卡组件前客户端根据配置文件的参数，调用 ConfigReader 函数，设置读卡器，如果配置文件中没有相关的读卡器配置信息，则客户端将默认采用 USB 读卡器方式设置读卡器。

2. 统一写卡组件接收到 ConfigReader 函数调用后，判断读卡器类型。

3. 对读卡器类型进行判断：
   1) 判断读卡器类型是否为 USB 口读卡器，统一写卡组件先枚举 USB 口读卡器，然后尝试连接系统中的 USB 读卡器设备。如果连接成功，则返回成功代码。如果连接失败，则返回错误代码。
   2) 判断读卡器类型是否为蓝牙读卡器，则统一写卡组件将利用读卡器 MAC 和连接密码尝试连接蓝牙读卡器。如果连接成功，则返回成功代码。如果连接失败，则返回错误代码。
   3) 判断读卡器类型是否为串口读卡器，如果为串口读卡器，则统一通过指定的串口端口号连接串口读卡器，如果连接成功则成功码，如果连接失败，则返回错误码。
   4) 判断读卡器类型是否为内置读卡器，如果为内置读卡器，则按照内置读卡器默认的连接方式直接连接内置读卡器，如果连接成功则成功码，如果连接失败，则返回错误码。

注：每次打开设备尽量用配置文件中的设备名(即最后一次成功操作的设备名称)，如果打开设备不成功或配置文件中设备名称不存在时，才调用“调用流程示意图”过程。配置文件的内容至少应包含 ReaderType，DeviceID（预留字段）和 Password（预留字段）三个读卡器参数。

10.3 CRM 系统与写卡资源库间接口

写卡资源库是现场写卡业务中管理数据资源的子系统或模块。相应功能的实现各省公司可视情况在现场写卡系统中实现，也可在 CRM 系统中实现。

如果写卡资源库在 CRM 系统中实现，则本节接口为内部接口，可按本章节规定接口实现方式实施，亦可按内部接口自行定义实现。以下描述假定写卡资源库在现场写卡系统中实现。

接口方式：HTTP 或 WebService + XML，把整个 XML 作为输入参数传递。

CRM 与写卡资源库间接口根元素名为 CRM2RSC。

表 10-1　接口数据描述格式说明

格式类型	格式符号	说明
出现次数	?	0.1：可选
	*	0..n：0 到多次
	+	1..n：至少出现一次
	1	1：必选
类型	String	基础数据类型，包括字符串、日期、数字等都采用 String 方式表示
	〈对象类型〉	对象数据类型

接口中出现的实时写卡数据或预置数据节点值均以 TLV 格式给出，具体参见第 8.3.3 节说明。

10.3.1 申请实时写卡数据

申请实时写卡数据由 CRM 向写卡资源库主动发起请求。

该接口可用于省内写卡，也可用于跨省写卡，每次返回最多包含一套实时写卡数据，如进行一卡多号写卡，则须进行多次请求。

表 10-2　请求报文格式

申请实时写卡数据 ApplyDynData							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2RSC	ApplyDynData	1	String	—	申请实时写卡数据	XML 格式
1.1	ApplyDynData	SeqNo	1	String	F10	流水号	十六进制字符

1.2	ApplyDynData	MSISDN	1	String	V20	手机号码	
1.3	ApplyDynData	CardInfo	1	String	V150	卡片信息包含卡片ICCID、卡片空卡序列号	参见表 8-9 定义

表 10-3　应答报文格式

申请实时写卡数据响应 ApplyDynDataRsp							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2RSC	ApplyDynDataRsp	1	String	—	申请实时写卡数据应答	XML 格式
1.1	ApplyDynDataRsp	SeqNo	1	String	F10	请求报文中的流水号	原值返回
1.1	ApplyDynDataRsp	ResultCode	1	String	V10	结果编码	0 为成功返回，其它失败
1.2	ApplyDynDataRsp	ResultMessage	1	String	V256	结果描述	
1.3	ApplyDynDataRsp	IssueData	?	—	—	实时写卡数据	
1.3.1	IssueData	ICCID	1	String	V32	ICCID	
1.3.2	IssueData	IMSI	1	String	V64	IMSI	
1.3.3	IssueData	SMSP	1	String	V20	SMSP	写卡资源库须根据 MSISDN 归属地传回相应的 SMSP
1.3.4	IssueData	PIN1	1	String	V10	PIN1	
1.3.5	IssueData	PIN2	1	String	V10	PIN2	
1.3.6	IssueData	PUK1	1	String	V10	PUK1	
1.3.7	IssueData	PUK2	1	String	V10	PUK2	

10.3.2 申请预置数据

申请预置数据由 CRM 向写卡资源库主动发起请求。

该接口可用于省内写卡，也可用于跨省写卡，对于省内写卡 CRM 在写卡成功后，根据空卡序列号向写卡资源库获取预置数据，与实时写卡数据一起组成一套完整的个人化数据发送给 BOSS 进行号码开通。对于跨省写卡，漫游省 CRM 系统在写卡成功后，根据空卡序列号向漫游省写卡资源库获取预置数据，并在向归属省 CRM 发起开通请求时一起回传预置数据，归属省 CRM 须向归属省现场写卡系统发起预置数据解密再加密请求，解密再加密成功后与实时写卡数据一起组成一组完整的个人化数据发送给 BOSS 进行号码开通。

表 10-4　请求报文格式

申请预置数据 ApplyPreData							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2RSC	ApplyPreData	1	String	—	申请预置数据	XML 格式
1.1	ApplyPreData	SeqNo	1	String	F10	流水号	十六进制字符
1.2	ApplyPreData	CardInfo	1	String	V150	卡片信息包含卡片 ICCID、卡片空卡序列号	参见表 8-9 定义

表 10-5　应答报文格式

申请预置数据响应 ApplyPreDataRsp							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2RSC	ApplyPreDataRsp	1	String	—	申请预置数据应答	XML 格式
1.1	ApplyPreDataRsp	SeqNo	1	String	F10	请求报文中的流水号	原值返回
1.2	ApplyPreDataRsp	ResultCode	1	String	V10	结果编码	0 为成功返回，其它失败
1.3	ApplyPreDataRsp	ResultMessage	1	String	V256	结果描述	
1.4	ApplyPreDataRsp	PresetData	?	—	—	预置数据	均为使用 KEK 加密的密文数据
1.4.1	PresetData	KI	?	String	F32	KI	如为 SIM 卡写卡，本字段必选，如为 USIM 卡写卡，

							无本字段
1.4.2	PresetData	collision	?	String	F120	索引随机数内容	同上
1.4.3	PresetData	FakeKI	?	String	F32	伪 Ki	同上
1.4.4	PresetData	K	?	String	F32	K	如为 USIM 卡写卡，本字段必选，如为 SIM 卡写卡，无本字段
1.4.5	PresetData	OPc	?	String	F32	OPc	同上

10.3.3 实时写卡数据状态更新

实时写卡数据状态更新由 CRM 向写卡资源库主动发起请求。

该接口可用于省内写卡，也可用于跨省写卡，对于省内写卡 CRM 在写卡完成或开通完成后（参见第 7.2.1 节本省写卡流程步骤 28 及步骤 32），根据完成结果状态向写卡资源库发起状态更新请求。对于跨省写卡，由归属省 CRM 向归属省写卡资源库发起实时写卡数据状态更新（参见第 7.2.2 节跨省写卡流程步骤 25 及步骤 32），状态更新规则详见 7.4。

表 10-6　请求报文格式

实时写卡数据状态更新 UpdateDynData							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2RSC	UpdateDynData	1	String	—	实时写卡数据状态更新	XML 格式
1.1	UpdateDynData	SeqNo	1	String	F10	流水号	十六进制字符
1.2	UpdateDynData	IMSI	1	String	V64	IMSI	
1.3	UpdateDynData	StatusCode	1	String	V10	目标状态编码	参见第 7.4 节

表 10-7　应答报文格式

实时写卡数据状态更新响应 UpdateDynDataRsp							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2RSC	UpdateDynDataRsp	1	String	—	实时写卡数据状态更新响应	XML 格式
1.1	UpdateDynDataRsp	SeqNo	1	Strin	F10	请求报文中的流	原值返回

				g		水号	
1.2	UpdateDynDataRsp	ResultCode	1	Strin g	V10	结果编码	0 为成功返回，其它失败
1.3	UpdateDynDataRsp	ResultMessage	1	Strin g	V256	结果描述	

10.3.4 预置数据状态更新

预置数据数据状态更新由 CRM 向写卡资源库主动发起请求。

该接口可用于省内写卡，也可用于跨省写卡，对于省内写卡 CRM 在写卡完成或开通完成后（参见第 7.2.1 节本省写卡流程步骤 28 和步骤 32），根据完成结果状态向写卡资源库发起状态更新请求。对于跨省写卡，由漫游省 CRM 向漫游省写卡资源库发起预置据状态更新(参见第 7.2.2 节跨省写卡流程步骤 16 和步骤 37)，状态更新规则详见 7.4。

表 10-8　请求报文格式

预置数据状态更新 UpdatePreData							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2RSC	UpdatePreData	1	String	—	预置数据数据状态更新	XML 格式
1.1	UpdatePreData	SeqNo	1	String	F10	流水号	十六进制字符
1.2	UpdatePreData	CardInfo	1	String	V150	卡片信息包含卡片 ICCID、卡片空卡序列号	参见表 8-9 定义
1.3	UpdatePreData	StatusCode	1	String	V10	目标状态编码	参见第 7.4 节

表 10-9　应答报文格式

预置数据状态更新响应 UpdatePreDataRsp							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2RSC	UpdatePreDataRsp	1	Strin g	—	预置数据数据状态更新响应	XML 格式
1.1	UpdatePreDataRsp	SeqNo	1	Strin g	F10	请求报文中的流水号	原值返回
1.2	UpdatePreDataRsp	ResultCode	1	Strin g	V10	结果编码	0 为成功返回，其它失败
1.3	UpdatePreDataRsp	ResultMessage	1	Strin g	V256	结果描述	

10.4 CRM 系统与现场写卡系统间接口

10.4.1 实时写卡数据加密及报文组装

CRM 系统获取实时写卡数据后，须向本省现场写卡系统发起写卡数据加密，并组装报文的请求，CRM 系统将得到的加密写卡报文透传至统一写卡组件即可完成写卡。如果一卡多号需要一次写入，请求报文中应该有多个 EncAssemDynData 节点，每个 EncAssemDynData 节点包括 MSISDN 和 IssueData 两个元素。

该接口可用于省内写卡，也可用于跨省写卡时漫游省获取到归属省实时写卡数据后调用漫游省现场写卡系统本接口进行数据加密及报文组装。

表 10-10　请求报文格式

实时写卡数据加密及报文组装 EncAssemDynData（只有在一卡多号的情况下才有 1.3.3 和 1.3.4 部分）							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2OPS	AssemDynData	1	String	—	写卡数据加密及报文组装	XML 格式
1.1	AssemDynData	SeqNo	1	String	F10	流水号	十六进制字符
1.2	AssemDynData	CardInfo	1	String	V150	卡片信息包含卡片 ICCID、卡片空卡序列号	参见表 8-9 定义
1.3	AssemDynData	ChannelFlag	1	String	V1	写卡请求渠道标示	1 现场写卡 2 两不一快
1.4	AssemDynData	EncAssemDynData	1	String	--	包含号码和实时写卡数据	
1.41	EncAssemDynData	MSISDN	1	String	V20	手机号码	
1.4.2	EncAssemDynData	IssueData	1	String	--	实时写卡数据	格式及取值均与 10.3.1 返回中的 IssueData 节点相同
1.4.3	EncAssemDynData	MSISDN	1	String	V20	手机号码（副号）	
1.4.4	EncAssemDynData	IssueData	1	String	--	实时写卡数据（副号）	格式及取值均与 10.3.1 返回中的 IssueData 节点相同

表 10-11　应答报文格式

实时写卡数据加密及报文组装响应 EncAssemDynDataRsp							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2OPS	EncAssemDynDataRsp	1	String	—	写卡数据加密及报文组装应答	XML 格式
1.1	EncAssemDynDataRsp	SeqNo	1	String	F10	请求报文中的流水号	原值返回
1.2	EncAssemDynDataRsp	ResultCode	1	String	V10	结果编码	0 为成功返回，其它失败
1.3	EncAssemDynDataRsp	ResultMessage	1	String	V256	结果描述	
1.4	EncAssemDynDataRsp	IssueData	?	—	—	实时写卡数据报文（如多条报文，用“|”分隔）	现场写卡的报文组装方式参考本标准 8.3.3.2 节，MAC 计算和加密方式参考 10.5.2.1 节；两不一快的报文组装参考《LTE USIM 卡两不一快自助换卡试点技术方案》

10.4.2 漫游省预置数据解密并加密

本接口用于跨省写卡，漫游省 CRM 系统从漫游省写卡资源库获取预置数据后，向漫游省现场写卡系统发起预置数据转加密请求，转加密成功后 CRM 系统将密文预置数据回传至归属省，归属省 CRM 系统调用归属省现场写卡系统“归属省预置数据转加密”接口完成转加密后，与实时写卡数据一起组成完整的个人化数据项向 BOSS 发起开通请求。

表 10-12　请求报文格式

漫游省预置数据解密并加密 RoamDecEncyPreData							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2OPS	RoamDecEncyPreData	1	String	—	漫游省预置数据解密并加密	XML 格式
1.1	RoamDecEncyPreData	SeqNo	1	String	F10	流水号	十六进制字符
1.2	RoamDecEncyPreData	EncPresetData	?	—	—	预置数据	预置数据格式参见 10.3.2 响应报文中节点 1.4
1.3	RoamDecEncyPreData	LocalProvCode	1	String	F3	归属省公司代码	见附录 C 中的注 1，根据《中国移动网状网接口规范-跨区服务分册》传输的省代码

表 10-13　应答报文格式：

漫游省预置数据解密并加密响应 DecEncyPreDataRsp							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2OPS	RoamDecEncyPreDataRsp	1	String	—	漫游省预置数据解密并加密响应	XML 格式
1.1	RoamDecEncyPreDataRsp	SeqNo	1	String	F10	请求报文中的流水号	原值返回
1.2	RoamDecEncyPreDataRsp	ResultCode	1	String	V10	结果编码	0 为成功返回，其它失败
1.3	RoamDecEncyPreDataRsp	ResultMessage	1	String	V256	结果描述	
1.4	RoamDecEncyPreDataRsp	EncPresetDataK	1	String	F176	密文预置数据 K	密文预置数据 K，具体要求见注 1 的说明
1.5	RoamDecEncyPreDataRsp	EncPresetDataOPc	1	String	F176	密文预置数据 OPc	密文预置数据 OPc，具体要求见注 1 的说明
1.6	RoamDecEncyPreDa	Signature	1	String	F17	签名	K、OPc 的签名

	taRsp				6		信息，具体要求见注 1 的说明

注 1：

密文预置数据 K：该字段是漫游省对 K 的密文，由 KEK 加密转换为采用归属省的公钥加密后的密文；

密文预置数据 OPc：该字段是漫游省对 OPc 的密文，由 KEK 加密转换为采用归属省的公钥加密后的密文；

签名：该字段是将密文预置数据 K 和密文预置数据 OPc 两部分数据合并后计算摘要（SHA-256）作为签名数据，调用加密机接口（采用本省私钥签名）生成的签名值；

加密和签名的计算方式参考 10.5.1.3 和 10.5.2.3 节。

10.4.3 归属省预置数据解密并加密

本接口用于跨省写卡，归属省 CRM 系统收到漫游省回传的预置数据后，须向归属省现场写卡系统发起归属省预置数据转加密请求，归属省 CRM 系统将转加密后的预置数据和实时写卡数据一起组成完整的个人化数据传至归属省 BOSS 进行号码开通。

表 10-14　请求报文格式

归属省预置数据解密并加密 LocalDecEncyPreData							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2OPS	LocalDecEncyPreData	1	String	—	归属省预置数据解密并加密	XML 格式
1.1	LocalDecEncyPreData	SeqNo	1	String	F10	流水号	十六进制字符
1.2	LocalDecEncyPreData	EncPresetDataK	1	String	F176	密文预置数据 K	见 10.4.2 节表 10-13 中注 1 的说明
1.3	LocalDecEncyPreData	EncPresetDataOPc	1	String	F176	密文预置数据 OPc	
1.4	LocalDecEncyPreData	Signature	1	String	F176	签名	
1.5	LocalDecEncyPreData	LocalProvCode	1	String	F3	漫游省公司代码	见附录 C 中的注 1 ，根据《中国移动网状网接口规范-跨区服务分册》传输的省代码

表 10-15　应答报文格式

归属省预置数据解密并加密响应 AssemDynDataRsp							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2OPS	LocalDecEncyPreDataRsp	1	String	—	写卡数据加密及报文组装应答	XML 格式
1.1	LocalDecEncyPreDataRsp	SeqNo	1	String	F10	请求报文中的流水号	原值返回
1.2	LocalDecEncyPreDataRsp	ResultCode	1	String	V10	结果编码	0 为成功返回，其它失败
1.3	LocalDecEncyPreDataRsp	ResultMessage	1	String	V256	结果描述	
1.4	LocalDecEncyPreDataRsp	PresetData	?	—	—	密文预置数据	内容参见 10.3.2 中表 10-5 的 1.4 节，该字段是从漫游省现场写卡系统接收到的数据由本省私钥解密后转换为本省 KEK 加密的密文数据。具体参考 10.5.2.4

10.4.4 写卡结果回传及校验

CRM 客户端完成实时写卡数据写入成功后，获得写卡结果，该写卡结果须回传现场写卡系统，以便现场写卡系统进行必要的验证及后续处理。CRM 系统在得到现场写卡系统验证通过的结果后方可继续后续流程。

表 10-16　请求报文格式

写卡结果回传及校验 WriteCardStatus							
序号	父元素名称	元素名称	约束	类型	长度	描述	取值说明
1	CRM2OPS	WriteCardStatus	1	String	—	写卡数据加密及报文组装	XML 格式
1.1	WriteCardStatus	SeqNo	1	String	F10	流水号	十六进制字符
1.2	WriteCardStatus	CardInfo	1	String	V150	卡片信息包含卡片 ICCID、卡片空卡序列号	参见表 8-9 定义
1.3	WriteCardStatus	CardRsp	1	String	V10	卡片返回结果	格式及取值参见

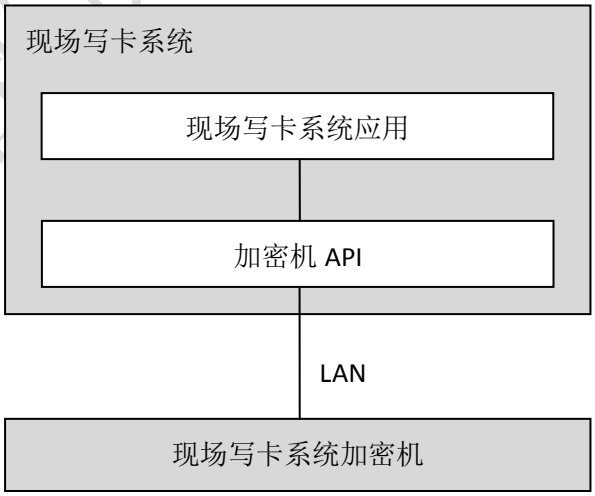
							8.3.3.2 节中第 3 部分“返回数据格式”，调用加密机流程参见 10.5.2.2

表 10-17　应答报文格式

写卡结果回传及校验 WriteCardStatusRsp							
序号	父元素名称	元素名称	约	类型	长度	描述	取值说明
1	CRM2OPS	WriteCardStatusRsp	1	String	—	写卡数据加密及报文组装应答	XML 格式
1.1	WriteCardStatusRsp	SeqNo	1	String	F10	请求报文中的流水号	原值返回
1.2	WriteCardStatusRsp	ResultCode	1	String	V10	结果编码	0 为校验通过，其它则失败
1.3	WriteCardStatusRsp	ResultMessage	1	String	V256	结果描述	

10.5 现场写卡系统与加密机间接口

现场写卡系统通过调用加密机的相关接口实现加解密及相关安全验证功能，如下图所示：



其中，现场写卡系统与现场写卡系统加密机之间以通过局域网进行通信；现场写卡系统软件通过调用加密机 API 完成与加密机的交互。

现场写卡系统加密机 API 提供两种语言的定义：C 和 Java，对于 C 接口，根据不同的平台需求可以提供 DLL 文件（Windows）或 SO 文件（Linux）；对于 Java 接口，以 Jar 包的方式提供。

加密机 API 内部需要提供加密机通信相关的管理功能，如：通信管理、负载均衡等。

现场写卡系统加密机的技术要求见附录-E，接口定义说明如下：

10.5.1 接口定义

10.5.1.1MAC 值计算

- C 接口：

Int DES3MAC([in] int KeyVer, [in] int KeyIndex, [in] int DvsNum, [in] char *DvsData, [in] char *IvData, [in] int MacDatalen, [in] char *MacData, [out] char *MAC)

- Java 接口：

public String DES3MAC(int KeyVer, int KeyIndex, int DvsNum, String DvsData, String IvData, int MacDatalen, String MacData) throws Exception

功能说明：

该函数用于上下行报文的 MAC 值计算，算法为标准 3DES-CBC，具体请参见第 12.2.3 节。

输入参数说明：

KeyVer: 省公司 K1 根密钥版本号（取值范围 0x01-0xff）

KeyIndex: 省公司 K1 根密钥索引（取值范围 0x01-0xff）

DvsNum: 省公司密钥的分散次数

DvsData：省公司密钥的分散因子，长度为 N*8BYTE，N 为分散次数；

IvData: MAC 计算初始值初始化向量（默认值为 8 字节的“0x00”）

MacDatalen：MAC 计算数据的长度

MacData：MAC 计算数据

输出参数说明：

C 接口：

MAC：MAC 计算结果

返回值说明:

C 接口：

0：函数执行成功

非 0：函数执行失败

Java 接口：

返回 MAC 值

10.5.1.2数据加密

- C 接口：

int EncryptData([in] int KeyVer, [in] int KeyIndex, [in] int DvsNum, [in] char *DvsData, [in] int DataLen，[in] char *Data , [out]char *Result)

- Java 接口：

public String EncryptData(int KeyVer, int KeyIndex, int DvsNum, String DvsData, int DataLen，String Data) throws Exception

功能说明：

该函数用于数据加密，算法为 3DES-CBC（具体要求见 12.2.4 节），该函数可用于以下场景：

- 现场写卡系统在本省写卡业务中用预置卡密钥 K1 对写卡数据报文进行加密

输入参数说明：

KeyVer:密钥版本号（取值范围 0x01-0xff）

KeyIndex:密钥索引（取值范围 0x01-0xff）

DvsNum:密钥的分散次数。若需要使用 K1 时，该值为 2；使用其他密钥时则该值为 0；

DvsData：密钥的分散因子，长度为 N*8BYTE，N 为分散次数；

Data：待加密数据（HEX字符串），若待加密数据是8的整数倍，则在数据块后增加一个8字节数据块“0x80 00 00 00 00 00 00 00”；若原始数据不是8的整数倍，则需要根据实际的数据长度在命令数据末尾填充1字节的“0x80”，其余字节用“0x00”填充补齐为8字节。

DataLen：待加密数据的长度

输出参数说明：

C接口：

Result：加密后的数据（HEX字符串）

返回值说明：

C 接口：

0：函数执行成功

非0：函数执行失败

Java 接口：

返回加密后的数据

10.5.1.3数据转加密

- C 接口：

int TransEncrypt([in] int Mode, [in] int DecKeyIndex, [in] int DecKeyVer, [in] int EncKeyIndex, [in] int EncKeyVer, [in] int EncPubKeyLen, [in] char *EncPubKey, [in] int DataLen，[in] char *Data , [out] int *ResultLen, [out]char *Result)

- Java 接口：

public String TransEncrypt(int Mode, int DecKeyIndex, int DecKeyVer, int EncKeyIndex, int EncKeyVer, int EncPubKeyLen, String EncPubKey, int DataLen，String Data) throws Exception

功能说明：

该函数用于数据转加密，该函数可用于以下场景：

- 漫游省现场写卡系统在跨省写卡业务中用漫游省 KEK 解密后用归属省的 K2pub 对预置数据进行加密
- 归属省现场写卡系统在跨省写卡业务中用本省 K2Pri 对预置数据进行解密后，采用本省 KEK 对预置数据进行加密

输入参数说明：

Mode:操作模式（1-对称密钥解密，公钥加密；2-私钥解密，对称密钥加密；3-对称密钥解密，对称密钥加密）

DecKeyIndex:解密密钥索引（取值范围 0x01-0xff）

DecKeyVer:解密密钥版本号（取值范围 0x01-0xff）

EncKeyIndex:加密密钥索引（取值范围 0x01-0xff）

EncKeyVer:加密密钥版本号（取值范围 0x01-0xff）

EncPubKeyLen: 外部输入的加密公钥的长度。

Mode=1: 如果该长度为 0，则加密机使用内部公钥，忽略 EncPubKey 参数；该长度不为 0，则使用 EncPubKey 参数传递的公钥

Mode=2/3: 忽略该参数和 EncPubKey 参数

EncPubKey: 外部输入的加密公钥（HEX 字符串）

DataLen：输入的密文数据的长度

Data：输入的密文数据（HEX字符串）

采用对称密钥加密的方式如下：

采用3DES-CBC算法，初始向量全0，填充规则参考12.2.4 加密算法部分的要求。

采用公钥加密的方式如下：

采用RSA1408算法，填充方式为PKCS1

输出参数说明：

C接口：

Result：转加密后的数据（HEX字符串）

采用对称密钥加密的方式如下：

3DES-CBC算法，初始向量全0，填充规则参考12.2.4 加密算法部分的要求。

采用公钥加密的方式如下：

采用RSA1408算法，填充方式为PKCS1

注：解密后的数据为带填充数据，需要根据加密时的填充方式去除填充内容。

返回值说明：

C 接口：

0：函数执行成功

非 0：函数执行失败

Java 接口：

返回转加密后的数据

10.5.1.4签名

- C 接口：

int GenSignature([in] int KeyIndex, [in] int KeyVer, [in] int DataLen, [in] char *Data, [out] int *SignatureLen, [out]char *Signature)

- Java 接口：

public String GenSignature(int KeyIndex, int KeyVer, int DataLen, String Data) throws Exception

功能说明：

该函数用于对外部输入的数据计算签名。

输入参数说明：

KeyIndex:密钥索引（取值范围 0x01-0xff）

KeyVer:密钥版本号（取值范围 0x01-0xff）

DataLen：输入待签名数据的长度

Data：输入的待签名数据（HEX 字符串，加密机内部进行填充）

输出参数说明：

C 接口：

SignatureLen：签名长度

Signature：签名值（HEX 字符串）

采用 SHA-256 计算摘要，填充方式为 PKCS1，采用 RSA1408 算法计算签名。

返回值说明：

C 接口：

0：函数执行成功

非 0：函数执行失败

Java 接口：

返回签名值

10.5.1.5签名验证

- C 接口：

int SignatureVerify([in] int KeyIndex, [in] int KeyVer, [in] int PubKeyLen, [in] char *PubKey, [in] int DataLen，[in] char *Data, [in] int SignatureLen, [in]char *Signature)

- Java 接口：

public int SignatureVerify(int KeyIndex, int KeyVer, int PubKeyLen, String PubKey, int DataLen，String Data, int SignatureLen, String Signature) throws Exception

功能说明：

该函数用于对外部输入的签名信息进行验证。

输入参数说明：

KeyIndex:密钥索引（取值范围 0x01-0xff）

KeyVer:密钥版本号（取值范围 0x01-0xff）

PubKeyLen: 密文公钥长度，如果该长度为 0，则使用内部公钥

PubKey: 外部传入的公钥值

DataLen：输入签名数据的长度

Data：输入的签名数据（HEX 字符串）

SignatureLen：签名长度

Signature：签名值，要求与签名接口相同（HEX 字符串）

返回值说明：

0：MAC 校验成功

非 0：MAC 校验失败

10.5.1.6公钥导入

- C 接口：

int PubKeyInput([in] int Mode, [in] int KeyIndex, [in] int KeyVer, [in] int PubKeyDataLen , [in] char *PubKeyData, [out] int EncPubKeyDataLen, [out]char *EncPubKeyData)

- Java 接口：

public String PubKeyInput(int Mode, int KeyIndex, int KeyVer, int PubKeyDataLen, String PubKeyData) throws Exception

功能说明：

该函数与密钥生成/录入操作的安全要求相同，需要经过密管操作鉴权（密钥管理员）后才可以调用。

该函数用于将外部输入的公钥导入加密机，根据操作模式的选择，加密机应该支持将公钥保存在加密机或者将公钥加密后输出，该函数可用于以下场景：

- 省公司接收到其它省的公钥后，将公钥导入加密机

输入参数说明：

Mode:操作模式（1-公钥存储在加密机内；2-公钥加密存储在加密机外）

KeyIndex:导入公钥索引（取值范围 0x01-0xff）

KeyVer: 导入公钥版本号（取值范围 0x01-0xff）

PubKeyDataLen：输入公钥数据的长度

PubKeyData：输入的公钥数据

输入为 RSA 公钥（1408Bit），公钥数据为采用 DER 编码

输出参数说明：

C 接口：

EncPubKeyDataLen: 输出数据的长度

EncPubKeyData（HEX 字符串）：

Mode=1，该输出为空

Mode=2，该输出为采用加密机对如下信息加密后的数据：

Data+SHA-256(Data)，其中：

Data = KeyIndex+KeyVer+PubKeyData

加密算法采用不低于128Bit对称密钥算法强度。

返回值说明：

C 接口：

0：函数执行成功

非 0：函数执行失败

Java 接口：

加密后的公钥

10.5.1.7公私钥对生成

- C 接口：

int GenKeypair([in] int KeyIndex, [in] int KeyVer, [in] int KeyLen，[out] int *PubKeyDataLen, [out]char *PubKeyData)

- Java 接口：

public String GenKeypair(int KeyIndex, int KeyVer, int KeyLen) throws Exception

功能说明：

该函数需要经过密管操作鉴权（密钥管理员）后才可以调用。

该函数用于生成指定长度的公私钥对，并输出公钥数据，该函数可用于以下场景：

- 省公司密管人员操作加密机生成 K2 密钥对

输入参数说明：

KeyIndex:密钥索引（取值范围 0x01-0xff）

KeyVer:密钥版本号（取值范围 0x01-0xff）

KeyLen：密钥长度（位长）

输出参数说明：

C 接口：

PubKeyDataLen：公钥数据长度

PubKeyData：

DER 编码的 RSA 公钥数据

返回值说明：

C 接口：

0：函数执行成功

非 0：函数执行失败

Java 接口：

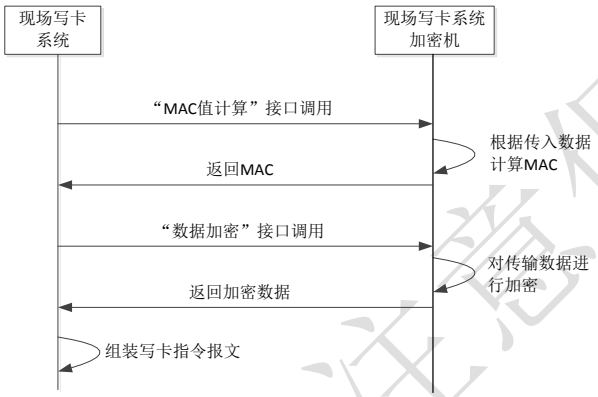
返回 DER 编码的 RSA 公钥数据

10.5.2 接口调用流程

在各类业务流程中，现场写卡系统需要调用 1 个或多个加密机接口 API，完成相应的业务功能，相关 API 的调用流程说明如下：

10.5.2.1 本省写卡指令生成（MAC 计算+数据加密）

当 CRM 系统调用 10.4.1 节中的“实时写卡数据加密及报文组装”接口时，现场写卡系统需要按照如下流程调用加密机接口，以完成安全写卡指令的组装（包括数据的加密及 MAC 计算）：

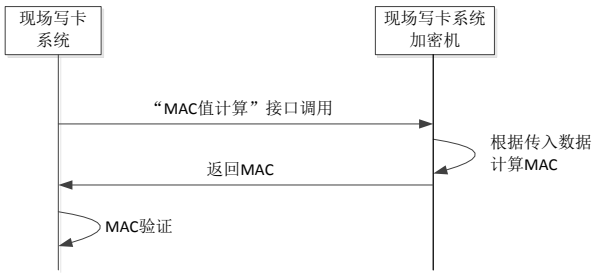


流程说明：

1. 现场写卡系统调用加密机的“MAC 值计算”API，主要参数说明如下：
   a) 密钥索引/版本：本省 K1 根密钥的索引和版本号；
   b) 分散次数和因子：分散次数为 3，分散因子依次为：卡商代码（补位至 8 字节）、卡片序列号后 8 字节、随机数，即将三个因子顺序连接；
   c) MAC 计算数据：按照 12.2.3 中的“下行”的要求进行组装；
2. 加密机返回 MAC 计算结果；
3. 现场写卡系统调用加密机的“数据加密”API，主要参数说明如下：
   a) 密钥索引/版本：本省 K1 根密钥的索引和版本号；
   b) 分散次数和因子：分散次数为 2，分散因子依次为：卡商代码（补位至 8 字节）、卡片序列号后 8 字节，即将两个因子顺序连接；
   c) 待加密数据：按照 8.3.3.2 节中的“报文格式”中对加密内容的要求进行组装；
4. 加密机返回加密数据；
5. 现场写卡系统按照 8.3.3.2 节规定的写卡指令要求组装写卡指令报文。

10.5.2.2 本省写卡指令响应的 MAC 验证

当 CRM 系统调用 10.4.4 节中的“写卡结果回传及校验”接口时，现场写卡系统需要对其中的 MAC 进行验证，需要按以下流程调用加密机接口完成验证：

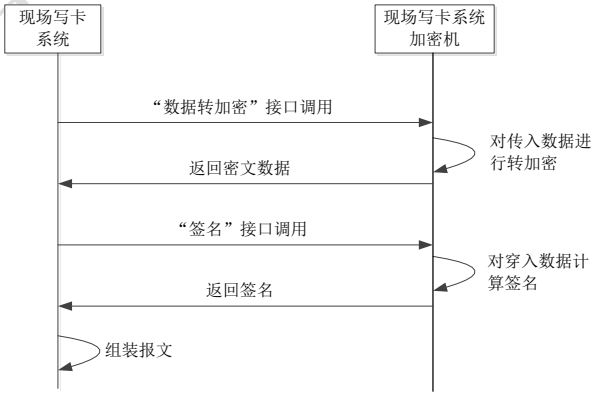


流程说明：

1. 现场写卡系统调用加密机的“MAC 值计算”API，主要参数说明如下：
   a) 密钥索引/版本：本省 K1 根密钥的索引和版本号
   b) 分散次数和因子：分散次数为 3，分散因子依次为：卡商代码（补位至 8 字节）、卡片序列号后 8 字节、随机数，即将三个因子顺序连接；
   c) MAC 计算数据：按照 12.2.3 中的“上行”报文的要求进行组装；
2. 加密机返回 MAC 计算结果；
3. 现场写卡系统完成 MAC 验证。

10.5.2.3 跨省数据发送（数据转加密+签名）

当 CRM 系统调用 10.4.2 节中的“漫游省预置数据解密并加密”接口时，现场写卡系统需要按以下流程调用加密机接口，以完成对跨省数据的转加密及签名：

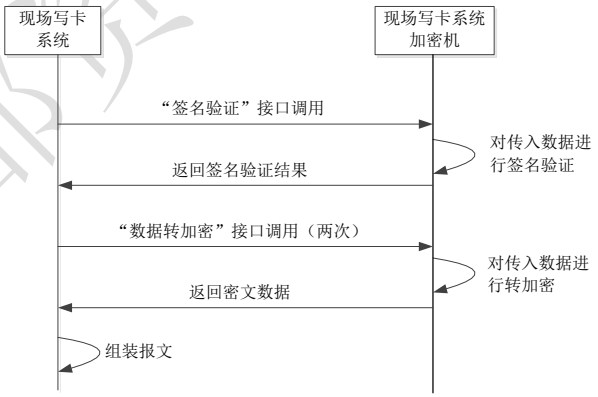


流程说明：

1. 现场写卡系统调用加密机的“数据转加密”API，对 K 和 OPc 的密文分别进行转加密（两个密文分别调用 API），主要参数说明如下：
   a) 操作模式：取值为 1，即对称密钥解密，公钥加密；
   b) 解密密钥索引/版本：漫游省 KEK 的索引和版本；
   c) 加密密钥索引/版本：归属省公钥的索引和版本；
   d) 输入的密文数据:CRM 传递的经 KEK 加密的 K 或 OPc 密文,见 10.4.2 节表 10-12 中相应字段；
2. 加密机返回转加密后的 K 和 OPc 密文数据（由归属省 K2pub 加密）；
3. 现场写卡系统调用加密机的“签名”API，主要参数说明如下：
   a) 签名密钥索引/版本：漫游省私钥的索引和版本；
   b) 输入的待签名数据：调用加密机“数据转加密”API 生成的密文数据，K 密文+OPc 密文；
4. 加密机返回签名；
5. 现场写卡系统按照 10.4.2 节的规定组装报文。

10.5.2.4 跨省数据接收（签名验证+数据转加密）

当 CRM 系统调用 10.4.3 节中的“归属省预置数据解密并加密”接口时，归属省的现场写卡系统需要按以下流程调用加密机接口，以完成对跨省数据的签名验证和转加密：



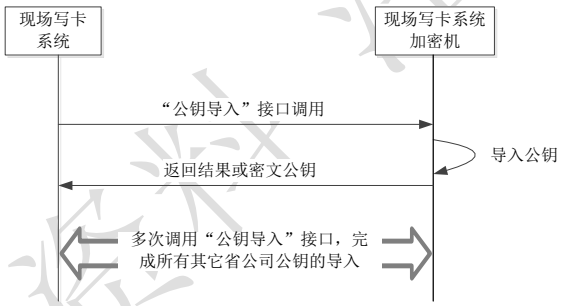
流程说明：

1. 现场写卡系统调用加密机的“签名验证”API，主要参数说明如下：
   a) 密钥索引/版本：归属省公钥的索引和版本号
   b) 输入的签名数据：10.4.3 节表 10-14 中的 K 和 OPc 的密文；
   c) 输入的签名值：10.4.3 节表 10-14 中的“签名”；

2. 加密机返回签名验证结果；
3. 如果以上的签名验证结果正确，则现场写卡系统调用加密机的“数据转加密”API，分别对 K 和 OPc 的密文进行转加密（K 和 OPc 转加密分别调用 API），主要参数说明如下：
   a) 操作模式：取值为 2，即私钥解密，对称密钥加密；
   b) 解密密钥索引/版本：归属省私钥的索引和版本；
   c) 加密密钥索引/版本：归属省 KEK 的索引和版本；
   d) 输入的密文数据：10.4.3 节表 10-14 中的 K 的密文或 OPc 的密文；
4. 加密机返回转加密后的密文数据；
5. 现场写卡系统按照 10.4.3 节表 10-15 的要求组装写卡指令报文。

10.5.2.5 其它省的公钥导入

对于其它省公司的公钥导入，可以由密钥管理工具按照以下流程调用加密机接口完成：

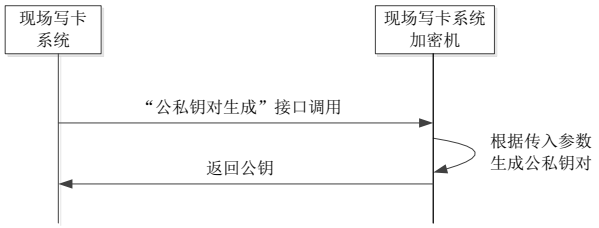


流程说明：

1. 密钥管理工具调用加密机的“公钥导入”API，主要参数说明如下：
   a) 操作模式：如公钥存储在加密机内，该值为 1，如公钥加密存储在加密机外，该值为 2；
   b) 导入公钥的索引/版本：其它省公司接收的公钥的索引和版本号；
   c) 输入的公钥数据：从其它省公司获取的 DER 编码格式的公钥；
2. 加密机返回导入结果以及加密的公钥（如果公钥存在加密机外部）；
3. 密钥管理工具重复调用加密机的 “公钥导入”API，完成所有其它省公司的公钥导入操作。

10.5.2.6 本省公私钥对生成

本省公私钥对的生成，可以由密钥管理工具完成，该工具需要按以下流程调用加密机接口：



流程说明：

1. 现场写卡系统调用加密机的“公私钥对生成”API，主要参数说明如下：
   a) 密钥索引/版本：本省私钥的索引和版本号；
   b) 密钥长度：选择 1408；
2. 加密机返回生成的公钥。

11 兼容性要求

为降低系统升级成本和保证市场运营平稳过渡，现场写卡系统按本标准要求进行升级改造时，应尽量考虑兼容旧版空卡的写卡。建议按以下原则处理：

1. 在升级前已有的写卡设备（例如ＰＣ终端），要求 CRM 客户端对所插入卡片根据空卡序列号进行新旧版本判别，若为旧版空卡，则调用旧版远程写卡系统处理模块进行写卡，若为新版预置空卡，则调用新系统处理模块进行写卡。各省公司视本省旧版空卡库存情况酌情考虑是否需要同时两个版本需要并行运行以及并行运行的时间。
2. 在升级后使用的新写卡设备（例如新 PC 终端、移动设备等），CRM 客户端须根据空卡序列号判别新旧版本空卡，若为旧版本空卡则报错误信息提示换卡并结束写卡流程。

12 安全性要求

密钥管理相关要求参考《中国移动(U)SIM 卡发卡密钥管理方案(电信应用部分)》。

12.1 密钥定义

为保证现场写卡业务中个人化数据的安全，在业务流程涉及的相关系统中需要安全存储多套加解密密钥，有关密钥的生成、更新等具体要求请参见另外的密钥管理相关文档，不在本标准中描述。

密钥使用位置详细参见下表：

表 12-1　密钥使用位置说明

	数据生成系统	写卡资源库	现场写卡系统配备的加密机	预置空卡	BOSS	HLR
K1	√	×	√	√	×	×
K2	×	×	√	×	×	×
KEK	√	×	√	×	×	√
KT	√	×	√	×	×	√

注 1：数据生成系统包括 SIM 个人化数据生成系统及一级卡数据管理系统。

注 2：密钥 K1 为一卡一密，加密机中只存储 K1 的根密钥，实时分散出卡的 K1 密钥。

注 3：密钥 K2 和 KEK 没有分散过程，直接将密钥存储在加密机中。

注 4：每个省公司的现场写卡加密机中保存本省的 KT 公钥(KTpub)和 KT 私钥(KTpri)，数据生成系统加密机保存省公司传递的 KT 公钥（KTpub）。

密钥用途如下图所示：

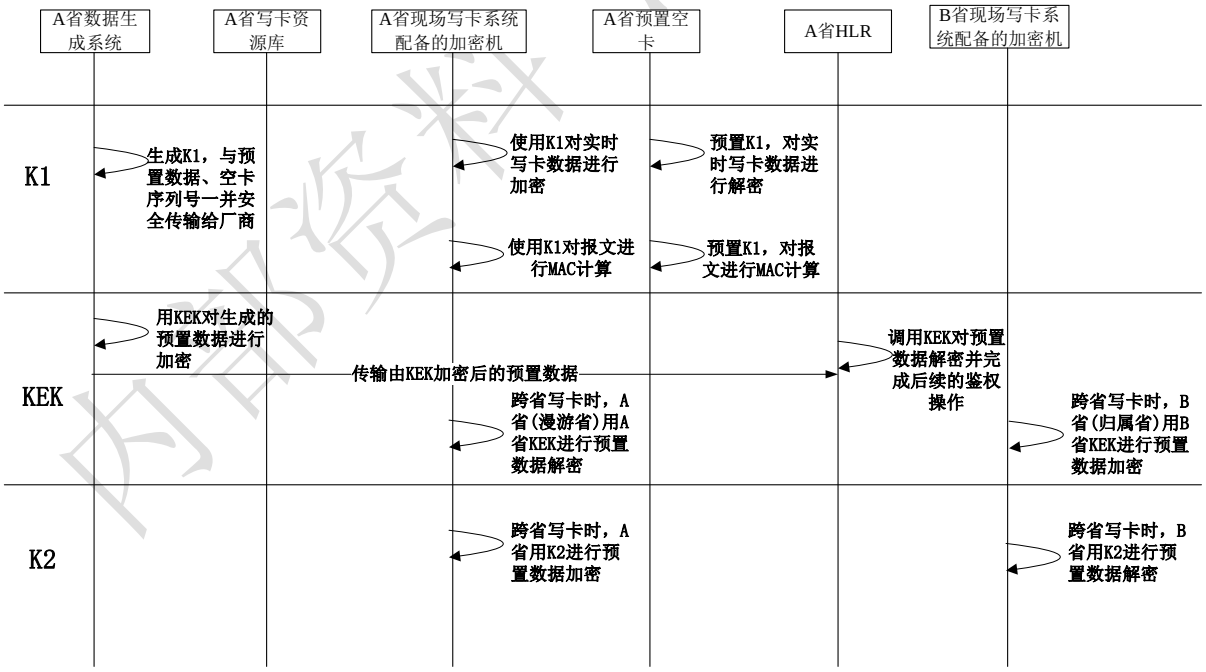


图 12-1　密钥使用图

12.1.1 K1

K1 为预置卡密钥，该密钥为对称密钥，长度为 128Bit，用于对写卡数据报文的加解密和生成写卡报文 MAC 计算的会话密码。

K1 的分散层次如下图所示：

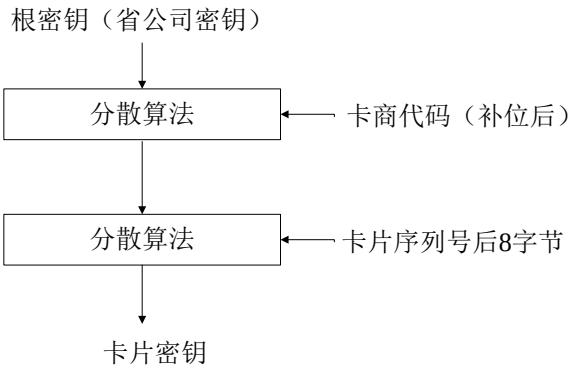


图 12-2　预置卡密钥 K1 分散层次图

其中，K1 根密钥（即省公司密钥）每省 1 个，各省独立管理。K1 卡片密钥由数据生成系统在生成预置数据时一并生成，一卡一密。该密钥与预置数据、空卡序列号一起提交卡商，卡商在生产预置空卡时一并写入。预置写卡密钥及预置数据传输给卡商。

K1 的分散算法如下图所示：

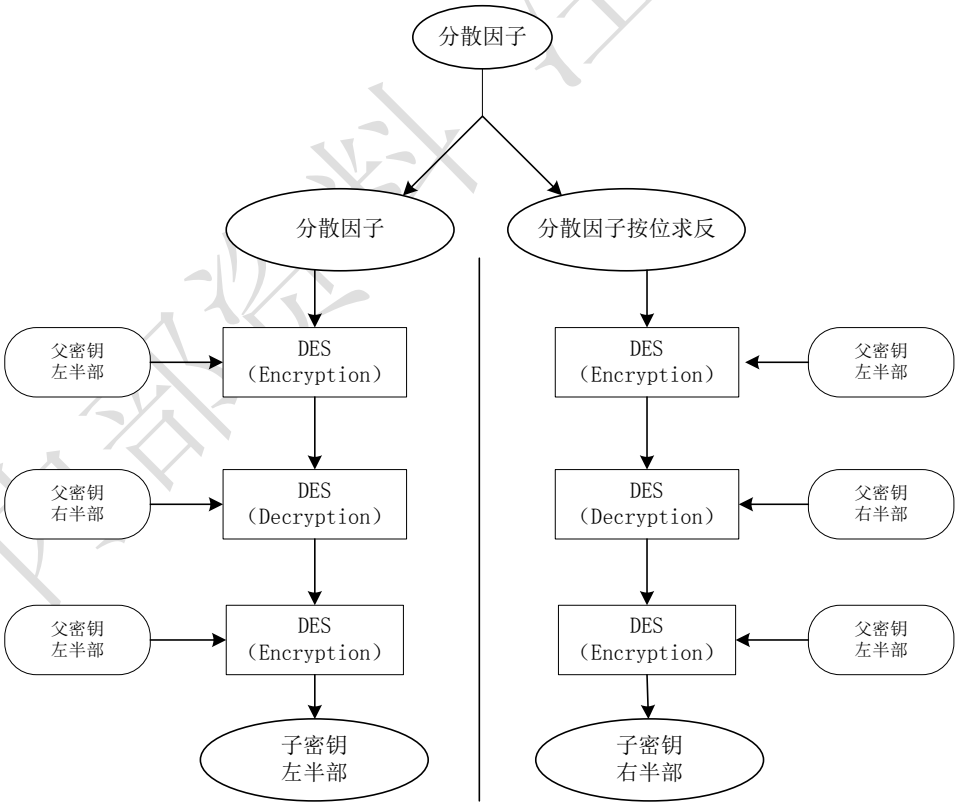


图 12-3　分散算法流程图

说明：分散算法中的 DES 算法全部采用标准的 DES－ECB 算法。卡商代码的补位规则如下：在卡商代码前先补一位 0，形成第一个字节，再补 7 个 0x20，变成 8 个字节。例如卡商代码为 1，则补位后的值为 0120202020202020。

12.1.2 K2

K2 为跨省传输保护密钥，是一对非对称密钥对的总称，包括公钥 K2pub 和私钥 K2pri，每省 1 对密钥。K2 采用 RSA 算法（模长 1408Bit），用于对跨省传输的预置数据进行安全传输。

漫游省 CRM 从写卡资源库获取预置数据后，调用现场写卡系统配备的加密机对预置数据进行转加密，转加密是在加密机内部完成的解密和加密的过程，其中采用漫游省 KEK 解密，使用归属省的 K2pub 加密。然后通过一级 BOSS 将数据回传至归属省 CRM 系统，归属省 CRM 系统发送开通指令前，须调用归属省现场写卡系统配备的加密机对预置数据转加密，转加密是在加密机内部完成的解密和加密的过程，其中采用归属省的私钥 K2pri 解密，然后采用归属省 KEK 加密。

12.1.3 KEK

KEK 是预置数据加密密钥，每省 1 个独立维护，该密钥为对称密钥，长度为 128Bit，提高预置数据存储在系统中的安全性。数据生成系统、现场写卡系统和 HLR 均保存该密钥。

SIM 个人化数据生成系统或一级卡数据管理系统生成预置数据后立即用该密钥对数据加密，存储在写卡资源库中，最终经过 KEK 加密的预置数据传入 HLR 中进行开通，除漫游省写卡外，整个业务各系统中流转的预置数据均为经 KEK 加密的密文数据。

12.1.4 KT

KT 是用于现场写卡系统加密机和其它加密机之间进行密钥传递过程中使用的传输密钥（非对称密钥），每省 1 对密钥，KT 采用 RSA 算法（模长 1408Bit）。

密钥传递过程采用密钥信封方式，发送方采用接收方的传输公钥（KTpub）对随机生成的加密密钥进行加密（采用加密密钥对目标密钥进行加密），接收方采用本方的传输私钥（KTpri）对加密密钥密文进行解密（进而采用加密密钥解密出目标密钥）。

具体的密钥传输技术要求见附录-F 中的说明。

12.2 写卡安全性要求

1. 预置数据

- SIM 个人化数据生成系统及一级卡数据管理系统，在预置数据生产完毕，确认已成功导入到相应的系统中后，必须删除相应的数据及数据文件。
- 写卡资源库负责预置数据的安全存储，写卡资源库必须保障数据的可靠性及提供完善的数据备份和恢复机制，预置数据使用后必须及时删除。

- 对自有营业厅或非自有营业厅现场写卡均要求对预置空卡进行写卡，即卡内需预置 Ki/（OPc、K）等预置数据、空卡序列号及预置卡密钥 K1。
- 预置数据在整个传输过程中必须采用密文传输。
- 在本省写卡及跨省写卡流程中对写卡数据起传输作用的系统或网元，例如 BOSS、现场写卡系统、CRM 等不得存储预置写卡数据。

2. 实时写卡数据

- SIM 个人化数据生成系统及一级卡数据管理系统，在实时写卡数据生产完毕，确认已成功导入到相应的系统中后，必须删除相应的数据及数据文件。
- 写卡资源库负责实时写卡数据的安全存储，写卡资源库必须保障数据的可靠性及提供完善的数据备份和恢复机制，实时写卡数据使用后必须及时删除或回收，对于写卡开通成功的 IMSI 资源进行删除，对于确认的写卡失败或开通失败的 IMSI 资源可进行回收再利用。
- 实时写卡数据下发到客户端及发送到卡内，均应密文传输，并保证数据完整性。
- 现场写卡系统必须配置加密机，对系统涉及的密钥必须保存在加密机中，加密机在写卡中还对敏感数据进行加解密和 MAC 运算。
- 加解密所用的密钥长度为 128bit 及以上，应有完善的机制保证密钥的安全。

12.2.1 本省写卡操作密钥使用情况

本省写卡预置数据及实时数据加解密过程见下图所示：

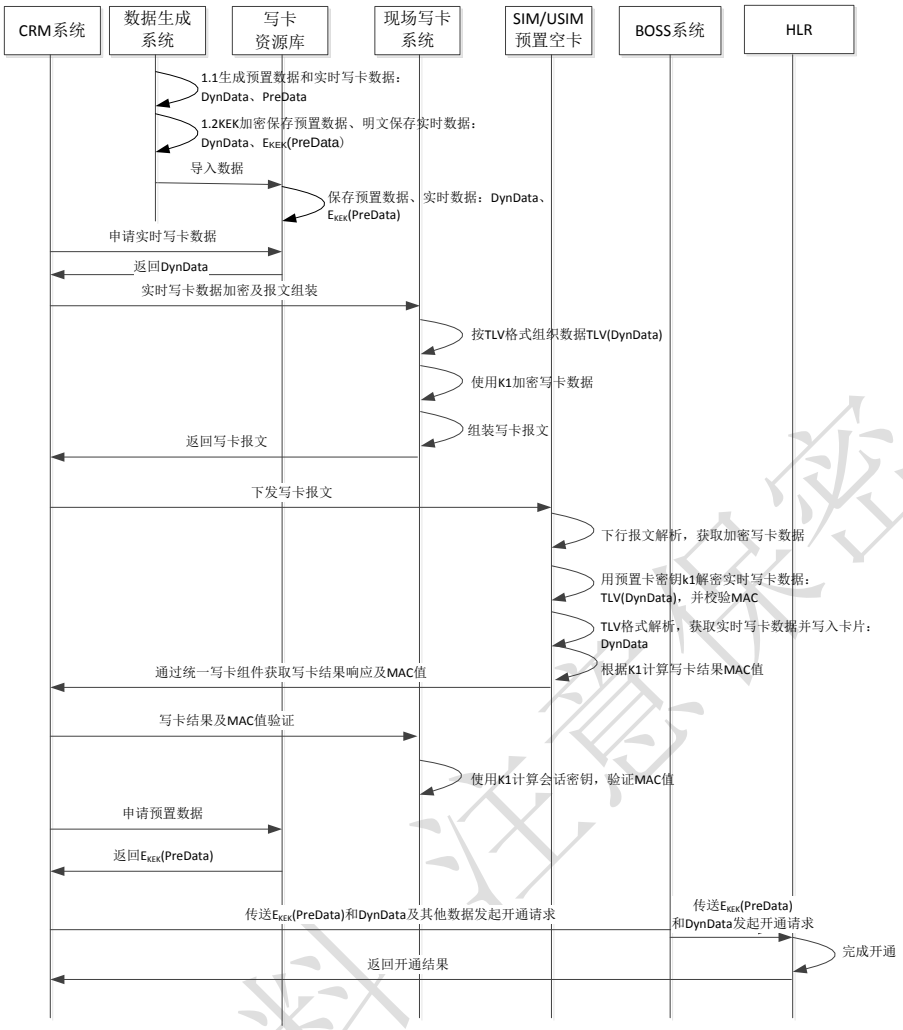


图 12-4　本省写卡预置数据及实时数据加解密流程图

12.2.2 跨省写卡操作密钥使用情况

跨省写卡预置数据及实时数据加解密及跨省传输过程见下图所示，与本省写卡相比，不同之处主要在于：

1. 漫游省 CRM 通过一级 BOSS 从归属省获取实时写卡数据后，向漫游省现场写卡系统发起数据加密及组包请求，然后将写卡数据报文通过统一写卡组件下发卡片。
2. 写卡成功后，漫游省 CRM 向写卡资源库查询预置数据。所查询到的预置数据为漫游省 KEK 加密的密文数据，CRM 向漫游省现场写卡系统发起转加密请求。
3. 漫游省 CRM 用归属省 K2pub 加密的预置数据和实时数据通过一级 BOSS 向归属省 BOSS 发起开通请求。
4. 归属省 BOSS 通过归属省 CRM 向现场写卡系统发起数据转加密请求
5. 归属省 BOSS 获得归属省 KEK 加密的预置数据后，与实时写卡数据一起发送 HLR 及 AUC 完成开通流程及后续流程。

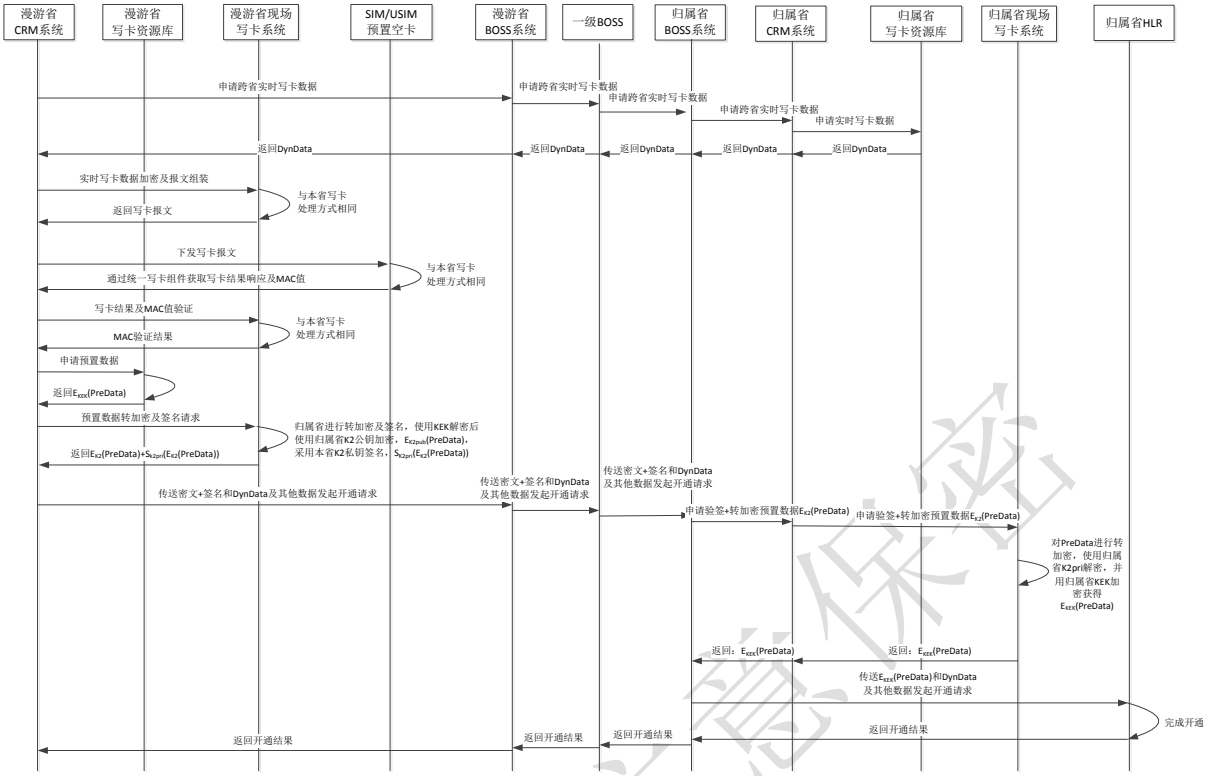


图 12-5　跨省写卡预置数据及实时数据加解密流程图

12.2.3 MAC 算法

MAC 运算采用标准的 3DES-CBC 算法。

MAC 密钥为 K1 根据写卡系统生成的写卡报文中的随机数分散运算获得，分散方式如下图所示。其中，K1 作为分散算法的父密钥，8 字节的随机数作为分散因子进行分散，生成 MAC 计算密钥。具体分散算法参见图 12-3。

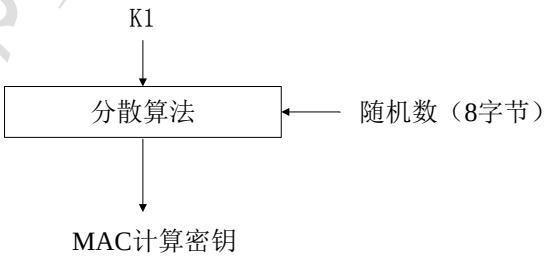


图 12-6　MAC 计算密钥分散图

计算 MAC 时应包含以下数据：

下行：CPL、 CHL 、SPI 、Kic、 KID、 TAR、 CNTR、 PCNTR、Secured Data

上行：写卡结果、下行报文中的随机数

MAC 计算的具体方法：

第一步：取 8 个字节的 16 进制’0x00’作为初始值。

第二步：将所有原始数据按照每 8 个字节一组进行分组 D1，D2，D3，D4，……，Dn，若原始数据是 8 的整数倍，则在数据块后增加一个 8 字节数据块’0x80 00 00 00 00 00 00 00’；若原始数据不是 8 的整数倍，则在该数据块后填补一个值为 16 进制’0x80’的字节，其余字节用 16 进制’0x00’的字节补齐为 8 字节。计算 MAC 所需填充的数据不包含在实际传送的报文数据中，由 MAC 值校验方在计算 MAC 码时根据数据长度自行填充。

第三步：对这些数据块使用会话密钥进行加密，会话密钥按照上节描述的方式产生。计算过程如下图所示。

第四步：最终得到是从计算结果左侧取得的 4 字节长度的 MAC。

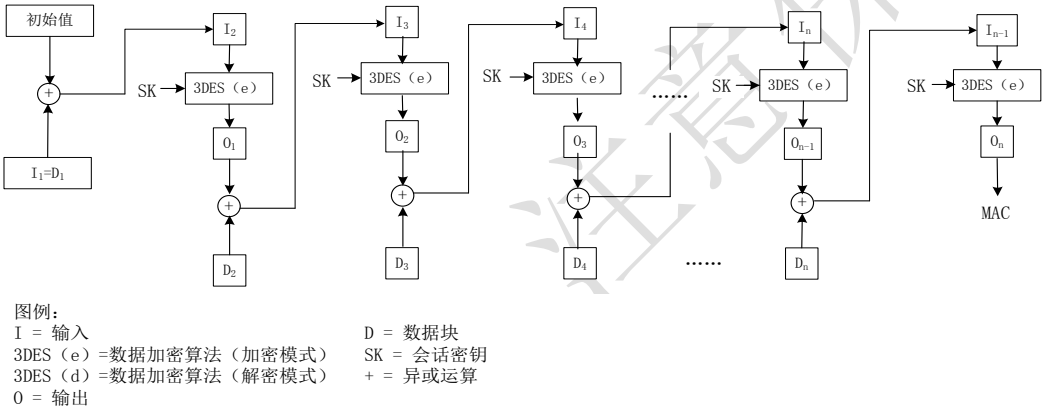


图 12-7 MAC 值计算流程图

12.2.4 加密算法

对于 K1 和 KEK 密钥，加解密算法采用 3DES-CBC，初始向量为 8 字节全 0。数据填充算法采用如下算法：

如果加密数据是 8 的整数倍，则在数据块后增加一个 8 字节数据块’0x80 00 00 00 00 00 00 00’；若原始数据不是 8 的整数倍，则在该数据块后填补一个值为 16 进制’0x80’的字节，其余字节用 16 进制’0x00’的字节补齐为 8 字节。

其中 K1 密钥需要按照 12.1.1 节的要求进行分散，分散方式参考 12.2.3 节。

对于 K2 密钥，加/解密、签名/验签的算法采用 RSA1408 算法，具体的要求见加密机接口部分的说明。

12.2.5 个人化数据更新要求

为保证写卡的安全性，卡内数据只允许成功更新一次，写卡成功后不允许再次更新。

12.3 网络安全性要求

在现场写卡业务系统组网中，通过采用内外网隔离机制（如防火墙），防止通过通信手段对内部网络中的重要数据和业务进行渗透和操纵。另外通过局域网 VLAN 的划分，实现不同子平台、不同级别用户之间的访问控制。

在网络中部署网络防病毒系统、入侵检测系统、安全扫描、加密机等安全相关系统，为平台提供全方位的立体安全保障。

13 编制历史

表 13-1 编制历史

版本号	更新时间	主要内容或重大修改
2.0.0 初稿	2012 年 10 月 30 日	本标准规定了 SIM 卡和 USIM 卡现场写卡的系统架构、业务流程、关键技术要求、设备要求、系统要求等内容。
2.0.0 修订稿	2012 年 11 月 28 日	根据与集团部门的方案评审会议进行业务开放范围、术语等修订
2.0.0 报批稿 2.0.1	2013 年 06 月 28 日 2013 年 11 月 14 日	根据试点省市反馈情况修订 MAC 计算密钥分散规则等内容 版本号：2.0.0；编号：QB-Y0031.13-2013 根据深圳业务运营支撑系统测评中心提交的《CMBSTC-PROJ-USIMCWT-QD037-V1.00 USIM 卡写卡测试项目测试报告 V1.00》进行修订，主要章节：7.2、7.3、7.7、7.8、8.3、8.6、9.3、10.2、10.3、10.4、12.1。
2.1.0	2014 年 1 月 16 日	1、 10.4.2、10.4.3 节密文预置数据中增加了签名 2、 K2 密钥修改为非对称密钥，见 12.1.2 节的说明 3、 删除如下接口： 10.5.3 数据解密接口 4、 增加加密机接口： 10.5.3 数据转加密 10.5.4 签名 10.5.5 签名验证 10.5.6 公钥导入 10.5.7 公私钥对生成 5、 加密算法修改：12.2.4 节
2.1.0	2014 年 2 月	1、 增加 9.10 节 “现场写卡系统加密机”一节

	11 日	2、 增加现场写卡系统与加密机间接口的相关说明，包括调用模式，API 的提供方式等 3、 增加现场写卡系统加密机 API 的 Java 语言接口：10.5.1 4、 增加现场写卡系统加密机 API 的调用流程说明：10.5.2 5、 增加现场写卡系统加密机技术要求：附录-E 6、 删除 10.4.2 中表 10-13 和 10.4.3 节中表 10-14 中的“加密密钥索引随机数”字段 7、 修订 8.3.3 节中“通过 0 次或多次 Fetch 指令” 8、 修订 8.3.3.2 注 1 内容，更新 8-13 表，删除 K、OPC 等 tag，修订 ACC 文件更新描述 9、 删除 10.3.2，表 10-5 中 Random 项 10、 更新 7.2.2 跨省写卡流程描述
2.1.0	2014 年 2 月 24	1、 在 10.4.2 节的 CRM 请求报文中增加省公司代码字段 2、 10.5.1 节的接口定义中修改 Java 接口定义为纯 Java 接口 3、 对附录-E 中的加密机技术要求进行补充 4、 增加附录-F 密钥传输卡技术要求 5、 修订了一些笔误
2.1.0	2014 年 2 月 26	1、 10.4.1 节表 10-10 增加 ChannelFlag 字段，兼容两不一快 2、 10.4.1 节表 10-11 修订 IssueData 取值说明，兼容两不一快
2.1.0	2014 年 3 月 07	1、 10.4.2 节表 10-13，10.4.3 节表 10-14，增加节点分别描述加密的 K、OPc、签名。修订表 10-12，省代码长度及描述 2、 修订附录 C，增加注 1,
2.1.0	2014 年 3 月 14 日	1、 附录-F 中增加了加密机与 IC 卡的指令交互流程

附录 A 卡商代码

表 A-1　卡商代码

雅斯拓	0	大唐微电子	5
天津杰普	1	北京握奇	7
武汉天喻	2	恒宝	8
江西捷德	3	北京华虹	9

东信和平	4	上海柯斯	A

附录 B 数据类型说明

表 B-1　数据类型说明

内容	长度（半字节）	描述	示例
MSISDN	11	客户手机号码	13912345678
ICCID	20	SIM 卡卡号	89860011223344556677
IMSI	15	IMSI 号码	460001234567890
Ki / K	32	鉴权密钥	1234567890ABCDEF1234567890ABCDEF
OPC	32	鉴权密钥	1234567890ABCDEF1234567890ABCDEF
SMSP	14	短信中心号码	+8613800100500
PIN1	4	PIN1 码	1234
PIN2	4	PIN2 码	1234
PUK1	8	PUK1 码	12345678
PUK2	8	PUK2 码	12345678
归属省信息	3	请求指向的省代码，参见附录 C	100
漫游省信息	3	发起请求的省代码，参见附录 C	220
流水号	8	申请批次标识,顺序累加,步长为 1,循环使用； 数据申请请求和个人化数据回传的流水号必须相同。	00000001

附录 C 各省移动公司代码

表C-1　各省公司代码

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

注 1：在涉及跨省业务时，网状网传输使用的省代码要求为：根据《中国移动网状网接口规范-总册》10.1.8 节要求：用于路由关键值的省代码取交换节点代码的前三位，如内蒙古为“471”，北京为“100”。交互节点代码参见附录 D。

附录 D 交换节点代码

根据《中国移动网状网接口规范-总册》10.1.4 节，交换节点代码如下：

表 D-1　交换节点代码

编码（DUNS）	交换节点位置
0000	枢纽交换节点
4710	内蒙古
1000	北京
2200	天津
5310	山东
3110	河北
3510	山西
5510	安徽
2100	上海
2500	江苏
5710	浙江
5910	福建
8980	海南
2000	广东

7710	广西
9710	青海
2700	湖北
7310	湖南
7910	江西
3710	河南
8910	西藏
2800	四川
2300	重庆
2900	陕西
8510	贵州
8710	云南
9310	甘肃
9510	宁夏
9910	新疆
4310	吉林
2400	辽宁
4510	黑龙江

附录 E 现场写卡系统加密机技术要求

一、总体要求

现场写卡系统加密机应通过国家密码管理局的认证（具有产品型号证书）。

二、功能要求

1、密钥管理

现场写卡系统加密机应具备完善的密钥管理能力（需要提供专用的管理工具），涵盖密钥管理的全过程，包括密钥的生成、注入、存储、备份、分发、更新等，具体要求如下：

- **密管人员鉴权**：所有的密钥管理过程中均需要提供基于 IC 卡的密管人员鉴权机制（双人控制）；
- **非对称密钥生成/更新/注入/分发**：具备生成/更新/注入/分发非对称密钥的功能；
- **对称密钥生成/更新/注入/分发**：对称密钥的生成应支持随机生成/更新方式以及多码单分量合成/更新/注入/分发密钥方式（码单数量≥2），对于码单合成方式，每码单长度与待生成的密钥长度相同，多码单采用异或方式合成密钥；
- **密钥的存储/备份**：加密机应支持内部安全存储或外部加密存储密钥的方式；同时提供安全备份加密机内密钥的功能。

针对密钥导出、导入的具体要求包括密钥导入/导出格式、公钥导出/导入、对称密钥导出/导入，分别说明如下：

1.1 密钥导入/导出格式要求

- 加密机内部保存的密钥分为对称密钥和非对称密钥两类，对称密钥支持 3DES、AES、SM1、SM4 等对称运算；非对称密钥又分为 RSA 密钥和 SM2 密钥，分别支持 RSA 和 SM2 非对称运算，对称密钥和非对称密钥支持以密文方式导出和导入。
- 如果需要导出对称密钥，可以进入加密机管理程序的对称密钥管理界面进行相应的导出导入操作。
- 如果需要导出非对称密钥，可以进入加密机管理程序的 RSA 密钥管理界面或 SM2 密钥管理界面进行相应的导出导入操作。
- 密钥可以密文格式导出到密钥传输 IC 卡中，也可从密钥传输 IC 卡导入到加密机，对密钥传输 IC 卡的技术要求见附录 F。

1.2 公钥导出

公钥导出可以作为对称密钥传输的辅助流程，也可以作为独立的传递流程。公钥导出的加密机操作流程如下：

1) 密钥管理员登录（采用授权 IC 卡鉴权，IC 卡需提供口令验证机制以及口令错误锁定机制）；
2) 选择生成公私钥对功能（指定索引和版本号），如果密钥对已经生成过，该步骤可省略；
3) 选择导出公钥，并输入要导出公钥的索引号和版本号；
4) 按照提示分别插入两张传输 IC 卡，将传输公钥导入到两张 IC 卡中；
5) 公钥导出完成。

1.3 对称密钥导出

对称密钥导出的加密机操作要求如下：

1) 密钥管理员登录（采用授权 IC 卡鉴权，IC 卡需提供口令验证机制以及口令错误锁定机制）；
2) 选择对称密钥导出操作，在加密机操作界面上输入需要导出的密钥个数，然后输入每个密钥的索引号和版本号；
3) 分别插入两张 IC 卡，并验证 IC 卡口令，若验证通过则转到下一步，失败则退出。加密机对待导出密钥进行加密，分别写入两张卡片（传输公钥从 IC 卡中读出）；
4) 对称密钥导出完成。

1.4 对称密钥导入

对称密钥导出的加密机操作要求如下：

1) 密钥管理员登录（采用授权 IC 卡鉴权，IC 卡需提供口令验证机制以及口令错误锁定机制）；
2) 选择对称密钥导入操作，在加密机操作界面上输入传输私钥的索引号和版本号；
3) 根据提示插入传输 IC 卡，并验证 IC 卡口令，若验证通过则转到下一步，失败则退出。对于每张传输 IC 卡分别读取卡内的密钥信息，两张卡片的信息读取完毕后，针对传输卡内每个密钥标识，加密机提示输入加密机内对应的密钥的索引和版本号；加密机完成密钥解密并判断密钥校验值后，将相应密钥写入加密机；

4) 对称密钥导入完成。

1.5 公钥导入

公钥导入的加密机操作要求如下：

1) 密钥管理员登录（采用授权 IC 卡鉴权，IC 卡需提供口令验证机制以及口令错误锁定机制）；
2) 选择公钥导入操作，根据提示插入传输 IC 卡，并验证 IC 卡口令，若验证通过则转到下一步，失败则退出。加密机读取 IC 卡内的公钥，提示输入导入加密机的公钥的索引和版本号，加密机将相应密钥写入加密机；
3) 公钥导入完成。

2、密码应用

支持加密/解密、MAC 生成及验证、数字签名及验证等功能，具体应遵循业务系统定义的 API 接口。

3、管理监控要求

加密机可以提供相关的管理监控能力，包括可以监控如下各类信息：

1) 加密机状态【正常、故障等】;
2) 加密机当前连接数；
3) 加密机 CPU 资源占用百分比；
4) 加密机内存占用百分比。

用户可以根据需求添加需要监控的指标，并可设置邮件自动发送服务，把监控信息发送指定邮箱。

通过监控界面，可以详细的列出当前加密机中业务状态情况。

4、审计功能要求

要求管理软件对加密机的操作记录相应的审计日志，可以通过加密机审计功能对加密机的所有管理操作进行审计，查看管理员及操作人员对加密机进行的操作动作，审计记录内容包括：

1) 用户登录、口令修改、用户增减等权限管理操作；
2) 修改设备配置、网络配置等系统管理操作；
3) 密钥初始化、对称密钥管理、非对称密钥管理、密钥备份等密钥管理操作，包括具体的密钥生成、密钥删除、密钥导出、密钥导入等操作；
4) 设置白名单、修改服务配置、启动服务、停止服务等服务管理操作。

三、技术指标

现场写卡系统加密机的技术要求如下表所示：

指标项	指标要求
通信协议要求	通信接口协议，要求支持 TCP/IP
	最大并发连接数，要求≥1024
密码算法要求	对称算法：SM1、SM4、DES/3DES、AES
	非对称算法：SM2、RSA（1024-4096）
	摘要算法：SM3、MD5、SHA1、SHA256、SHA384、SHA512
功能要求	国产密码算法：支持国产 SM1 分组算法、SM2 非对称算法、和 SM3 摘要算法及 SM4 对称算法
	通用密码算法：对称算法支持 DES/3DES，AES，非对称算法支持 RSA（1024～4096 比特），摘要算法支持 MD5、SHA1、SHA224/256/384/512 等常用算法
	数据加密/解密：支持国产 SM1、SM4 分组密码算法。支持国际通用算法（对称算法：DES/3DES，AES，非对称算法 RSA。）
	消息鉴别：支持 MAC/HMAC/TAC 的产生和验证
	数字签名/验证：支持 1024～4096 bit RSA 公钥密码算法
	支持多种 PIN 格式的加密和转换。包括 ANSI X9.8 格式即 ISO 95641－格式 0，Docutel 格式，Diebold 和 IBM 格式，ISO 95641－格式 1
	真随机数产生功能。使用硬件产生随机数，产生的随机数符合国家密码管理局颁布的《随机数检测规范》。 支持双物理随机源，符合《商用密码产品随机数检测要求》
	具有打印密码信封功能，支持打印机
标准要求	ANSI X3.92 数据加密算法
	ANSI X9.52 三重数据加密算法，操作模式
	ANSI X3.106 数据加密算法，操作模式
	ANSI X9.9 信息鉴别
	ANSI X9.8 PIN 的管理与安全
	ANSI X9.17 密钥管理
	ANSI X9.19 零售金融信息的鉴别
	多种 ATM 机用户 PIN 块格式：ISO 9564 1 – 格式 0/1/2/3
	中国人民银行金融 IC 卡规范，PBOC3.0； 即智能 IC 卡符合《中国金融集成电路(IC 卡)规范》第七部分应用安全规范
	银联联网联合规范 2.0
	EMV2000 规范
	GlobalPlatform 卡规范

配置要求	具有 2 个 100M/1000M 自适应以太网接口
	具有 1 个 IC 卡插口
	提供配套的密钥管理卡片
	支持 19 英寸标准机架
密钥存储要求	≥64KB
	RSA 密钥存储 100 对
	SM2 密钥存储 100 对
	对称密钥存储 4096 条
性能要求	RSA1024 大于 30 对/秒
	RSA2048 大于 5 对/秒
	SM2 大于 4900 对/秒
	随机数生成速率大于 20Mbps
	RSA1024 签名速率大于 4000 次/秒
	RSA1024 验签速率大于 20000 次/秒
	RSA2048 签名速率大于 500 次/秒
	RSA2048 验签速率大于 10000 次/秒
	SM2 签名速率大于 6000 次/秒
	SM2 验签速率大于 5000 次/秒
	SM2 加密速率大于 4000 次/秒
	SM2 解密速率大于 5000 次/秒
	SM1 加解密速率大于 100Mbps
	SM3 摘要运算速率大于 300Mbps
	SM4 加解密速率大于 100Mbps
	3DES 加解密速率大于 100Mbps
	AES 加解密速率大于 100Mbps
可靠性指标	平均无故障时间 MTBF 大于等于 30000 小时
	密码机支持多机热备功能，可以为应用提供高可用性密码服务。 1、密码机目前提供 API 接口的实现方式，在 API 接口中实现多机并行控制机制，可以实现客户端访问密码服务时的负载均衡、故障切换和断链修复功能，切换和修复时间都在毫秒的量级。 2、多机并行部署时，密钥通过备份恢复的方式保持多机的密钥同步。 3、对于 API 接口应用方式的集群中动态添加密码机时，仅需在客户端的配置文件中增加新密码机的 IP 地址即可。 4、同时也支持通过第三方集群软件或设备实现 HA 功能。

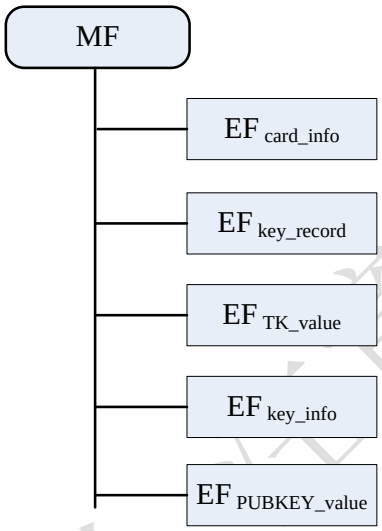
附录 F 密钥传输卡技术要求

密钥传输卡是一张标准的 IC 卡，其物理和电气特性应符合 ISO7816-1、ISO7816-2、ISO7816-3 规范的要求。

本规范中将针对传输卡中的文件结构及接口指令进行定义。

一、传输卡文件结构

卡片文件结构如下：



MF 下包括 4 个文件，说明如下：

文件名称	说明
卡片信息文件（card_info）	该文件存储卡片相关信息
密钥记录文件（key_record）	该文件存储工作密钥（即接收方需要导入的密钥）密文信息
传输密钥文件（TK_value）	该文件存储传输密钥密文信息
公钥文件（PUBKEY_value）	该文件存储传输公钥值
密钥信息文件（key_info）	密钥的数量及长度说明

1、卡片信息文件

文件标识		‘0001’
文件类型		透明文件
文件大小		60
文件存取控制	读/写 = 校验口令	
位置	**数据元**	**长度（Byte）**
0-7	卡片序列号	8
8	A/B 卡标识	1

9-16	卡片校验信息	8
17-18	机构标识	2
19-59	保留	41

数据元说明：

- 卡片序列号：卡片的唯一标识，编码方式为：卡商编号（1 字节）+年份（2 字节）+流水号（5 字节）
- A/B 卡标识：标识该卡片是 A 或 B 卡，01-A 卡，02-B 卡
- 卡片校验信息：采用 PIN 作为 DES 密钥，加密的 8 字节秘密信息
- 机构标识：机构类型（1 字节）+机构代码（1 字节），用于标识密钥发送机构，包括省公司、卡商、一级卡数据生成系统等，编码方式见附录
- 保留

2、密钥记录文件

文件标识		‘0002’
文件类型		记录
文件大小		记录数 128 个
文件存取控制	读/写 = 校验口令	
位置	**数据元**	**长度（Byte）**
0	密钥 1 传输算法标识	1
1	密钥 1 密钥标识	1
2-17	密钥 1 密文	16
18-21	密钥 1 传输 MAC	4

数据元说明：

- 传输算法标识：

0x00—标识 SM1 算法

- 密钥标识：

该标识用于传输密钥双方标识具体的传输密钥，该标识的范围是 01~FF

- 密文

加密的密钥数据，加密机生成 16 字节随机数作为分量 1，随机数与待加密密钥异或产生分量 2，两个分量分别加密存储在两张卡中

- 传输 MAC

为了保证密钥传输过程的完整性，传出方加密机对密钥计算的校验码。MAC 计算采用标准的 3DES-CBC MAC 算法。初始向量为 8 字节全零，对 8 字节 0 进行 MAC 计算，取结果的前 4 字节作为传输 MAC

3、随机传输密钥文件

文件标识	‘0003’

文件类型		二进制
文件大小		180
文件存取控制	读/写 = 校验口令	
位置	**数据元**	**长度（Byte）**
0	算法标识	1
1-2	后续数据总长度	2
3	随机传输密钥明文长度	1
4-179	随机传输密钥值	176

说明：

- 算法标识：
  0x00 – RSA1408
- 后续数据总长度：包括后续两个字段（随机传输密钥长度、随机传输密钥值）的总长度
- 随机传输密钥明文长度：该字段定义随机传输密钥的明文长度
- 随机传输密钥值：随机传输密钥的密文值分量。加密机生成 16 字节随机数作为分量 1，随机数与随机传输密钥异或产生分量 2，两个分量分别采用传输公钥加密存储在两张卡中

4、公钥文件

文件标识		‘0004’
文件类型		二进制
文件大小		512
文件存取控制	读/写 = 校验口令	
位置	**数据元**	**长度（Byte）**
0	公钥类型	1
1-176	模	176
177-179	指数	3
180-183	验证信息	4
184-511	保留	328

说明：

- 公钥类型：
  0x00 – RSA1408
- 模数：1048Bit 的模数分量

  加密机随机生成 176 字节数据作为分量 1，随机数与公钥模数异或产生分量 2，两个分量分别存储在两张 IC 卡中。
- 指数：65537（两张卡相同）
- 验证信息：用 16 字节的 0x00 作为 3DES 密钥，用模数+指数（采用真实的模数+指数作为输入数据，而不是分量）作为 3DES 算法的明文输入数据，进行 3DES-CBC 的 MAC 计算，以“0x00 00 00 00 00 00 00 00”为初始向量。如果明文数据是 8 的整数倍，则补“0x80 00 00 00 00 00 00 00”,否则在其后填充 0x80（当需要填充一个字节时）或 0x80,0x00…直至明文数据长度为 8 的整数倍，取计算结果的前 4 字

节作为校验信息，两张卡中的校验信息相同。

- 保留

5、密钥信息文件

文件标识		‘0005’
文件类型		二进制
文件大小		2
文件存取控制	读/写 = 校验口令	
位置	**数据元**	**长度（Byte）**
0	密钥数量	1
1	记录长度	1

二、APDU 指令定义

1、校验 PIN（Verify PIN）

1) 定义和范围

Verify 命令用于校验命令数据域的个人密码的正确性。除了 PIN 操作指令外，其它所有指令均需要校验 PIN 成功后才可以执行。

2) 命令报文

Verify 命令报文编码如下：

代码	值
CLA	00
INS	20
P1	00
P2	00
Lc	08
DATA	外部输入的人个密码

3) 命令报文数据域

命令报文数据域由持卡者输入的个人密码组成。

- 若校验成功，错误允许计数器被置成初始值。若校验错误，则可试次数减 1；
- PIN 校验失败时，IC 卡将回送 SW1 SW2＝63CX，X 表示允许重试的次数。当卡回送 63C0 时，表示不能重试，此时再使用校验命令时，将回送失败状态码‘6983’；
- PIN 失败尝试次数初始值设置为 6，如果失败超过该次数，则卡片锁定并不能恢复（后续需要做销毁操作），成功的 PIN 输入应该清除失败次数的记录；

4) 响应报文数据域

响应报文数据域不存在。

5) 响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
63 CX	校验失败，X 表示允许重试的次数
67 00	长度错误
6A 86	P1 或 P2 不正确
6D 00	不正确的 INS
6E 00	不正确的 CLASS
93 02	应用永久锁定

2、修改 PIN（Change PIN）

1) 定义和范围

Change PIN 允许持卡人将指定个人密码修改为新的密码。当 Change PIN 命令成功完成后，卡片要进行以下操作：

①PIN 尝试计数器复位至尝试次数上限；

②将指定个人密码置为新的个人密码。

2) 命令报文

Change PIN 命令报文编码如下：

代码	值
CLA	00
INS	24
P1	00
P2	00
Lc	11
DATA	当前的 PIN || 'FF' || 新的 PIN

3) 命令报文数据域

命令报文数据域为当前的 PIN || 'FF' || 新的 PIN。只有当前的 PIN 验证通过，才可以完成 PIN 的修改。PIN 的验证过程与 Verify PIN 指令相同。

4) 响应报文数据域

响应报文数据域不存在。

5) 响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
63 CX	X 表示允许重试的次数
69 82	不满足安全状态
69 83	验证方法锁定
6A 81	功能不支持(无 MF 或卡片已锁死)
6A 82	未找到文件

3、选择指令（Select File）

1) 定义和范围

Select File 命令用于选择 IC 卡中的文件。

2) 命令报文

Select File 命令报文编码如下：

代码	值
CLA	00
INS	A4
P1	00-按文件标识符选择 MF 或 EF
P2	00- 第一个或仅有的一个 02-下一个
Lc	XX
DATA	文件标识符

3) 命令报文数据域

命令报文数据域为文件标识符或文件名称。

4) 响应报文数据域

应答报文数据域包括所选择的 MF 或 EF 的文件控制信息 FCI。

MF 回送的文件控制信息 FCI：

标志	值	存在方式
6F	文件控制信息模板	必备
84	DF 名	必备
A5	文件控制信息专用模板	必备
88	目录基本文件的短文件标识符	必备

EF 回送的文件控制信息 FCI：

标志	值	存在方式
6F	文件控制信息模板	必备
A5	文件控制信息专用数据	必备
9F 0C	EF 文件控制信息（含文件标识符、类型、长度）	必备

5) 响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
61XX	命令正确执行
67 00	数据长度错误
6A 81	不支持此功能(无 MF 或应用已锁)
6A 82	未找到文件
6A 86	参数 P1 P2 不正确

4、读二进制文件（Read Binary）

1) 定义和范围

Read Binary 命令用于读取二进制文件的内容。

2) 命令报文

Read Binary 命令报文编码如下：

代码	值
CLA	00
INS	B0
P1	XX
P2	XX
Le	XX

- P1 的最高位不为 1，则 P1 P2 为欲读文件的偏移量，所读文件为当前文件。
- Le 表示要读取的字节数，若 Le 为 00，则送回警告状态 6C XX，请求 Le 置为 XX 并重发该命令。

3) 命令报文数据域

命令报文数据域不存在。

4) 响应报文数据域

应答报文数据域的内容为读出的二进制文件的内容。

5) 响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
69 81	不是二进制文件
69 82	不满足安全条件
6A 81	不支持此功能
6A 82	未找到文件
6B 00	参数错误(偏移地址超出了 EF)
6C XX	长度错误（Le 不正确，‘XX’表示实际长度）

5、写二进制文件（Update Binary）

1) 定义和范围

Update Binary 命令用于以密文或明文的形式修改二进制文件。

2) 命令报文

Update Binary 命令报文编码如下：

代码	值
CLA	00
INS	D6
P1	XX
P2	XX
Lc	XX

DATA	写入的数据

参数说明：P1 的最高位为 0，P1 P2 为欲写文件的偏移量，所写文件为当前文件。

3) 命令报文数据域

命令报文数据域包括更新原有数据的新数据。

4) 响应报文数据域

响应报文数据域不存在。

5) 响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
65 81	写 EEPROM 失败
67 00	长度错误
69 81	不是二进制文件
69 82	写的条件不满足
6A 82	未找到文件
6A 86	P1 或 P2 不正确
6D 00	不正确的 INS
6E 00	不正确的 CLASS
93 02	应用永久锁定

6、读记录文件（Read Record）

1) 定义和范围

Read Record 命令用于读取记录文件的内容

2) 命令报文

Read Record 命令报文编码如下：

代码	值
CLA	00
INS	B2
P1	记录号
P2	XX
Le	表示要读的字节数

- P1 为记录号，如果文件有 N 个记录，则 P1 可取为 1-N。
- P2 的低 3 位为 100，若高 5 位不为 00000 表示短文件标识符，否则表示当前文件。

3) 命令报文数据域

命令报文数据域不存在。

4) 响应报文数据域

所有执行成功的 Read Record 命令的响应报文数据域由读取的记录组成。

5) 响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
69 81	文件类型错误
69 82	读的条件不满足
69 86	不满足命令执行条件（无当前 EF）
6A 81	不支持此功能
6A 82	未找到文件
6A 83	未找到记录
6C XX	长度错误（Le 不正确，‘XX’表示实际长度）

7、更新记录文件（Update Record）

1) 定义和范围

Update Record 命令用于修改记录文件。

2) 命令报文

Update Record 命令报文编码如下：

代码	值
CLA	00
INS	DC
P1	= 00 当前记录 ≠00 指定的记录号
P2	XX
Lc	后续数据域的长度
DATA	更新原有记录的新记录

参数说明：P2 的低 3 位为 100，如果高 5 位不为 00000 则表示短文件标识符，否则表示当前文件。本命令可操作的三种记录文件被选择后当前记录都是第一条记录。

3) 命令报文数据域

命令报文数据域包括由更新原有记录的新记录组成。

4) 响应报文数据域

响应报文数据域不存在。

5) 响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
65 81	写 EEPROM 失败
67 00	长度错误
69 81	当前文件不是线性定长文件或线性变长文件
69 82	写的条件不满足
6A 82	未找到文件
6A 83	未找到记录
6A 84	文件中存储空间不够

6A 86	P1 或 P2 不正确
6D 00	不正确的 INS
6E 00	不正确的 CLASS
93 02	应用永久锁定

三、密钥说明

- 传输公私钥对：

  RSA 公私钥对，模长为 1408Bit。接收方需要将传输公钥提供给密钥发送方。密钥发送方加密机采用采用接收方的传输公钥对随机传输密钥进行加密（采用 RSA1408），加密填充方式为 PKCS1。

- 随机传输密钥（TK）：

  该密钥为 SM1 密钥，长度为 128Bit。

四、IC 卡操作指令流程

密钥传输流程中，加密机对传输 IC 卡的操作步骤包括如下四个流程：

- 公钥导出到 IC 卡
- 对称密钥导出到 IC 卡
- IC 卡中对称密钥导入到加密机
- IC 卡中的公钥导入到加密机

1、公钥导出到 IC 卡

密钥管理员操作加密机界面，导出公钥到 IC 卡，并输入公钥索引和版本信息。加密机提示分别插入两张 IC 卡，对于每张传输卡加密机按照如下指令流程完成导出公钥操作。

第一步：修改 PIN（设置新的 PIN 码）

00 24 00 00 11 [原 PIN 码+'FF'+新 PIN 码]

第二步：校验新 PIN

00 20 00 00 08 [新 PIN 码]

第三步：将本地公钥及自签名信息写入 00 04 文件（公钥文件）

加密机计算校验信息，然后通过 1 条或多条如下所示的写卡指令将公钥和校验信息写入文件：

00 D6 00 00 XX [文件内容]

第四步：加密机计算卡片校验信息写入卡片

加密机采用新的 PIN 码作为 DES 密钥加密 8 字节全 0，得到的数据写入卡片信息文件（0001）的【卡片校验信息】字段，其它字段不变，指令如下：

00 D6 00 09 08 [卡片校验信息]

2、对称密钥导出到 IC 卡

密钥管理员操作加密机，按照提示输入需要导出的密钥数量及每个密钥的索引号和版本号，然后分别插入两张传输卡，对于每张传输卡，指令流程如下：

第一步：校验 PIN

00 20 00 00 08 [PIN 码]

第二步：读取 00 01 文件（卡片信息文件）

00 B0 00 00 3C

采用 PIN 码对【卡片校验信息】字段进行校验，如果校验通过，继续下一步，否则终止操作。

第三步：加密机读取卡片中的公钥文件，并对公钥进行校验：

通过 1 条或多条 00B0 指令读取公钥及校验信息，两张 IC 卡中的公钥分量读取完毕后，将两个分量异或操作，并按照要求对公钥进行验证：

00 B0 XX XX XX

第四步：加密机生成随机密钥并加密导出密钥：

加密机随机生成 SM1 密钥（16 字节），加密机生成 16 字节随机数作为分量 1，随机数与 SM1 密钥异或产生分量 2，两个分量分别采用第三步中读取的传输公钥加密，分别存储到两张传输卡内（随机传输密钥文件，0003）：指令如下：

00 D6 00 00 B4 [密文数据]

第五步：写入密钥记录文件（0002）

针对每个待导出密钥，由加密机生成 16 字节随机数作为分量 1，随机数与待导出密钥异或产生分量 2，两个分量分别采用 SM1 密钥加密后，执行如下指令将分量 1 写入 IC 卡 1（提示插入 IC 卡 B 后，将分量 2 写入 IC 卡）：

00 DC 01 04 16 [记录 01（密钥 1 分量 1 密文及相关参数）]

00 DC 02 04 16 [记录 02（密钥 2 分量 1 密文及相关参数）]

….

00 DC XX 04 16 [记录 XX（密钥 XX 分量 1 密文及相关参数）]

第六步：更新密钥信息文件（0005）

更新 0005 文件，将待传输密钥数量（1 字节）写入偏移 01 位置

00 D6 00 00 01 XX

3、IC 卡中对称密钥导入到加密机

按照加密机的提示，输入传输私钥的索引和版本号，然后按如下流程执行：

第一步：校验 PIN

00 20 00 00 08 [PIN 码]

第二步：读取 00 01 文件（卡片信息文件）

00 B0 00 00 3C

采用 PIN 码对【卡片校验信息】字段进行校验，如果校验通过，继续下一步，否则终止操作。

第三步：读取密钥信息文件（00 05）

读取密钥信息文件中的密钥数量信息：

00 B0 00 00 01

按照加密机提示分别输入传输卡中密钥导入加密机后的索引号和版本号。

第四步：读取随机传输密钥文件（0003）

加密机读取随机传输密钥文件中的随机传输密钥密文，并采用传输私钥解密出随机传输密钥分量，两张卡片读取完成后，两个分量异或后得到随机传输密钥（SM1 密钥）。

00 B0 00 00 B4

第五步：读取密钥记录文件（0002）

00 B2 01 04 16　　// 读取第 01 条记录中的密钥密文

00 B2 02 04 16　　// 读取第 02 条记录中的密钥密文

….

00 B2 XX 04 16　　// 读取第 XX 条记录中的密钥密文

加密机读取两张卡片的密钥记录文件后，采用随机传输密钥解密每个密钥记录中的密钥密文后，将两个分量异或，得到每个密钥，然后按照输入的参数导入到加密机。

4、IC 卡中公钥导入到加密机

按照加密机的提示，按如下流程执行：

第一步：校验 PIN

00 20 00 00 08 [PIN 码]

第二步：读取 00 01 文件（卡片信息文件）

00 B0 00 00 3C

采用 PIN 码对【卡片校验信息】字段进行校验，如果校验通过，继续下一步，否则终止操作。

第三步：加密机读取卡片中的公钥文件，并对公钥进行校验：

通过 1 条或多条 00B0 指令读取公钥及校验信息，两张 IC 卡中的公钥分量读取完毕后，将两个分量异或操作，并按照要求对公钥进行验证：

00 B0 XX XX XX

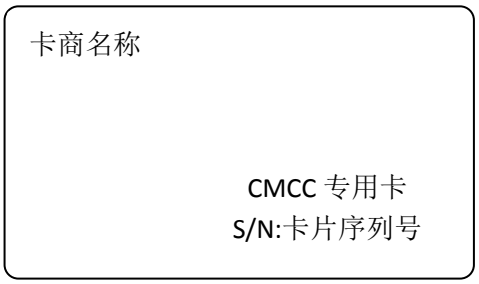
第四步：公钥导入加密机

加密机提示输入要导入的公钥的索引和版本号，按照输入的索引和版本号将公钥导入加密机。

五、传输卡初始化说明

卡商成套提供白卡，每套两张卡，分别写入相应的标识信息，并按要求初始化卡片序列号（卡片序列号，每卡唯一），初始 PIN 均设置为”00000000”。

卡面印刷要求：



六、机构标识

机构标识包括：机构类型+机构代码

机构类型：

00：中国移动集团

机构代码，00：一级卡数据生成系统

01：中国移动省公司

机构代码即为省公司编码，见附录 C

02：卡商

机构代码即为卡商编码，见附录 A