3G 手机卡 USAT 功能测试

摘 要

USAT 技术是在原来 SIM 卡被动式的操作模式基础上，增加了 SIM 卡新的主动式操作的能力，即允许 SIM 卡中的应用和服务主动与手机终端进行交互操作。

在 USAT 技术获得广泛应用之前，手机与 SIM 卡之间是一种不对称的主从关系，即 SIM 卡只能处于被动的接受手机的指令并执行的地位，手机则处于绝对的主动控制地位。任何一个动作只能由手机发起命令，并由 SIM 卡响应来完成。这种命令——响应的动作模式最大的缺陷在于 SIM 卡不具有主动权，从而限制了在 SIM 卡上的开发，制约了新的移动增值业务的发展。而 USAT 可以为 SIM 卡的增值业务提供了良好的开发环境，可在 SIM 卡中设计功能丰富、操作简便的菜单，使用户可以用可视化、交互式的手段享受移动运营商提供的增值业务。

当前 3G 网络相关技术逐渐成熟，即将在中国商业运营，3G 网络设备的测试工作也随之深入展开。中国从 GSM 时代就开始采用智能卡作为用户身份校验和部分增值业务的平台，同样在 3G 网络中也需要智能卡，而且还要保证增值业务从 2G 向 3G 平滑过渡。此外由于国内运营商对 3G 相关规范的广泛参与和掌握，他们也会提出一些针对国内特殊需求的 3G 功能，这些都需要针对 3G 使用的卡片进行完整的测试。本课题根据上述需求，通过模拟仿真，实现 3G 卡片的 USAT 功能测试。

关键词 USAT USIM TPDU CMPP

USAT FUNCTION TESTING FOR 3G MOBILE PHONE CARDS

ABSTRACT

USAT technology bases on the original model of SIM cards passive operations and adds proactive SIM function, which gives a mechanism whereby the SIM can initiate interactions to be taken by the ME.

Before USAT technology widely available, it is an asymmetry between mobile phones and SIM cards, which mean that SIM cards can only receive the commands from the ME. The ME is at the absolute control position, and all actions can only be initiated by the phone and executed by the SIM cards. The biggest shortcoming of such action mode is that the SIM cards are all passives, thereby restricting the possibilities of opening up and using new mobile value-added services on the SIM cards.

As technology related to the 3G network in China will gradually become mature and commercial operation, 3G network equipment start-depth testing. Since China began to use smart cards as GSM User Identity Verification and as part of value-added business platform. Then that will the same in the 3G network, and smooth transition from 2G to 3G will also be ensured。Further more, with the abroad participating in and the mastering relevant norms, the domestic 3G operators bring forward some requirements in view of the special needs of our country. All these require the use of the cards for 3G integrity tests. According to the above demand, this topic discussed the function of simulation testing 3G USAT card technology, in order to achieve the USAT functional full testing.

KEY WORDS: USAT USIM TPDU CMPP

独创性（或创新性）声明

本人声明所呈交的论文是本人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得北京邮电大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

申请学位论文与资料若有不实之处，本人承担一切相关责任。

本人签名：刘伸 日期：2007年3月29日

关于论文使用授权的说明

学位论文作者完全了解北京邮电大学有关保留和使用学位论文的规定，即：研究生在校攻读学位期间论文工作的知识产权单位属北京邮电大学。学校有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许学位论文被查阅和借阅；学校可以公布学位论文的全部或部分内容，可以允许采用影印、缩印或其它复制手段保存、汇编学位论文。（保密的学位论文在解密后遵守此规定）

保密论文注释：本学位论文属于保密在__年解密后适用本授权书。非保密论文注释：本学位论文不属于保密范围，适用本授权书。

本人签名：刘伸 日期：2007年3月29日

导师签名：刘宏 日期：2007.4.2

第一章 绪论

数字蜂窝移动通信系统（GSM）是当前全球许多国家都支持和采用的一种数字蜂窝移动通信系统，是目前世界上最成熟的数字移动通信系统，它具有较完善的技术规范和标准。并且 GSM 数字移动电话系统还开辟出许多新业务，如语音信箱、短信息业务、呼叫转移、多方通话，甚至还可以进行传真和数据通信，为移动的发展提供了一个崭新天地。

80 年代初期以数字处理器为基础的智能卡便在移动通信领域中应用。当时欧洲有些国家讨论要在模拟移动通信网中采用 IC 卡。而此时，欧洲正在讨论建立新的数字移动通信标准，以便为用户提供国际漫游。因此，在新的数字移动通信系统中采用 IC 卡技术，很自然地被列入了移动通信系统（即 GSM 系统）的技术标准中，并将这种 IC 卡称作用户识别模块——SIM 卡。它提供两个方面的功能：业务的保密接入性能和数据的可移植性。

SIM 卡是 GSM 系统中不可缺少的一个重要组成部分，是 GSM 系统移动台的两基本构成部分之一。在 SIM 卡中，包含有用户识别信息、辅助业务信息、短信息、移动性信息和无线电资源信息等。只有插入 SIM 卡后，移动终端才能进网，而在没有 SIM 卡的情况下，移动终端只能拨 112 等急救号码。

SIM 卡是可拆装的，当要发送或接收呼叫时，用户可将 SIM 卡插入电话中，当用户需要使用其它的 GSM 终端时，可以方便地将其取下，插入到相应的 GSM 终端上。通过 SIM 卡物理接口、逻辑接口的明确定义，可以完成移动终端的连接和信息交换，同时还要在 SIM 卡内部进行用户信息存储，执行鉴权算法和产生加密钥等工作。用户通过由移动终端人机接口输人的 PIN 码向 SIM 卡证实其使用权，移动终端将 PIN 送到 SIM 卡，并由 SIM 卡与其内部所存的号码作比较。比较通过后，SIM 卡转换状态，才允许移动终端接通无线接口。

在不同 GSM 网络之间的漫游协议达成之后，用户可在不同的 GSM 网络中使用同一张 SIM，只需带 SIM 卡，租用手机即可进行通信。SIM 卡的采用，必将改变人们的传统观念，即从“我拥有手机”改变为“我拥有卡”。此外，SIM 卡使用户及其通信都与具体的终端设备无关，这种不相关性与智能网相结合，为在网络中和网络间实现个人通信提供了保证。

1.1 卡的发展

1.1.1 SIM 卡

SIM 卡即用户识别卡，该卡片内记录数字移动电话用户的个人资料信息，通过这些资料，可以对无线通信进行鉴权和加密。鉴权的作用是保护网络，防止非法盗用。同时通过拒绝假冒合法用户的“入侵”，从而保护 GSM 网络用户。

SIM 卡就是用来对用户信息存储和网络身份鉴权，其主要业务应用是 GSM 基本电信业务。

1.1.2 STK 卡

STK 是 SIM Tool Kit 的英文缩写，即“用户识别应用开发工具”。它包含一组指令用于手机与 SIM 卡的交互，这样可以使 SIM 卡运行卡内的小应用程序，实现增值服务。

STK 卡与普通 SIM 卡的区别在于：在 STK 卡中固化了应用程序。通过软件激活提供给用户一个文字菜单界面。这个文字菜单界面允许用户通过简单的按键操作就可实现信息检索，甚至交易。另外 STK 通过固化在卡中的程序，可以使用户不必记忆命令代码和服务平台号，达到了方便用户的目的。

其主要功能是支持用户信息存储和网络身份鉴权，以及符合 GSM11.14 规范，支持各种 STK 移动增值应用。

业务主要可以应用在基本电信业务，比如移动增值服务，如移动梦网、动感地带、移动银行、天气预报、位置服务等。

1.1.3 USIM 卡

在 3G 系统的核心，通用移动通信系统（Universal Mobile Telecommunication System ,UMTS）中的用户服务识别模块 USIM （User Service Identity Module）是实现通信服务最关键的因素。

USIM 是用户获得 3G 服务的关键，是安全性的保障，就如同个人身份识别模块 SIM 卡一样，能安全地存储用户私人信息，并执行加密算法。SIM 卡和 USIM 卡都是防篡改的智能卡，可确保网络和私人数据的安全。加密算法则是提供了一种鉴权机制，只有鉴权之后的服务才能获得网络资源，并享受网络服务。

其功能特点是支持新的 3GPP 认证方案，包括双向认证、可定制算法、可变密钥长度，以及 MILENAGE 算法功能，这使运营商在实施安全策略中获得前所未有的灵

活性；同时通过新文件系统设计实现了真正的多应用功能。因此，相同的卡可以同时运行 3G USIM 应用和 2G SIM 应用，或任何其他智能卡应用。并且有高级、灵活的安全性管理：可针对任何文件修改访问权限，甚至在发行卡后可提供多个 PIN 代码。另外高级电话簿可以为最终用户提供能够与其它设备保持同步的个人数据库功能。最后它还提供一个开放式环境：USIM 应用工具包(USAT)、WAP 识别模块以及 PKI 密码功能，这些能够为一流电子服务的开发提供安全、全面的执行平台。

虽然 3G 的应用还未全面展开，但俗话说："兵马未动，粮草先行"，这个"粮草"就包括了未来 3G 手机要用到的 USIM 卡，USIM 卡拥有与 SIM 卡相同的物理特性。但是它最少支持一个 USIM 卡的网络应用，并且在 3G 系统里，一张 USIM 卡可以拥有用户的一套或多套信息。此外，对于特定的卡片信息可以实施安全的空中管理。

1.2 卡系统简介

从开始使用到最近一段时间，SIM卡都是一个8位的控制器，但是SIM卡中的内存数量却一直在增长，最初只是由256字节的RAM和3K字节的EPROM组成，目前的RAM已经增长到1024字节，EPROM也增长到32K字节。SIM卡使用的所有软件：操作系统、文件处理系统和APDU的代码，都被烧入固化在32K或64K字节大小的ROM中。80多个数据文件则保存在EEPROM中，RAM则被用作SIM卡与手机之间的通信的I/O缓冲区。

1.2.1 SIM 卡逻辑结构图

无论哪个厂商哪个系列的产品，SIM 卡的逻辑结构都基本类似，见下图[1]：

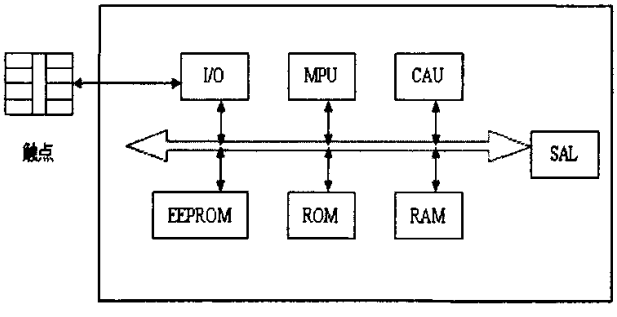


图 1-1 SIM 卡逻辑结构图

- I/O 接口是芯片与外界联系的唯一通道；
- 微处理器（MPU）是 SIM 卡的核心，在功能上类似于 PC 机的 CPU，完成基本的指令执行、存储控制和逻辑控制等；

- CAU 是加密协处理器，功能是完成一些常用算法，例如奇偶校验、非对称密钥的相关算法等；
- EEPROM：电可擦可编程只读存储器，主要用来存储数据，还可以存放部分代码，使其直接在 EEPROM 空间中执行；
- 只读存储器（ROM）存储 COS 代码和一些基本常数，在芯片的掩模阶段这些代码和数据一起写入，在使用阶段就不能进行更改；
- 随机读写存储器（RAM）是卡片使用阶段的临时数据空间，在卡片每次复位时自动清零，掉电以后数据也全部丢失；
- 安全访问逻辑（SAL）是芯片自定义的一些硬件安全逻辑。

1.2.2 文件系统简介

SIM 卡用户存储器中保存有 SIM 卡文件，用户的管理信息，应用的数据，以及其他信息都是存储在 SIM 卡中的这个文件系统中。

1. SIM卡文件的组织形式

SIM卡中的数据在用户存储器中以树型文件结构的组织形式存放。按照文件的等级，由高到低可以分为：主文件（Master File，MF）、专用文件（Dedicated File，DF）和基本文件（Elementary File，EF）。SIM卡文件系统树型结构见下图[2]：

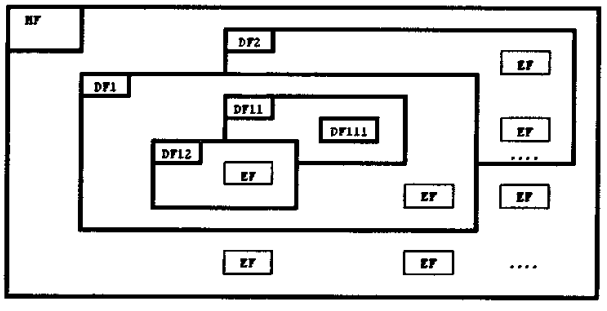


图 1-2 SIM 卡文件系统结构图

在文件系统中文件用文件ID唯一标示，每一个ID由2字节的16进制数字组成，其中第一个字节表明了文件的等级。在GSM中，‘3F’表明为MF，‘7F’表明为第一级的DF，‘5F’为第二级的DF，‘2F’则表明此文件为MF文件的EF子节点。

2. MF

在SIM卡的文件结构中，只能存在一个MF，并且MF随操作系统一起生成，用户无法控制。在文件存取过程中，不能越层存取，若想读写子专有文件下的文件，必须经过其高层文件逐层选取。

3. DF

在SIM卡的文件结构中，DF是MF的直接孩子节点，主要存在四个一等级的DF：

- DF_{GSM}：存储GSM和DCS 1800的应用文件；
- DF_{IS41}：存储ANSI T1P1中定义的IS-41应用；
- $DF_{TELECOM}$：存储电信服务；
- DF_{FP-CTS}：储存无线电话系统的应用。

4. EF

MF 和 DF 中仅有头部分，在 EF 中还有一个数据体部分，用来存储具体的数据信息。例如文件访问条件，文件大小，记录长度等。EF 虽然有 3 种格式，但是 ME 可以自己判断当前 EF 文件为哪一种类型。SIM 卡文件的数据结构有：透明结构（Transparent），线性定长结构（Linear Fixed）和循环结构（Cyclic）三种。

- 透明结构：包含一系列按次序排列的字节。利用相对地址对此文件进索引，其相对地址存放在首字节中，数据长度存放在 EF 文件头中；
- 线形定长结构：包含一系列相同固定长度的记录，第一个记录的记录号是 1，记录的长度以及它与记录总数的乘积都由文件头指出；
- 循环结构：循环结构以时间顺序存储记录。当所有记录都已存满时，下一个数据将覆盖最旧的信息。值得注意的是目前此类型文件所存储的数据长度不可以超出 255 个字节的长度[2] 。

1.3 3G 终端侧业务的实现技术

随着通信终端智能化程度的提高以及个性化业务需求的增长，在终端和应用服务器之间直接开设业务接口，可以使用户自由地按需调用业务。3G 的业务实现技术包含了网络侧和终端侧的所有的业务工具，它们是在 3G 系统中实现业务能力特征的手段。目前 3GPP 已经定义的终端侧业务工具包括：MExE 与 USAT。

1.3.1 MExE

MExE 即 Mobile Execution Environment，是 3GPP 定义的移动台执行环境标准，通过将一个 Java 虚拟机内置到移动电话中，允许通过编程实现复杂的业务。具有该标准能力的手机可以直接向网络运营商或第三方提供的 MExE 服务器发起业务请求，享用除一般通话以外的各种增值业务，特别是各类 Internet 业务。

未来 3G 的终端将是多功能的终端，3GPP 制定的移动终端应用执行环境技术 MExE，有助于移动终端对计算和娱乐业务的支持。MExE 使不同的移动终端可以在

存储、显示和计算能力的范围内，实现对 MExE 业务环境数据、Applet 和应用程序的支持，享受 MExE 业务。网络运营商或业务提供商可以利用 MExE 标准的 API 和工具箱实现标准的 MExE 业务。

1.3.2 USAT

USAT 即 USIM 卡应用工具包，是基于客户机/服务器模式工作的。在 USAT 相关规范中，短消息服务（SMS）是一个关键。网络运营商或业务提供商可以随时在服务器中发送内嵌于短信息中的程序，从而改变移动终端中的 USIM 信息。

USAT 具有很强的灵活性，允许随时对 USIM 卡信息进行更新，以便修改服务，并且可以通过无线方式下载新的服务。例如，网络运营商可以通过从服务器中发射嵌入在短信息中的代码来远程修改用户无线终端中的 USIM 信息。并且终端可以通过无线方式下载新的服务。另外因为 USIM 卡中存有个人化的信息，可以应用于那些安全级别要求较高的服务，如电子商务、银行业务等，可以实现与安全相关的身份认证。

USAT 提供的一套标准执行环境运行存储在 USIM 卡上，通过定义 USIM 卡和终端之间的应用编程接口，从而可以在 USIM 卡上直接开发小的业务应用程序。 同时 USAT 被许多移动终端制造商如 Nokia、Siemens、Alcatel 和 Motorola、Ericsson 等集成到手机中。

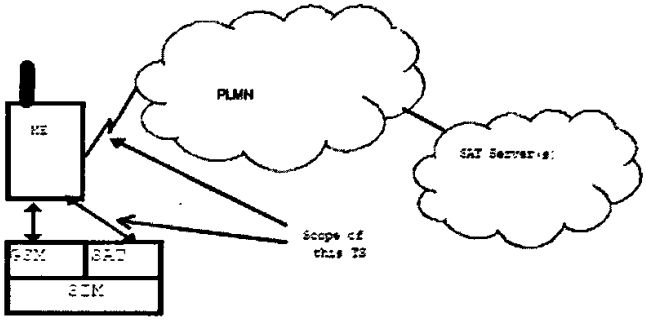


图 1-3 USAT 应用环境结构图

USIM卡的USAT具体应用，充分利用现有移动设备支持的功能，提供了一种允许应用存储到USIM，与移动设备ME进行交互操作的机制，重要的是USIM与ME之间的互操作性独立于厂商和操作者。并USAT还提供一种允许应用下载及修改的机制。

1.4 课题的意义及内容

1.4.1 课题的意义

随着通信技术的发展，移动通信的主体地位在通信市场中进一步加强，目前移动通信数据业务发展迅速，增长势头强劲，移动通信数据业务的研究自然也越来越重要。有吸引力的业务是拥有广大客户的基础！当前增值业务发展步伐进一步加快，增值业务的种类也日趋丰富，使用量迅速增长，成为移动运营商新增收入的重要组成部分，可见新的增值业务的研发是非常重要的。

目前我国存在 GSM 网络和 CDMA 网络，GSM 体系占据重要地位，可是随着 3G 牌照的发放，有可能将会出现更多的运营网络。那么在研发新业务的时候，就会出现因网络不同，而使得新业务的研发、调试存在困难。

本课题所研究的测试系统除了可以对 USAT 功能进行全面测试，还可以利用本系统进行一些新业务的研发、调试和测试。本测试系统将有线网络环境模拟无线网络环境，因屏蔽了无线网络环境，可以除去具体运营商网络的限制，不用区分网络所使用的技术，让 ME 端的短消息直接发送到 OTA Server 端，降低了新业务测试的难度和复杂度。此外通过此系统可以清晰观测到所使用的每一条命令的详细信息，包括执行后的结果，可以方便的比较数据的结果，这对新业务的调试有着很大的帮助。

1.4.2 课题的内容

本课题中描述的测试系统由两大部分组成：USAT 部分和网络部分。

USAT 部分完成对 USIM 卡的测试和操作，提供操作和管理卡的接口，支持 STK 功能测试、USAT 功能测试、脚本方式批量执行测试、单条指令测试等多种测试；并且，可以提供测试数据和测试结果保存、分析，检测卡是否满足执行条件；此外，还可以传递命令数据，显示卡执行过的每一条命令，以及显示详细的执行流程，以实现对 3G 手机卡进行全面 USAT 功能测试的目标。此部分的设计与实现主要参照 3GPP 中相关协议[2][3]，以及中国移动相应协议[6]。

网络部分则是模拟 USIM 卡与 OTA Server 之间的无线环境，通过卡与 OTA Server 之间的通信和指令的传递，实现基于 USAT 技术的一个应用。此部分设计与实现主要参照中国移动相应协议[4]。通过模拟卡与 OTA Server 之间的环境，网络部分主要实现了 USIM 卡与用户之间的操作，以及卡与 OTA Server 之间的透明/显示通信的两大功能，并且此部分还具备一定的调试与测试功能。用户可以通过软件界面与卡进行操作，比如菜单选择，短信发送；并且可以通过读卡器实现 USIM 卡和 OTA 服务器的交互

操作。

第二章　功能概述

2.1 功能模块

测试系统要分别完成与 USIM 卡和 OTA Server 之间的通信，并且确保 USIM 卡和 OTA Server 之间可以进行通信。测试软件与 USIM 卡部分主要使用 USAT 命令和协议，完成 USAT 功能，命名为 USAT 模块；测试软件与 OTA Server 部分主要使用 CMPP 命令与 OTA 命令，完成与 OTA Server 通信，命名为网络模块。测试系统结构见下图：

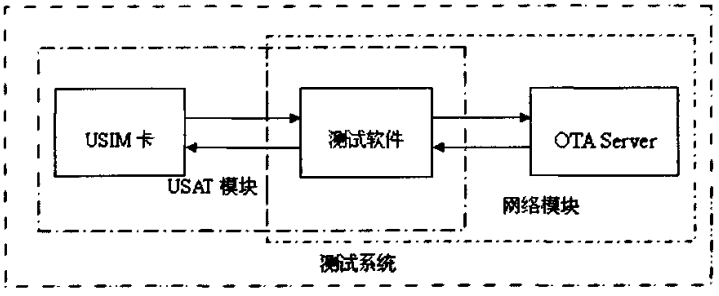


图 2-1 测试系统结构图

2.2 USAT 模块

USAT 模块实现测试系统与 USIM 卡之间通信，命令传递和数据交换。主要可实现的功能如下：

- 读取 USIM 卡内文件系统，根据协议规定，设计并实现相应流程，判断是否支持 USAT 功能，并且得到 USIM 卡的基本信息；
- 扫描 USIM 卡文件系统，显示其中存储的信息，得到 EF 文件的使用情况，明确此卡所支持的功能以及目前的状态；
- 接收 USIM 卡端发送出的指令，分析指令含义，根据其中内容做出处理，同时在界面上做出相应显示；
- 与用户进行互操作，将用户操作表示为 USAT 指令，之后向卡发出指令，同时显示用户操作结果；
- 执行编辑好的多条 USAT 指令，批量执行 USAT 命令；
- 显示在通信过程中所用到的 USAT 指令，并且对指令进行详细描述，包括指令名称，执行的数据，响应数据以及执行的结果，并且可以对数据保存；

此模块为以下几个部分，详述如下：

2.2.1 基本信息部分

此部分通过扫描卡中的 MF、DF、以及 EF 文件，显示卡中文件系统的使用情况，得到卡所支持的功能。除此之外，还实现扫描 USIM 卡基本信息的功能，显示卡中详细的信息，主要有如下信息：

- ATR： Answer To Reset，应答复位。
- ICCID：IC 卡的唯一识别号码，共有 20 位数字组成。对于中国移动，其编码格式为 898600MFSSYYGXXXXXXX，分别介绍如下：
  - 898600：固定不变。
  - M：移动接入号的末位有 4、5、6、7、8、9、0，分别对应于 134、135、136、137、138、139、159。
  - F：用户号码第四位取值范围为（0～9）。
  - SS：省代码。
  - YY：为编制 ICCID 时的年号取后两位。
  - G：SIM 卡供应商代码。
- IMSI：International Mobile Subscriber Identity，国际移动用户识别码。
- PHASE：用来表征 SIM 卡的状态以及可能支持的功能或者服务。

SIM 卡的相位信息存储在 EF_{Phase} 文件中，可分为：Phase1，Phase2，Phase2+三种。在 Phase1 情况下，ME 就只会假设 SIM 卡仅支持 Phase2 和 Phase2+条件下的部分功能。并且只有在 Phase2+的条件下，支持 SIM 卡应用工具箱的 ME 才会执行 USAT 过程。

- ACC：Access control class，访问控制级别。在 SIM 卡中，有 15 个级别 10 个普通级别 5 个高级级别。
- PIN：Personal Identification Number，个人识别号码。
- PUK：PIN Unblocking Key，个人开锁码。

2.2.2 SST

SST 即 SIM Service Table，SIM 卡服务列表，存储在 EF_{SST} 文件中。EF_{SST} 的 ID 号为‘6F38’，为透明类型 EF 文件，它用来指出 SIM 卡可以提供服务的种类，哪些业务被激活，哪些业务没有开通。如果一项服务不允许使用，或者是没有被激活，那么终端就不可以选择此项服务。

在 EF_{SST} 内，服务信息是从序号 1 开始排列，每 4 个服务信息为一组，每一个服

务信息占用 2 比特，其中，第一比特标示服务是否被允许，第二比特则标示服务是否是激活的。EF_{SST} 中一共有 50 种服务信息[3]，主要用到的主要有如下一些：

表 2-1 SST 表

序号	内容	序号	内容	序号	内容
1	CHV1 取消	12	SMS 参数	28	呼叫控制
2	ADN	13	LND	29	主动式 SIM
3	FDN	14	CBMI	31	BDN
4	SMS	17	服务提供商	35	短消息状态报告
5	AoC	18	SDN	37	通过 USIM 控制的短消息
6	CCP	25	SMS-CB 方式数据下载	38	GPRS
7	PLMN 选择	26	SMS-PP 方式数据下载	39	IMG
9	MSISDN	27	菜单选择	40	SoLSA

2.2.3 USAT 测试

在测试过程中首先需要判断 SIM 卡是否满足 3GPP 相关的协议规范的要求[2][3][9][12][13][14][15][16][17]，并且只有 PHASE 大于 2 的 SIM 卡才可以完全支持主动式命令。在满足协议要求的情况下，模拟 ME 向 SIM 卡发送 Terminal Profile 命令，并对 SIM 卡进行初始化。初始化之后，在操作界面（模拟为一个手机）上可以对 SIM 卡发出操作命令，进行与 SIM 卡之间的交互操作，并且在手机操作界面上可以显示操作结果，同时在另一窗口上，按照命令执行顺序显示操作过程中命令的细节，使用到的数据，以及执行结果和错误提示（如果有的话）。

在 USAT 操作过程中，显示如下内容：

- 操作过程中相关 EF 文件的使用情况；
- 正在执行的命令，命令使用到的数据，以及执行之后的结果；
- 用户的操作，输入的信息；
- 程序或者卡的输出，执行结果；
- 手机操作界面相应信息显示；
- 错误信息，错误提示。

在显示操作命令的界面上，所有的命令名称均在界面上用英文显示。而使用到的

数据在下一行显示，之后便是操作结果，这些信息用 16 进制的数字显示，每两个数字一组，每组之间用空格隔开，每行最多显示 8 组。

2.2.4 单步测试

在单步测试中，每个命令均是单步执行，软件每执行完一步都需在用户输入一定的信息之后，再进行下一步操作。用户还可以主动选择对 SIM 卡的操作，而非像 USAT 测试那样需要等待命令，重要的是还可以由用户选择操作执行的结果。

单步测试中可以选择的操作命令或功能：

- SMS-PP：通过 SMS-PP 方式的数据下载；
- SMS-CB：通过 SMS-CB 方式的数据下载；
- Call Control Mobile Originated Calls：通过 USIM 的呼叫控制；
- MO Short Message Control by USIM：通过 USIM 控制的 MO-SMS；
- Send Control by USIM：通过 USIM 的 SS 消息发送；
- Send USSD Control by USIM：通过 USIM 的 USSD 消息发送；

在操作过程中有多种执行结果可以选择，每种结果均是用 2 位 16 进制数字表示。单步测试中可以选择的操作结果（执行结果）有下面三类[3]：

- ‘0X’ 与 ‘1X’ 表示命令已经执行；
- ‘2X’ 表示命令虽然因某种原因没有执行，但是值得 USIM 重新执行此命令；
- ‘3X’ 表示此命令不值得重新执行，因为很有可能得到相同的结果，然而最后是否要重新执行此命令要依赖 USIM 的响应；

其中，使用比较多的是 ‘00’，表示命令成功执行。

2.3 网络模块

USAT 应用最终都要通过短消息（SMS）的方式，将各项业务请求发送给业务中心，业务中心将有关信息再通过短消息的方式返回给用户进行应答。利用短消息发送的业务请求，用户可以得到诸如天气预报、时事新闻、股市资讯等信息服务，甚至还可以直接通过手机进行银行账户的查询、转账、代缴费或进行股票交易。

短消息通信一次最多只能传递一条消息。对于点对点短消息每条消息最长为 160 个 ASC 码编码或最长 70 个汉字编码。从网络的角度，短消息的发送和接收总是在移动台和短消息中心之间进行；而从用户的角度，不管是发出或接收短消息，其目的地最终总是某个用户。

然而实际过程中通信过程十分复杂，并且无线网络与有线网络均参与其中，对开

发新业务会产生一定影响，特别是在新业务研发过程中增加研发的复杂度和调试难度。为此，在网络模块中去除了无线网络，让 ME 端的短消息直接发送到 OTA Server 端。这样不仅降低了研发的难度，而且重要的是可以不用区分网络所使用的技术，无论在目前的 GSM 网络，CDMA 网络中可以使用此环境帮助研发新业务，而且对于未来的 3G 网络同样有用武之地。

为此本模块需要建立测试系统与 OTA Server 之间的连接，实现二者之间的通信，数据传递和命令控制，以及实现短信业务菜单的 OTA 下载。这些功能的实现主要依据《中国移动通信互联网短信网关接口协议》[5]和《STK 卡梦网短信业务菜单 OTA 下载实现方案（二阶段）》[4]实现，下面分别详述功能和设计。

2.3.1 CMPP 功能实现

此部分建立测试系统与 OTA Server 之间的连接，实现二者之间的通信，数据传递和控制命令接收。

2.3.1.1 网络结构

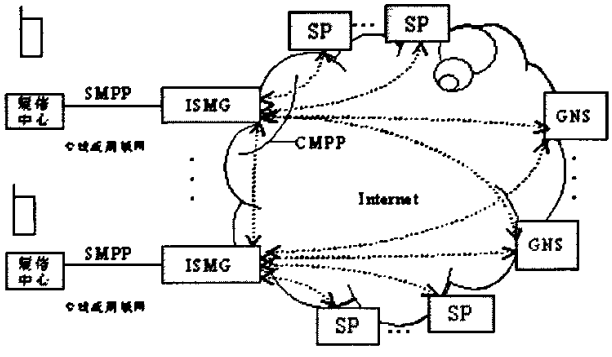


图 2-2 互联网短信网关逻辑结构图

如图所示，互联网短信网关（ISMG）是外部信息资源站实体（SP）与移动网内短信中心之间的中介实体，互联网短信网关一方面负责接收 SP 发送给移动用户的信息和提交给短信中心。另一方面，移动用户点播 SP 业务的信息将由短信中心通过互联网短信网关发给 SP。另外，为了减轻短信中心的信令负荷，互联网短信网关还应根据路由原则将 SP 提交的信息转发到相应的互联网短信网关。互联网短信网关通过向汇接网关（GNS）查询的方式获得网关间的转发路由信息。

在测试系统中，OTA Server 就可以实现 SP 功能，提供 SP 业务，而此时测试系

统中的模拟手机操作可以实现 SP 业务点播。

2.3.1.2 CMPP 功能概述

CMPP模块依据CMPP协议，主要提供以下两类业务操作：

1. 短信发送（Short Message Mobile Originate，SM MO），其典型的业务操作如图所示：

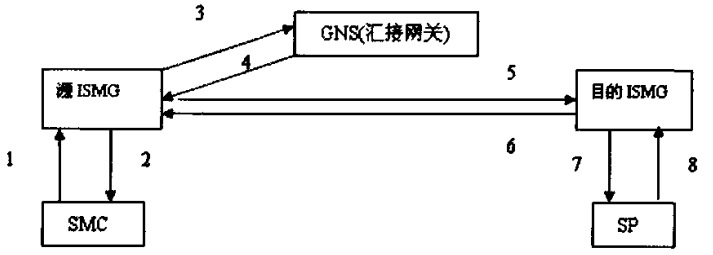


图 2-3 MO 示意图

1) 手机发出数据请求，可能是订阅信息或图片点播等，被源 ISMG 接收；

2) 源 ISMG 对接收到的信息返回响应；

3) 源 ISMG 在本地查询不到要连接的 SP，向 GNS 发路由请求信息；

4) GNS 将路由信息返回；

5) 源 ISMG 根据路由信息将请求前转给目的 ISMG；

6) 目的 ISMG 对接收到的信息返回响应；

7) 目的 ISMG 将请求信息送 SP；

8) SP 返回响应。

在以上操作中，步骤3到步骤8均使用CMPP协议[5]。在随后的操作中，目的ISMG在接收到SP的响应后将产生MO状态报告发给源ISMG。

2. 短信接收（Short Message Mobile Terminated，SM MT），其典型的业务操作举例如下所示：

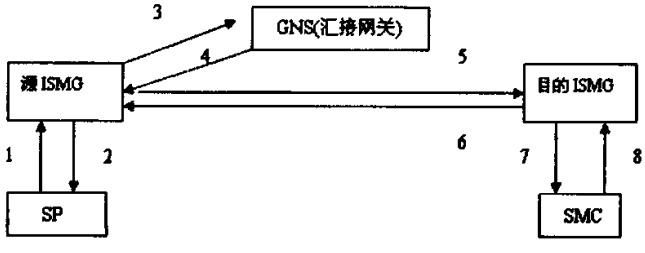


图 2 -4　MT 示意图

SP 发出数据请求，可能是短信通知或手机铃声等，被源 ISMG 接收；

1) 源 ISMG 对接收到的信息返回响应；

2) 源 ISMG 在本地数据库中找不到要目的手机号段所对应网关代码，向 GNS 发路由请求信息；

3) 汇接网关将路由信息返回；

4) 源 ISMG 根据路由信息将请求前转给目的 ISMG；

5) 目的 ISMG 对接收到的信息返回响应；

6) 目的 ISMG 将请求信息发送至 SMC；

7) SMC 向目的 ISMG 返回响应；

在上述操作中，步骤 1 到步骤 6 均使用 CMPP 协议[5]。

在随后的操作中，SMC 将通过 NO.7 信令网向移动用户发送信息，移动用户收到后将返回状态报告给短信中心，如果 SP 要求返回状态报告，短信中心将按照 MO 操作的流程将状态报告返回给 SP。

2.3.1.3 协议栈

CMPP 协议以 TCP/IP 作为底层通信承载，具体结构由下图所示[5]：

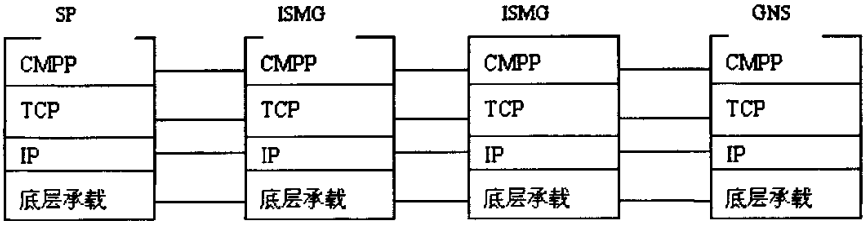


图 2-5 协议栈结构图

2.3.1.4 通信方式

SP 与 ISMG 之间、ISMG 之间进行信息交互时，可以采用长连接方式，也可以采用短连接方式。所谓长连接，指在一个 TCP 连接上可以连续发送多个数据包，在 TCP 连接保持期间，如果没有数据包发送，需要双方发链路检测包以维持此连接。短连接是指通信双方有数据交互时，就建立一个 TCP 连接，数据发送完成后，则断开此 TCP 连接，即每次 TCP 连接只完成一对 CMPP 消息的发送。本测试系统使用长连接方式保持通信。

2.3.2 OTA 功能实现

在 CMPP 功能实现之后，即建立 CMPP 连接之后，就可以通过发送 PP_Download 命令进行卡与 OTA Server 之间的消息传递，通过这些消息可以进行下载服务列表更新，用户卡注册，以及 MO 下载操作等 OTA 功能。

2.3.2.1 系统逻辑模型

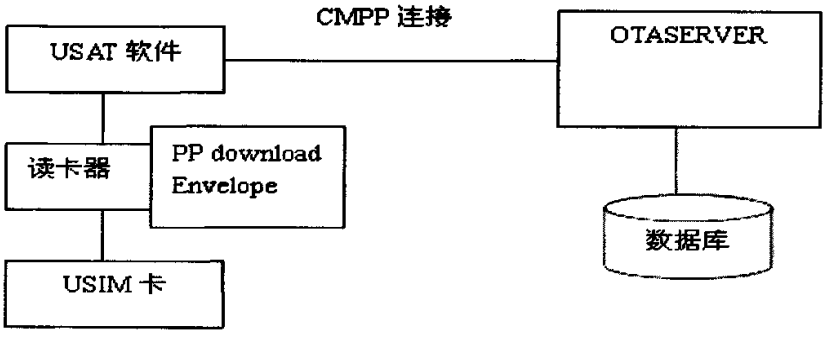


图 2-6 系统逻辑模型图

2.3.2.2 基本功能实现流程

实现的基本流程图如下：

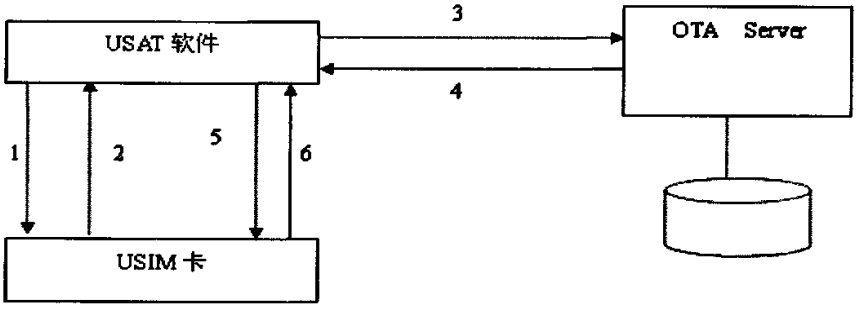


图 2-7 基本功能实现流程图

其中：1. USAT 软件向 SIM 卡发送初始化命令；

2. USIM 卡发送请求数据；

3. CMPP MO 请求短信；

4. CMPP MT 响应短信；

5. 用 PP-DOWNLOAD 下载到 USIM 卡；

6. 显示 OTA 操作结果信息。

在步骤 1，2 中，使用 USAT 主动式命令，完成 USIM 卡的初始化，之后等待 USIM 卡向 OTA Server 发送信息，并且也要开始监视 OTA Server 是否给卡发送信息，步骤 5，6 使用的也是 USAT 命令，步骤 3，4 则是使用 CMPP 命令。USAT 软件的一个重要作用就是将二种不同格式的命令转换，使发送方，接收方均可以得到正确的信息。

USAT 软件接到 USIM 卡发向 OTA Server 的命令后，便对命令进行加 CMPP 前缀，转换为适合的格式，之后将信息通过网络发送到 OTA Server；反之若 USAT 软件接收到 OTA Server 发向 USIM 卡的命令，便开始对命令进行分析，去掉 CMPP 格式，取出其中数据项，用 USAT 命令中的 PP_Download 命令发送到 USIM 卡。

第三章 USAT 模块设计

3.1 概述

一般命令的正常结束标志仅是‘9000’，而对一个支持主动式USAT命令的ME进行操作，其命令结束标志可以改用状态字‘91XX’作为响应。响应状态字‘91XX’与‘9000’一样，都可以通知ME，USIM卡已经成功执行前一命令。另外，‘91XX’还表示响应数据中包含一个针对特定ME过程的USAT命令。其中‘XX’值表示响应数据的长度，ME可以使用FETCH命令获得此数值长度的数据。

USIM卡将使用‘91XX’返回值一直提醒ME还有一个未执行的主动式命令，直至ME读取该命令为止。

若ME使用主动式命令，就会立即进行以下处理：

- 如命令执行成功，ME就用TERMINAL RESPONSE命令尽快通知USIM。
- 如命令未执行成功，ME就用带有错误条件的TERMINAL RESPONSE命令尽快通知USIM。

USIM通过ME在TERMINAL RESPONSE命令中给出的信息，判断是否重发同样的命令、发不同的命令、或是不再重发。如果USIM卡希望ME再次尝试，它会发出一个新的（同样的）命令。需要注意的是USIM一次只能执行一个主动式命令。

3.2 APDU

命令传递过程中基本的传输数据单位是 APDU，即 Application Protocol Data Unit，是应用协议数据单元。从应用层送出的命令报文，以及从 SIM 卡回送到应用层的响应报文均称作 APDU[16][17]。

我们知道一个特定的响应对应于一条特定的命令，在一个 APDU 中，无论含有命令报文，还是含有响应报文，都可以从接口设备送到 SIM 卡，或者反过来从 SIM 卡送到接口设备，并且命令和响应报文中都可以包含有或者没有数据。因而，一共存在四种情况[7]：

表 3-1 APDU 类型表

	情况 1	情况 2	情况 3	情况 4
命令数据	无	无	有	有
响应数据	无	有	无	有

APDU 有命令 APDU 和响应 APDU 两种不同类型，它们有着不同的映射格式：

- 命令 APDU 的一般格式如下：

CLA	INS	P1	P2	P3	Data

- 响应 APDU 的一般格式如下：

Data	SW1	SW2

在 USAT 模块中采用 T=0 传输协议传输 APDU，而其他的协议可将 APDU 嵌入它们特有的传输结构之中。其中：

- CLA 是指令级别，用来指示命令和响应数据应在何等程度上遵从 ISO/IEC 7816-3，或者在什么时候可以使用保密报文的格式以及逻辑通道的数量。在数字蜂窝移动通信应用中采用的 CLA 为‘A0’。
- INS 是指令码，遵从 ISO/IEC 7816-3 规定。
- P1，P2，P3 是指令的参数。‘FF’对于 P1，P2 和 P3 是有效值。P3 给出了数据单元的长度。在输出数据传输命令中(响应方向)，P3=‘00’则表示引入 SIM 发送的一个 256 个字节的数据传输。在输入数据传输命令中(命令方向)，P3=‘00’表示无数据发送。
- Data 是数据，保存响应中接受的数据字节串。
- SW1 和 SW2 为指示命令成功或不成功的状态字。状态字常用的有如下一些：

表 3-2　状态字含义表

SW1	SW2	含义	SW1	SW2	含义
‘90’	‘00’	命令正常结束	‘92’	‘40’	内存问题
‘91’	‘XX’	命令正常结束，但 SIM 发送‘XX’长度的主动式命令到 ME	‘94’	‘08’	文件与命令描述不一致
‘9E’	‘XX’	在 SIM 卡下载数据出错的情况下，发送‘XX’长度的响应数据	‘94’	‘04’	文件 ID 不存在，或是类型不匹配
‘9F’	‘XX’	‘XX’长度的响应数据	‘94’	‘02’	溢出
‘93’	‘00’	SIM 工具箱忙，此命令目前无法执行	‘94’	‘00’	没有 EF 文件被选中
‘92’	‘0X’	命令在重新尝试‘X’次后成功执行	‘98’	‘02’	无 CHV 初始化

3.3 功能描述

USIM卡应用工具箱USAT，是在原SIM卡被动式的操作系统上，衍生出的USIM卡主动交互式的操作系统。它提供的机制，允许USIM卡中的应用与支持该应用的ME进行交互操作，即支持USIM卡与ME之间的主动式对话，从而使移动用户拥有个人化

附加业务。这些机制采用GSM11.11 和GSM11.14 中与USIM卡应用工具箱相关的命令和协议。下面按照卡执行的逻辑顺序详细描述。

3.3.1 USIM 卡初始化

对 USIM 卡初始化，经历了比较复杂的过程。首先 ME 选择专用文件 DF_{GSM} 并发出首选语言请求。若此文件不可访问或 ME 不支持在此文件中的语言，则 ME 选择一个缺省语言。然后运行 CHV1 证实程序。

若成功的执行了 CHV1 证实程序，则 ME 运行 USIM 卡阶段请求程序。若 ME 确定是第一阶段的卡，则将告知用户此卡第一阶段的卡，之后退出程序。

对于第二阶段卡，只有满足下列条件之一时，GSM 操作才能开始：

1) 若 EF_{LMSI} 和 EF_{LOCI} 有效，则 GSM 操作立即起动；

2) 若 EF_{LMSI} 和 EF_{LOCI} 中存在至少一个无效，那么 ME 恢复这两个文件，使它们有效，则 GSM 操作随后起动。

如果 ME 没有 FDN 能力将不能恢复 EF_{LMSI} 和 EF_{LOCI}，因此，就不能访问这些 EF，故 GSM 操作将禁止执行。这种机制是通过对此类业务的 USIM 卡应用，控制表 2-1 SST 表中的 No.3 业务实现的。

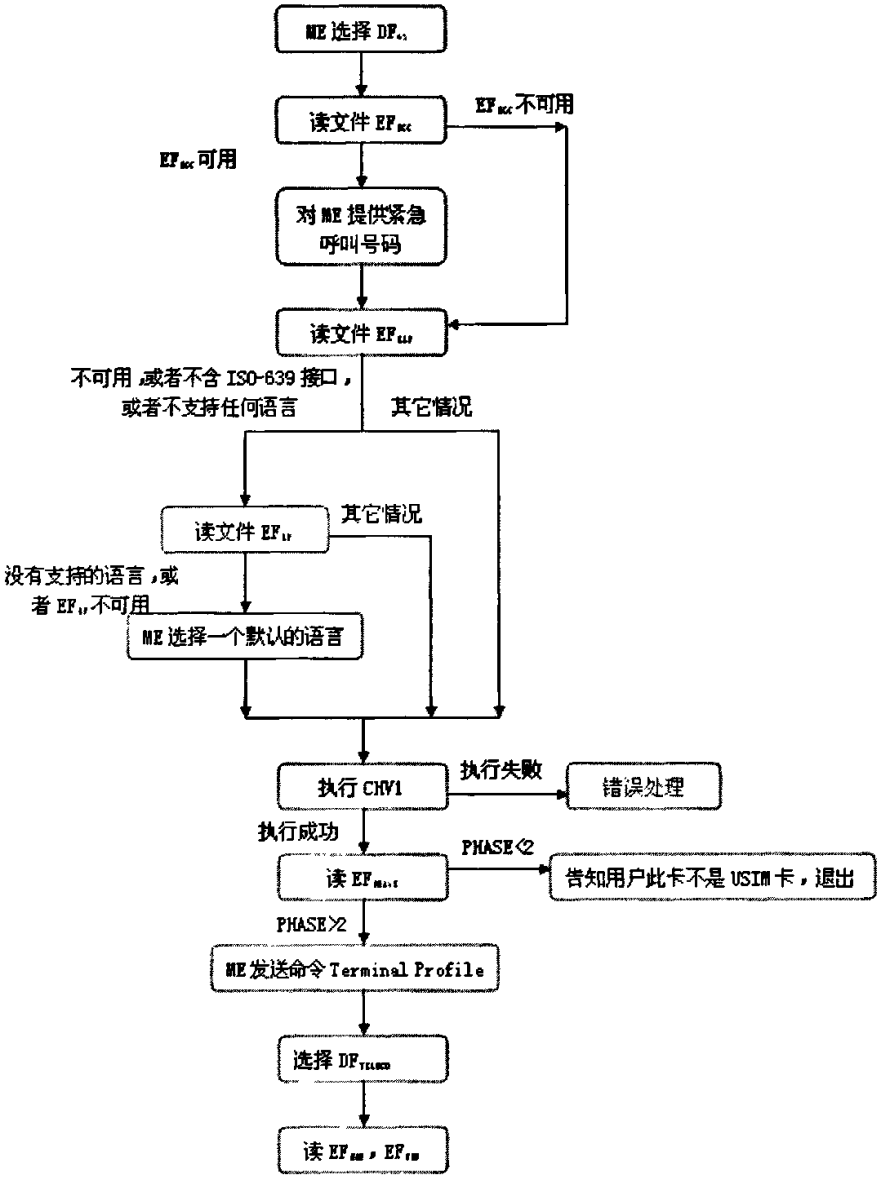
若 FDN 能力程序指示为：

1) 在 USIM 卡中已配置和激活了 FDN，并且将 FDN 设置为“使能”，即 ADN 无效并且未激活，而 ME 还是支持 FDN 功能；

2) FDN 在 USIM 卡中已配置并激活，而且 FDN 设置为“不使能”，即 ADN 有效；

3) FDN 未配置和未激活。

满足上述条件之一时，则 GSM 操作应该启动。而在所有其他情况下 GSM 操作将不启动。详细流程图如下：


ME 选择 DF
读文件 EF
EF 不可用
EF 可用
对 ME 提供紧急呼叫号码
读文件 EF
不可用，或者不含 ISO-639 接口，或者不支持任何语言
其它情况
读文件 EF
其它情况
没有支持的语言，或者 EF 不可用
ME 选择一个默认的语言
执行 CHV1
执行失败
错误处理
执行成功
读 EF
PHASE<2
告知用户此卡不是 USIM 卡，退出
PHASE>2
ME 发送命令 Terminal Profile
选择 DF
读 EF，EF

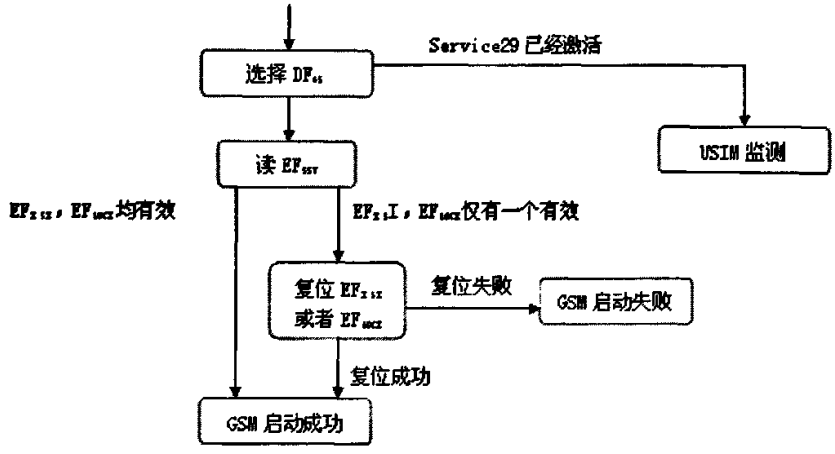


图 3-1 GSM 启动流程图

之后，完成管理信息请求，USIM 卡业务表请求，IMSI 请求，访问控制条件请求，HPLMN 搜索周期请求，PLMN 选择器请求，位置信息请求，密钥请求，CPBCCH 信息请求，BCCH 信息请求，禁用 PLMN 请求，小区广播消息识别请求，以及 LOCI GPRS 信息请求。

这样 USIM 卡初始化工作成功地完成了。

3.3.2 交互操作

GSM 成功启动之后，测试系统还要通过执行多条命令以实现某些具体功能，概述如下：

1. SIM 监测功能

USIM 监测功能作为一种附加机制，是为了及时得到 USIM 卡在一个卡对话期间是否被移出的信息。此功能是通过 ME 在每次呼叫期间频繁的发出 STATUS 命令实现的，其命令间隔不超过 30 秒。若响应数据不是当前 DF 的响应数据，或没有响应数据返回，则呼叫应在 5 秒钟之后终止，同时将告知用户 SIM 卡被移出。

2. SMS-CB 功能

SMS-CB 即为小区广播消息，在 Service25 为“允许的并且激活的”的情况下，收到服务器发来的小区广播消息时，测试系统应该完成的功能，执行流程见下图[20][21]：

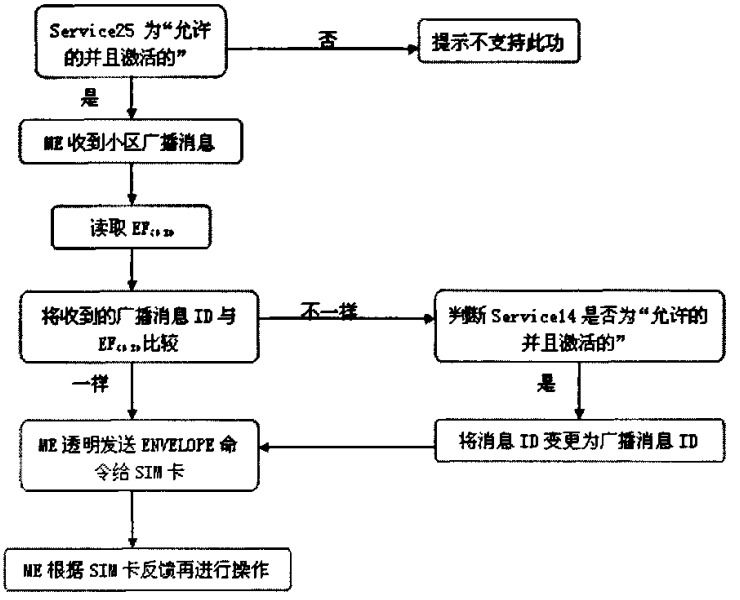


图 3 - 2　SMS-CB 流程图

3. SMS-PP 功能

SMS-PP 是点对点数据下载，执行流程如下：

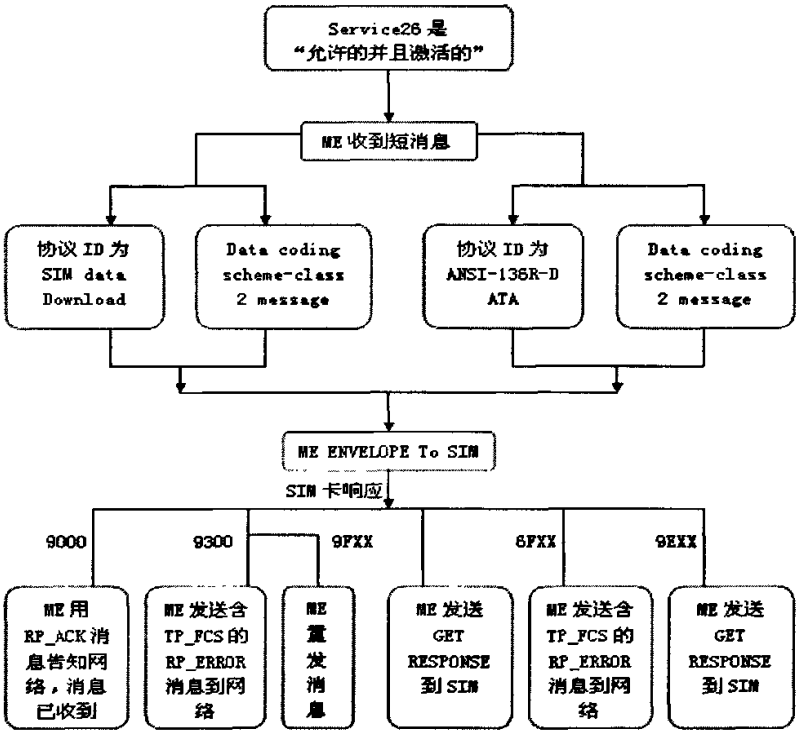


图 3-3　SMS-PP 流程图

4. 菜单选择功能

菜单选择功能利用主动式命令提供一套菜单，向 SIM 卡传送用户选择的应用菜单项，也可以用于请求应用菜单中各项的帮助信息。

在 Service27 为“允许的并且激活的”的情况下，测试系统收到如下之一指示时，便向 SIM 发送 ENVELOPE 命令：

- SIM 卡选中之前建立菜单中的某项；
- 用户需要某一条菜单项的帮助信息。

5. 呼叫受控功能

当 SIM 卡激活此业务后，所有拨出的数字串、补充业务控制字符串和 USSD 字符串在 ME 建立呼叫、补充业务操作或 USSD 操作前要先传递给 USIM 卡。ME 也应同时向 USIM 卡传递其当前服务区信息。USIM 卡还具有用一个呼叫请求、补充业务操作或 USSD 操作替换另一个呼叫请求、补充业务操作或 USSD 操作的能力[14][15]。

在 Service28 为“允许的并且激活的”的情况下，当用户建立呼叫时，除 ME 自动重新拨号，或者用户拨打 112 或 EF_{ECC} 中的紧急号码之外的情况，ME 均要通过发送 ENVELOPE 命令，向 USIM 卡告知呼叫细节。之后 ME 根据 USIM 卡的响应数据再做出进一步动作，可能一个呼叫请求被一个补充业务操作或 USSD 操作替换。

补充业务操作和 USSD 操作的情况与此类似。

6，用户指示信息功能

在 ME 发送呼叫控制命令之后，若在 SIM 的响应数据中含有 a 标示符标记，那么 ME 将根据响应信号为“允许的，没有修改的”，“不允许”，还是“允许的，但是有修改”，以及联系 a 标示符标记的内容，一同决定是否告知用户当前操作的情况。

7，USIM 卡的 MO 短消息控制

当 USIM 卡激活此业务后，在 ME 发送短消息之前，所有 MO 短消息首先传递给 USIM 卡。ME 也应同时向 USIM 卡传递其当前服务区信息。在发送短消息之前，USIM 卡具有允许发送、禁止发送或修改短消息目的地址的能力。

8，刷新功能

此命令用于使 ME 得到 UICC 配置改变的通知。该命令将一直执行，直到 USIM 应用确认了刷新正确完成为止。

UICC 可以指示需要刷新的 USIM 应用 AID。

- 若所指的 USIM 是激活的，ME 应进行刷新；
- 若所指的 USIM 未激活，ME 应发送 TERMINAL　RESPONSE，而不选择该

USIM；

- 如果没有给出 AID，ME 刷新当前 USIM 应用。

此命令支持 7 种不同的模式：

1）USIM 初始化。此模式通知 ME 在 PIN 校验后对 USIM 进行初始化；

2）文件改变通知。此模式通知 ME 在 USIM 中文件结构和/或内容已经改变的 EF 文件的标识符。若在 ME 的存储器中有 USIM 的 EF 文件映像(如 EF_{ADN} 文件)，ME 可通过该通知来决定是否需要更新这些映像的内容；

3）USIM 初始化和文件改变通知。是上述两种模式的合并；

4）USIM 初始化和全部文件改变通知。此模式在 PIN 校验后对 USIM 进行初始化，并且通知 ME 在 USIM 中某些 EF 文件的结构或内容已经改变。若在 ME 的存储器中有 USIM EF 文件的映像，ME 将通过 REFRESH 命令全部更新这些映像的内容；

5）UICC 复位。此模式可使 ME 终止会话过程。随后，ME 复位（首选热复位）UICC 并开始一新的应用会话。一般情况下命令完成后发送 TERMINAL RESPONSE, 然而此模式中 ME 不发送 TERMINAL RESPONSE 命令，这是正常过程的特例。UICC 将复位作为隐含的 TERMINAL RESPONSE 命令。当 USAT 请求执行 ATR 或完整的 UICC 初始化过程时，采用 UICC 复位模式。

6）USIM 应用复位。该模式使 ME 终止 3G 会话，关闭 USIM 应用。随后，ME 进行 USIM 初始化。

7）3G 会话复位。该模式相当于“USIM 初始化和文件改变通知”模式，此外请求 ME 进行重启动。

若 ME 对上述模式中指示的 EF 文件成功执行了 REFRESH 命令，命令完成后 ME 应发送 TERMINAL RESPONSE(OK)命令通知 USIM 卡。

3.3.3 GSM 终止

GSM 对话需要由 ME 终止。ME 要运行所有必要的程序将以下用户相关的信息传送给 USIM 卡：

- 位置信息更新；
- 密钥更新；
- BCCH 信息更新；
- 计费通知增加；

➢ 禁用 PLMN 更新。

一旦 USIM 卡表示已完成这些程序，便完成了去活 ME/USIM 链路。最后，ME 将从存储器中删除所有与用户相关的信息单元。

3.4 命令描述

USAT 模块中所使用到的命令均在 USAT 相关协议[2][3][6]中有详细介绍，针对在测试系统实现过程所用到的主要命令做如下概要描述。

1. TERMINAL PROFILE，概要信息下载

作为 USIM 初始化的一部分，概要信息下载命令由 ME 发给 USIM。ME 发送的概要信息说明 ME 支持的 USAT 相关功能项。通过这个过程 USIM 知道 ME 的能力并根据情况限制它的命令范围。如果 ME 没有发出此命令，USIM 认为 ME 不支持 USAT。

命令方向是从 ME 到 USIM，内容为 ME 支持的 USAT 功能列表。每个功能项使用 1 位比特。其中‘1’表示 ME 支持的功能；‘0’表示 ME 不支持的功能。

第一字节（下载）：

BIT8：Bit=1，支持 USIM 呼叫控制；

BIT7：Bit=1，支持 USIM 呼叫控制；

BIT6：定时器终止；

BIT5：Bit=1，支持 SMS-PP 数据下载；

BIT4：菜单选择；

BIT3：小区广播数据下载（只对 GSM 网络）；

BIT2：SMS-PP 数据下载；

BIT1：概要信息下载。

第二字节（其他）：

BIT8 ：Bit=1，支持文本显示；

BIT7 ：支持 UCS2 显示；

BIT6 ：支持 UCS2 输入；

BIT5 ：Bit=1，支持 USIM 呼叫控制；

BIT4 ：USIM 卡的 MO 短消息控制；

BIT3 ：Bit=1，支持 USIM 呼叫控制；

BIT2 ：USIM 呼叫控制；

BIT1 ：命令结果。

第三字节（主动式 USAT 命令）：

BIT8：主动式 USAT 命令 REFRESH；

BIT7：主动式 USAT 命令 POLLING OFF；

BIT6：主动式 USAT 命令 POLL INTERVAL ；

BIT5：主动式 USAT 命令 PLAY TONE ；

BIT4：主动式 USAT 命令 MORE TIME；

BIT3：主动式 USAT 命令 GET INPUT；

BIT2：主动式 USAT 命令 GET INKEY ；

BIT1：主动式 USAT 命令 DISPLAY TEXT。

第四字节（主动式 USAT 命令）：

BIT8：主动式 USAT 命令 PROVIDE LOCAL INFORMATION（NMR）；

BIT7：主动式 USAT 命令 PROVIDE LOCAL INFORMATION（MCC，MNC，LAC，Cell ID，IMEI）；

BIT6：主动式 USAT 命令 SET UP MENU；

BIT5：主动式 USAT 命令 SET UP CALL；

BIT4：主动式 USAT 命令 SEND USSD；

BIT3：主动式 USAT 命令 SEND SS；

BIT2：主动式 USAT 命令 SEND SHORT MESSAGE；

BIT1：主动式 USAT 命令 SELECT ITEM。

第五字节（事件驱动信息）：

BIT8：读卡器状态；

BIT7：空闲屏幕可用；

BIT6：用户活动；

BIT5：位置状态；

BIT4：呼叫拆线；

BIT3：呼叫接线；

BIT2：MT 呼叫；

BIT1：主动式 USAT 命令：SET UP EVENT LIST。

第六字节（事件驱动扩展信息）：

BIT8,7,6,5：RFU，bit=0；

BIT4：表示数据通道状态；

BIT3：表示数据可用；

BIT2：表示浏览器终止；

BIT1：表示语言选择。

第七字节（多用途卡主动式命令）：

BIT8,7,6：RFU，bit=0；

BIT5：主动式 USAT 命令 GET READER STATUS，读卡器识别；

BIT4：主动式 USAT 命令 GET READER STATUS，读卡器状态；

BIT3：主动式 USAT 命令 PERFORM CARD APDU；

BIT2：主动式 USAT 命令 POWER OFF CARD；

BIT1：主动式 USAT 命令 POWER ON CARD。

第八字节（主动式 USAT 命令）：

BIT8：Bit=1，支持 USIM 呼叫控制；

BIT7：Bit=1，支持 SETUP CALL 命令；

BIT6：执行 AT 命令；

BIT5：建立空闲模式文本；

BIT4：Bit=1，支持 GET INKEY 命令；

BIT3：主动式 USAT 命令 PROVIDE LOCAL INFORMATION（日期,时间和时区）；

BIT2：主动式 USAT 命令 TIMER MANAGEMENT（取当前值）；

BIT1：主动式 USAT 命令 TIMER MANAGEMENT（启动，停止）；

第九字节：

BIT8：RFU，bit=0

BIT7：主动式 USAT 命令 LAUNCH BROWSER；

BIT6：主动式 USAT 命令 LANGUAGE NOTIFICATION；

BIT5：主动式USAT命令 PROVIDE LOCAL INFORMATION (当前时间)；

BIT4：主动式 USAT 命令 PROVIDE LOCAL INFORMATION (语言)；

BIT3：主动式USAT命令PROVIDE LOCAL INFORMATION（NMR）；

BIT2：发送DTMF命令；

BIT1：Bit=1，支持 DISPLAY TEXT 命令。

第十字节(软键支持)：

BIT8,7,6,5,4,3：RFU，bit=0；

BIT2：软键支持SET UP MENU命令；

BIT1：软键支持 SELECT ITEM 命令；

第十一字节(软键信息)：

可用软键的最大数量，‘FF’留作将来使用。

第十二字节(承载无关协议主动式命令)：

BIT8,7,6：RFU，bit=0；

BIT5：主动式 USAT 命令 GET CHANNEL STATUS；

BIT4：主动式 USAT 命令 SEND DATA；

BIT3：主动式 USAT 命令 RECEIVE DATA；

BIT2：主动式 USAT 命令 CLOSE CHANNEL；

BIT1：主动式 USAT 命令 OPEN CHANNEL。

第十三字节(承载无关协议所支持的承载)：

BIT8,7,6：ME 支持的数据通道数；

BIT5,4,3：RFU，bit=0；

BIT2：ME 支持 GPRS；

BIT1：ME 支持 CSD。

第十四字节(屏幕高度)：

BIT8：屏幕尺寸参数；

BIT7,6：RFU，bit=0；

BIT5,4,3,2,1：ME支持纵向显示的字符数。

第十五字节(屏幕宽度)：

BIT8：支持多种字号的字体；

BIT7,6,5,4,3,2,1：ME 支持横向显示的字符数。

第十六字节(屏幕效果)：

BIT8,7,6：菜单宽度缩小；

BIT5,4：RFU；

BIT3：支持文本上下滚屏；

BIT2：支持文本换行；

BIT1：调整屏幕显示大小。

第十七字节(承载无关协议所支持的传输接口)：

BIT8,7,6,5,4,3：RFU，bit=0；

BIT2：UDP；

BIT1：TCP。

第十八字节(留作将来使用)：

BIT8,7,6,5,4,3,2,1：RFU，bit=0。

第十九字节(为 TIA/EIA-136 工具保留):

BIT8,7,6,5：RFU，bit=0;

BIT4,3,2,1：TIA/RIA-136-123 中规定的协议版本，代码。

后续的字节：BIT8,7,6,5,4,3,2,1：RFU，bit=0。RFU 位和所有后续字节留作将来使用。只支持此[6]规范定义的 USIM 卡应用工具箱的 USIM 卡不检查 RFU 各位的值。响应参数/数据：无。

2. SELECT，选择

COMMAND	CLASS	INS	P1	P2	P3
SELECT	'A0'	'A4'	'00'	'00'	'02'

此命令的输入为文件 ID，文件类型不同，其输出的类型也不相同。当选择 MF 或者 DF 类型文件时，输出文件 ID，可用的空间，CHV 使能指示，CHV 状态以及其他一些 GSM 详细数据，如当前目录下的 DF，EF 文件数目。当选择 EF 类型文件时，输出文件 ID，文件大小，访问条件，使能指示，F 结构，以及记录的长度。

3. STATUS，状态

返回有关当前目录的信息，此命令的操作不影响当前的 EF。

输入：无。输出：文件 ID，全部可用的存储空间，CHV 使能/不使能指示器，CHV 状态和其他 GSM 专用的数据。

4. READ BINARY，读出二进制

用来从当前透明 EF 文件中读取出一个字节串。

输入：相对地址和字节串的长度。输出：字节串。

5. UPDATE BINARY，更新二进制

用来用一个字节串更新当前透明 EF 文件。

输入：相对地址和字节串的长度，字节串。输出：无。

6. READ RECORD，读出记录

从当前线性固定的或循环的 EF 中读出一个完整记录。若 READ RECORD 功能不成功，则记录指针不变，规定了 4 种方式：

1）当前的，读出当前记录，不影响记录指针。

2）绝对的，读出已给出记录号码的记录，不影响记录指针。

3）下一个，在执行 READ RECORD 功能以前，增加记录指针，读出被指向的记录。若在选择的 EF 里没有设置记录指针，则 READ RECORD（下一个）将读出第一个记录并对这个记录设置指针。

若在线性固定的 EF 中的记录指针定位在最后的记录上，则 READ RECORD（下一个）将不引起记录指针变化，而且也没有数据读出。

若在循环的 EF 中的记录指针定位在最后的记录上，则 READ RECORD（下一个）将这个 EF 中记录指针设置在第一个记录上，并读出这个记录。

4）上一个，在执行 RDAD RECORD 功能之前记录指针减少，并读出指针的记录。若在已选择的 EF 中没有设置指针，则 READ RECORD（上一个）将读出最后的记录，并将记录指针设置在这个记录上。

若在线性固定的 EF 中把记录指针定位在第一个记录上，则 READ RECORD（上一个）不引起记录指针的变化也没有数据读出。

若在循环的 EF 中把记录指针定位在第一个记录上，则 READ RECORD（上一个）将记录指针置在最后一个记录上并读出这个记录。

输入：方式，记录号码（只有绝对方式）和记录的长度。输出：记录。

7. UPDATE RECORD，更新记录

在当前线性固定的或循环的 EF 中更新一个完整的记录。若 UPDATE RECORD 不成功，则记录指针不变化。

规定 4 种方式：

1） 当前的，更新当前记录，不影响记录指针。

2） 绝对的，更新给定记录号码的记录。不影响记录指针。

3） 下一个，在 UPDATE RECORD 功能执行之前，增加记录指针，并更新指向的记录。若在选定的 EF 之中没有设定记录指针，则 UPDATE RECORD（下一个）将记录指针设在第一个记录上并更新这个记录；若在线性固定的 EF 中记录指针指向最后一个记录上，则 UPDATE RECORD（下一个）将不引起记录指针变化也没有记录被更新。

4）上一个，对于一个线性固定的 EF，在执行 UPDATE RECORD 功能之前使记录指针减少，并更新此记录。若在选定的 EF 之中没有设定记录指针，则 UPDATE RECORD（上一个）将记录指针设置在最后的记录上，并更新此记录；若在线固定的 EF 中记录指针已定位在第一个记录上，则 UPDATERECORD（上一个）将不引起记录指针变化且也没有记录被更新。对于循环的 EF 含有最原始数据的记录被更新，记录指针将设置在这个记录上，并使这个记录成为 1 号记录。

输入：方式，记录号码（只有绝对方式）和记录的长度；用来更新记录的数据。输出：无。

8. SEEK，查找

搜寻当前线性固定 EF 中的以图样开始的记录。有如下两种类型：

1）类型 1，记录指针指向含有给定图样的记录，没有输出。

2）类型 2，记录指针指向含有给定图样的记录，输出是记录号码。

SEEK 可接受 1－16 字节（包括 16 字节）的图样长度，但是不能超过记录的长度。规定了 4 种方式：

1）从头部正向查找；

2）从尾部反向查找；

3）从下一个位置正向查找；

4）从上一个位置反向查找。

若记录指针没有设在已选择的线性固定 EF 上，则从下述位置开始搜寻：

- 在从下一个位置正向查找的情况下，从第一个记录开始；
- 在从上一个位置反向查找的情况下，从最后一个记录开始。

查找成功之后，记录指针指向含有已找到的图样的记录上。不成功则记录指针将不发生变化。

输入：类型和方式，图样，图样的长度。输出：类型 1，无；类型 2：状态/记录号码。

9. INCREASE，增加

将 ME 给定的值加到当前循环 EF 最后增加/更新的记录的数值上，并把这个结果保存在最原始的记录里。此时，记录指针被设置到此记录上，该记录变成 1 号记录。只有满足这个 EF 的 INCREASE 访问条件，才能执行此功能。若其结果已超过记录的最大值者，则 SIM 卡不执行此功能（把全部字节重置为‘FF’）。

输入：要增加的数值。输出：增加后记录的数值，已增加的数值。

10. VERIFY CHV，验证 CHV

将 ME 提供的 CHV 与已存储在 SIM 卡中的进行比较，其验证过程是在满足 CHV 使能与 CHV 解锁条件下进行的。

若在最后选择的文件上执行一个功能的访问条件是 CHV1 或是 CHV2，则必须预先完成 CHV 成功验证请求程序，除非 CHV 不使能。

若提供的 CHV 是正确的，则剩余的 CHV 尝试次数重置初始值为 3。

若提供的 CHV 是错误的，则减少 CHV 尝试次数。在出现 3 次连续错误后，将闭锁 CHV 并且直到 CHV 上成功的执行 UNBLOCK CHV 后，才能访问条件。

输入：CHV1/CHV2，CHV 的指示方式。输出：无。

11. CHANGE CHV，变更 CHV

只有在满足已使能 CHV 与已解锁 CHV 条件下，才能指配一个新的数值，提供原来的和新的 CHV。

若提供原来的 CHV 是正确的，则剩余的 CHV 尝试次数将重置初始值为 3 而且 CHV 的新值是有效的；若提供原来的 CHV 是错的，则减少的 CHV 尝试次数且不变更 CHV 值。在出现连续 3 次错的 CHV 后，将闭锁 CHV 直到在 CHV 上成功的执行 UNBLOCK CHV 后，才能满足访问条件。

输入：CHV1/CHV2，原来的 CHV ，新的 CHV 指示方式。输出：无。

12. DISABLE CHV，不使能 CHV

此功能仅适用于 CHV1，即可访问被 CHV1 所保护的文件。当 CHV1 已经不使能或闭锁时，该功能不能执行。

若提供的 CHV1 是正确的，则剩余的 CHV1 尝试次数重置初始值为 3，CHV1 不使能。若提供的 CHV1 是错的，则减少 CHV1 尝试次数，在出现 3 次连续出错之后，将闭锁 CHV1 并且直到在 CHV1 上成功的执行 UNBLOCK CHV 命令后，才能满足访问条件。

输入：CHV1。输出：无。

13. ENABLE CHV，使能 CHV

仅适用于 CHV1，与 DISABLE CHV 功能相反。当 CHV1 已使能或闭锁，则该功能不能执行。

若提供的 CHV1 是正确的，则剩余的 CHV1 尝试次数重置初始值为 3，CHV1 使能。若提供的 CHV1 是错的，则减少 CHV1 尝试次数，在出现 3 次连续错误之后，将闭锁 CHV1 并且直到在 CHV1 上成功的执行了 UNBLOCK CHV 命令后，才能满足访问条件。

输入：CHV1。输出：无。

14. UNBLOCK CHV，解锁 CHV

解锁已闭锁的 CHV。无论 CHV 是否闭锁，此功能均可以执行。

若提供的 UNBLOCK CHV 是正确的，把 UNBLOCK CHV 提供的 CHV 的值指配给 CHV。剩余的 UNBLOCK CHV 尝试的次数重置初始值为 10，剩余的 CHV 尝试的次数重置初始值为 3。在成功地解锁尝试之后，使能 CHV 并且满足相关的访问条件。

若提供的 UNBLOCK CHV 是错的，则减少 UNBLOCK CHV 尝试的次数，在 10 次连接出现错误之后，将闭锁各自的 UNBLOCK CHV；只有一次错的 UNBLOCK CHV 将对各自的 CHV 的状态不产生影响。

输入：CHV1/CHV2，UNBLOCK CHV 和新的 CHV。输出：无。

15. INVALIDATE，使无效

使当前 EF 无效，在执行了 INVALIDATE 功能之后，在文件状态中的各自识别符应相应的改变。只有对当前的 EF 满足了 INVALIDATE 访问条件才能执行此功能。

一个无效的文件在任何功能的应用程序中，除了 SELECT 和 RELIABILITATE 功能之外，都不可用。

输入：无，输出：无

16. REHABILITATE，使修复

修复已无效的当前 EF。在执行 REHABILITATE 之后，在文件状态中的各自识别符应相应地改变。只有对当前的 EF 满足了 REHABILITATE 访问条件才能执行此功能。

输入：无，输出：无

17. RUN GSM ALGORITHM ，运行 GSM 算法

用来鉴定一个要进入 GSM 网络的 SIM 卡和生成密钥。SIM 卡采用一个 16 字节的随机数和已存储在 SIM 卡中的用户鉴权钥 Ki 来运行已规定的 A3 和 A8 算法。该功能返回计算出响应 SRES 和密钥 Kc。

只有当选择了 DF_{GSM} 作为当前目录和已经成功地执行了 CHV1 验证程序之后，此功能才是可执行的。

输入：RAND。输出：SRES，Kc。

18. ENVELOPE，信封函数

该函数实现向 SIM 卡中的 SIM 卡应用工具箱传送数据。在 SIM 卡数据点到点下载或与在 SIM 卡响应无关期间，使用 ENVELOPE 命令。

ENVELOPE 命令可以用于实现点到点短消息（SMS-PP）数据下载，小区广播短消息(SMS-CB)数据下载，菜单选择(Menu Selection)， USIM 卡的呼叫控制，MO 短消息控制，移动端发起的呼叫过程，补充业务及非结构化补充业务数据的过程，给用户的指示，与固定拨号的交互操作，禁止拨号（BDN）业务，定时器终止，事件下载，MT 呼叫事件，已连接呼叫事件，呼叫拆线事件，位置状态事件，用户动作事件，空闲屏幕可用事件，浏览器终止事件，数据可获得事件，以及信道状态事件功能。

输入：数据串。输出：1～16 个证实数据。

19. FETCH，取出数据

此命令实现从 SIM 卡向 ME 传送应用工具箱命令。

输入：无。输出：ME 接受的 SIM 卡应用工具箱命令的数据串。

20. TERMINAL RESPONSE 终端响应

该命令是实现 ME 向 SIM 卡传送以前接收的 SIM 卡应用工具箱命令的响应。

表 3-3　TERMINAL　RESPONSE 命令细节表

字节	描述	长度
1	命令细节标记	1
2	长度= '03'	1
3	命令代码	1
4	命令类型：　与 UICC 相应命令一致	1
5	命令限定符：与 UICC 相应命令一致	1

如 ME 未收到有效的命令代码，则所有命令细节数据的值应置为 '0'，并在结果值中指明出错。在命令中设备是用特定的代码表示的，详见表 3-4。TERMINAL RESPONSE 命令执行后的结果以及结构详见表 3-5。

表 3-4　TERMINAL RESPONSE 命令设备标示表

字节	描述	长度
1	设备标识标记：02/82	1
2	长度 = '02'	1
3	起始端设备标识：80=ME	1
4	目的端设备标识：81=UICC	1

表 3-5　TERMINAL RESPONSE 命令结果表

字节	描述	长度
1	结果标记：03/83	1
2 到(Y-1)+2	长度(X)	Y
(Y-1)+3	一般结果	1
(Y-1)+4 到(Y-1)+X+2	结果的附加信息	X-1

在表 3-5 中，一般结果是由已定义的代码表示特定的结果，以及 UICC 适当的动作，编码见表 3-6：

表 3-6　一般结果编码表

代码	含义	代码	含义
'00'	命令执行成功	'11'	用户请求在主动式会话中后退
'01'	执行命令，部分理解	'12'	用户无响应
'02'	执行命令，有丢失信息	'13'	用户请求帮助信息
'03'	执行 REFRESH 命令，带有 EF 读功能	'14'	用户终止 USSD 或 SS。
'04'	命令执行成功，但不能显示响应图标	'20'	ME 当前不能处理命令
'05'	命令执行，但 USIM 对呼叫进行了修改	'21'	网络当前不能处理命令
'06'	命令执行成功，服务受限	'22'	用户不接受呼叫建立请求
'07'	执行命令修改	'23'	在接入网络或释放前用户清除呼叫
'08'	执行 REFRESH，但无可用 USIM 卡	'24'	行为与当前定时器状态矛盾
'10'	用户终止的主动式 UICC 会话	'25'	与 USIM 呼叫控制交互，暂时问题

21. DISPLAY TEXT，显示文字信息

此命令指示 ME 显示文本和/或图标，并且允许 UICC 定义消息的优先级和文本字符串的格式。

协议中存在定义的两种类型的优先级：

- 屏幕显示普通优先级文本和/或图标；
- 屏幕显示高优先级文本和/或图标。

并且文本字符串为下列3种格式之一：

- SMS默认字符的打包格式；
- SMS默认字符的非打包格式；
- UCS2字符格式。

文本字符串的长度可达240个字节。并且可通过设置标志位来通知ME在'DISPLAY TEXT'结束的短暂时延后、或在人机对话后，显示屏是否可用于显示后续信息，不同ME厂商时延长度不同。对于在短暂时延后清除文本信息的情况，ME允许用户提供人机对话清除显示文本。值得注意的是：无论什么原因，ME清除屏幕显示信息后不再发送TERMINAL RESPONSE命令。

22. GET INPUT，获得输入

此命令指示 ME 显示文本或图标，用户键入的任何响应字符都会由 ME 透明传输给 USIM 卡，而不会保存在 ME 中。ME 将显示 USIM 卡提供的默认文本，用户可以接收、拒绝或编辑此默认文本作为响应字符串。

这里文本字符串为下列3种格式之一：

- SMS默认字符的打包格式；
- SMS默认字符的非打包格式；
- UCS2字符格式。

USIM 卡可以通过提供接收长度的最小和最大值来指定响应字符串的字符数。并且 ME 根据命令可显示或隐藏用户输入的文本字符串。

用户键入的响应可采用下列 3 种格式之一：

- 数字(0～9，*，#，+)或SMS默认字符表的字符；
- SMS默认字符表的字符或UCS2编码字符；
- 数字(0～9，*，#，+)或SMS默认字符表的字符可用非打包格式，也可用打包格式；

需要注意的是，SMS默认字符表中的字符组合不允许采用隐藏的输入模式。在隐藏的输入模式中，仅允许用户输入“0～9”，“*”，“#”，不允许用户输入“+”。如果USIM请求隐藏用户输入的文本串，只要不显示输入字符本身，就允许ME指示字符的输入。

收到命令，ME就显示文本。ME允许用户输入字符作为响应。并且ME的人机界

面负责确保输入正确的字符数；若USIM请求用户以打包格式输入，ME就应将文本打包后再发送给USIM。

23. SET UP MENU，建立菜单

USIM提供的一套菜单项可以添加进ME原有菜单系统中，供用户选择使用。每项由一个短标识符（用于指示选项），一个文本串，和可选的图标标识符组成，在项目图标标识符列表中数据对象位于项目列表的末尾。

USIM包含用作菜单项目列表标题的a标识符和可选的图标标识符。ME可使用此图标标识符指示用户进入工具箱菜单项列表。

ME除了使用a标识符或文本串之外，若USIM提供图标，ME还可以使用命令中图标限定符规定的图标。若命令细节指示的软键可用，并且ME支持SET UP MENU使用软键，以及图标数不超过可用的软键数，那么ME将这些图标作为软键显示。

USIM可以在菜单项目列表的最后包含一个“下一个动作指示器”数据对象项目，可使ME提示用户执行项目选择的结果。

需要注意的是一个主动式USIM命令中发送的最大数据量是256字节。因此在项目数和描述文本长度（SET UP MENU命令的a标识符和项目的文本字符串）之间需要权衡，例如，若项目数最大值为18，则每个文本串的平均长度为10字节。

若此命令的帮助信息可用，且用户指示需要某菜单项的帮助信息，ME 就使用菜单选择机制通知 USIM 请求帮助。

24. SELECT ITEM，选择菜单项

UICC提供一套菜单项目列表供用户选择，每项由一个短标识符，一个文本串，以及可选的图标标识符组成，在项目图标标识符列表中数据对象位于项目列表的末尾。

UICC应包含用作菜单项目列表标题的a标识符和可选的图标标识符。在菜单项目列表最后有一个“下一个动作指示器”数据对象，可使ME提示用户执行项目选择的结果。

ME使用UICC内的a标识符作为项目列表的题目。ME除了使用a标识符之外，若UICC提供图标，ME还可以使用命令中图标限定符规定的图标。若命令细节指示“软键选择可用”，并且ME支持SELECT ITEM使用软键，以及图标数不超过可用的软键数，那么ME将这些图标作为软键显示。

注意：一个主动式USAT命令中发送的最大数据量是256字节。因此在项目数和描述文本长度（SELECT ITEM命令的a标识符和项目的文本字符串）之间需要权衡，例如，若项目数最大值为18，则每个文本串的平均长度为10字节。

25. SEND SHORT MESSAGE，发送短信

此命令定义两种类型[9]：

- 用 SMS-SUBMIT 消息或 SMS-COMMAND 消息向网络发短消息，用户数据为透明传输；
- 用 SMS-SUBMIT 消息向网络发短消息，文本由 ME 打包。

若文本被打包，则 UICC 提供的文本串长度不超过 160 个字符。可以采用 SMS 默认 7bit 编码字符表，并打包成 8bit 字节。数据编码方案字节中指出的数据编码应是“默认字符表”。UICC 给出的文本长度值（SMS TPDU 的一部分）应指出文本串中 7bit 字符的数目，命令细节是“不要求打包”。

UICC可发送8bit字符的短消息，命令中应指出不要求打包。数据编码方案字节中指出的数据编码应是“8 bit”，文本串长度不应超过140个字节，并且SMS TPDU 中的文本串长度值应指出文本串的字节数。

若ME支持UCS2编码，UICC可发送16bit字符的短消息。UICC提供的文本串长度不超过70个字符，并应采用16 bit的UCS2字符格式。UICC给出的文本长度值（SMS TPDU的一部分）应指出文本串中16bit字符的数目。命令细节是“不要求打包”。

UICC可发送SMS命令短消息，可算作打包文本。SMS TPDU中应指明是SMS-COMMAND, 命令细节是“不要求打包”。

若要求ME打包，UICC提供的文本串长度不超过160个字符。采用SMS默认7bit编码字符表，bit8置0。UICC给出的文本长度值（SMS TPDU的一部分）应指出文本串中字符的数目。在向网络发送短消息之前，ME应打包文本串并将数据编码字节置为“默认字符表”。

若ME支持SMS-MO，应将数据以SMS TPDU发往目的地址。从网络收到SMS RP-ACK或RP-ERROR 短消息后，ME就发送含命令执行结果值的TERMINAL RESPONSE命令（指示短消息传输成功或失败）通知UICC。若UICC提供a标识符，ME收到SMS RP-ACK或RP-ERROR 短消息后不给用户提供任何信息。

若网络没有成功接收短消息TPDU（例如收到CP-ERROR），ME应发送含“网络当前不能处理命令”结果值的TERMINAL RESPONSE命令通知UICC。若UICC提供空值a标识符，在网络接收不成功的情况下，ME不给用户提供任何信息。

26. SEND SS/USSD，发送SS/USSD

ME收到SEND SS命令之后便开始执行，只有在SIM卡提供a信息时，才将SS的结果信息显示给用户。

即使允许固定拨号（FDN）业务，SEND SS主动式命令中包含的补充业务控制字

符串也无需再核对FDN列表。ME收到此命令，就判断是否可以执行。

若ME支持“最后一次拨号”业务（Last Number Dialed），ME不将此命令中由UICC发送的补充业务控制字符串存入EFLND中。

ME收到SEND USSD命令之后也是便开始执行，并且也是根据SIM卡提供的a信息，来判断是否将信息显示给用户

27. MORE TIME，时间延长

处理时间过长，会危及 3G 正常操作、导致时钟停止并阻碍正常的处理，提供此命令可以允许 USAT 任务有更多的处理时间。

当 ME 收到该命令后，不会采取特别的行动，也不会影响其他的操作。ME 在收到 MORE TIME 命令后，给 USAT 发送 TERMINAL RESPONSE（OK）来结束该命令。

28. SET UP CALL，建立通话

此命令定义 3 种类型：

- 在没有其他呼叫时,建立呼叫；
- 保持所有其他的呼叫（如果有），建立呼叫；
- 切断所有其他的呼叫（如果有），建立呼叫。

对于以上每种类型，USIM 可请求使用自动重拨机制。USIM 也可为重拨机制请求可选的最大持续时间，当然 ME 应至少尝试建立一个呼叫。

除被叫用户号码，命令中可给出性能配置参数（给出请求呼叫的承载能力）和被叫用户子地址。ME 在向网络请求呼叫建立时需使用这些参数。在呼叫已经连接后，ME 还可将命令中给出的 DTMF 值发送给网络。ME 不能在本地产生 DTMF 音频并播放给用户。

USIM 可以提供‘12’作为被叫号码，请求 ME 建立紧急呼叫，USIM 不能使用 EF_{ECC} 中的号码建立紧急呼叫。

即使允许固定拨号(FDN)业务，SET UP CALL 主动式命令中给出号码也无需再核对 FDN 列表。

若 ME 支持“最后一次拨号”业务（Last Number Dialed），ME 不应将此命令中由 USIM 发送的呼叫建立细节(被叫号码和相关参数)存入 EF_{LND} 中。

29. GET INKEY

此命令指示 ME 显示文本或图标，并且希望用户键入一个字符作为响应。由用户键入的响应会由 ME 透明传输给 USIM。

文本字符串为下列3种格式之一：

- SMS默认字符的打包格式；
- SMS默认字符的非打包格式；
- UCS2字符格式。

用户键入的响应可采用下列 3 种格式之一：

- 仅数字（0～9，*，#，+）；
- SMS 默认字符表的字符；
- UCS2 字符表的字符。

收到命令，ME 就显示文本。ME 允许用户键入一个字符作为响应。

若ME的人机界面为了选择一个字符需要多次按键，ME厂商就需要指示用户如何结束操作（如按SEND键或OK键），并将用户输入的字符显示在屏幕上。

对数字（0～9，*，#，+）和SMS默认字符集而言，要用非打包格式的SMS默认字符对响应进行编码。

3.5 处理未知的，无法预料的和错误的信息

此处所描述的处理过程适用于 BER-TLV 和 SIMPLE-TLV 数据对象。该处理过程专门描述当 ME 和 USIM 接收到不完全符合其设计标准的主动式命令和响应时，该如何进行处理。最终将依靠结果字段中的大致结果给 USIM 发出响应。

如果 ME 给 USIM 发送的 FETCH 或 TERMINAL RESPONSE 命令中含有 UICC 不能理解的值，USIM 将发送恰当的 SW1/SW2 错误响应字段。当前的主动式处理会被完全考虑，且无论是 ME 还是 USIM 都不能进行进一步的处理。既然这样，除非完成“大致结果”处理，否则 USIM 认为命令没有执行并且相关的特定主动式命令发生了永久性错误。如果命令已执行但“结果附加信息”字段无法识别，USIM 会在当前 3G 会话的最后阶段再次尝试该命令。

如果 USIM 已经拥有足够的信息，那么它将继续向下进行..

包含如下类型：

1) 消息太短：

接收到的信息没有完整性标识，其长度将被忽略。

2) 缺少最小化信息：

如果接收到的短消息没有全部的命令，当所有的最小化设置都存在时，接收者将完成命令并发送“命令执行，有信息丢失”的报告。如果最小化设置不完整时，ME 将发送“出错，响应值丢失”的响应。

3) 未知标识值：

如果接收到的 BER-TLV 标识可识别但其中的 SIMPLE-TLV 部分有未知标识，当拥有完整的最小化设置时，“标识识别”字将决定如何接受数据。

如果标识识别字有一个未知标记设为‘1’，且 ME 既不能识别也不能期望短消息中还有更多的 SIMPLE-TLV 数据信息，此时它将发送“ME 不能识别命令数据”的响应。

如果标识识别字的标记设为‘0’，ME 将读取后续的长度字段并且忽略数据。此时，ME 在不能识别 SIMPLE-TLV 部分的情况下也能执行命令。它将发送“命令部分执行”的响应。

4) 无法预料的标识值：

如果接收到的 BER-TLV 数据标识可识别，但与短消息在何处关联无法预料，此时将丢弃该部分。然后与对待未知标识做同样的处理。

如果接收到的数据有一个已经接收过的标识，此时将使用第一种情况并将丢弃后续的所有情况。

5) 长度错误：

如果 SIMPLE-TLV 数据的总长度与 BER-TLV 数据中给出的长度不一致，那么整个 BER-TLV 数据将被拒绝。终端响应的结果将出现错误“ME 不能识别命令数据”。

如果 BER-TLV 数据的长度比响应数据长度短，ME 将忽略位于完整 BER-TLV 数据之后的响应数据。

6) 内容无法理解：

如果一个 SIMPLE-TLV 数据对象中包含一个作为保留的域值，则整个 SIMPLE-TLV 数据将被视为无效。此时将根据相关标记的标识识别字判断是拒绝整个 BER-TLV 数据还是忽略部分 SIMPLE-TLV 数据。

如果 BER-TLV 内容中包含 RFU 字，会将其忽略。

7) 扩展数据长度：

如果一个 SIMPLE-TLV 数据的长度比期望的长，例如附加了许多信息，接收者将忽略数据结尾的额外信息。可以通过查找数据的长度域找到数据的结尾。

第四章　网络部分设计

网络部分中含有 CMPP 模块和 OTA 命令处理模块两大部分，它们之间的数据格式和命令遵循不同的协议规范，CMPP 模块和 OTA 命令处理模块主要的作用之一就是进行不同协议规范之间的格式转化，同时保证传递的命令含义保持不变。

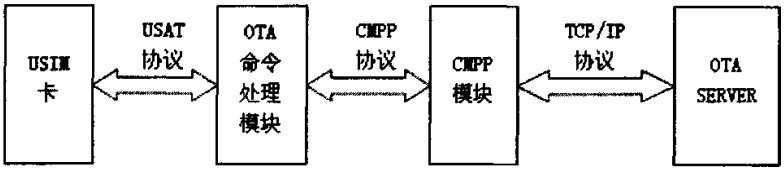


图 4-1 测试系统逻辑结构图

4.1 CMPP 模块

4.1.1 交互过程中的应答方式

在 SP 与 ISMG 之间、SMC 与 ISMG 之间及 ISMG 之间的交互过程中均采用异步方式，即任一个网元在收到请求消息后应立即回送响应消息。举例如图所示[5]：

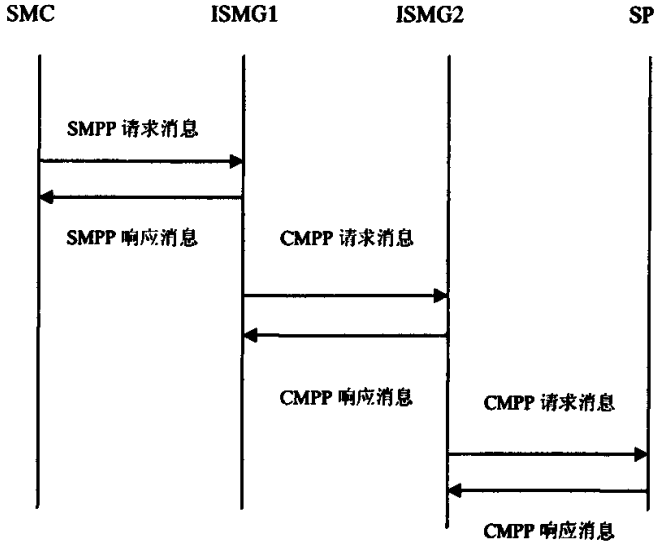


图 4-2 异步交互方式示意图

4.1.2 消息结构

每一个消息包含消息头和消息体两个部分，消息头固定长度为 12 字节，其他消息长度各异，但是同一类型消息的长度是固定的。所有消息的各个字段基本上有 3 种类型：

- Unsigned Integer：无符号整数；
- Integer：整数，可为正整数、负整数或零；
- Octet String：定长字符串，位数不足时，如果左补 0 则补 ASCII 表示的零，如果右补 0 则补二进制的零。

4.1.3 消息头

消息头由 3 个 Unsigned Integer 字段组成，包括：

1）4 字节的 Total_Length （Unsigned Integer），包含此消息的总计（包括了头部分）长度。

2）4 字节的 Command_Id（Unsigned Integer），指明此消息到底是什么消息，就是消息的枚举值。应用程序根据此值确定本数据包到底是什么消息，从而可以按照确定的消息类型，解析余下的消息体。

3）4 字节的 Sequence_Id（Unsigned Integer），指明了此数据包在发送此消息端的唯一编号。这个唯一编号，实际上可以看作流水操作编号。因为分析到交互模式，SP 发送数据到 ISMG，不是每发送一次就停下来等待 ISMG 的回复，而是“一下子”发送多个数据包过去，然后等待 ISMG 的回应。然而，怎么知道回应的消息是到底对应之前发送过去的消息中的那一条？本字段就是解决此难题。SP 按照编号发送消息过去，等待 ISMG 的回应，通常情形下回应消息数据结构都表明本消息回应的是 SP 发出的哪一条消息，这个对应就是依靠 Sequence_Id。它并不要求一定要严格唯一，但是在给定的一段时间内，必须唯一。如果是需要 SP 回答的消息，SP 也必须将 ISMG 发送过来的消息的 Sequence_Id 填入相应字段，表明这是某个消息的回应。SP 端和 ISMG 端 Sequence_Id 都没有确定具体的算法。SP 可以采用数据库的唯一 Id 作为此值。

4.1.4 消息体

消息体的种类比较多，CMPP 消息也有很多种，SP 同 ISMG 之间交流这些消息。大体上这些消息发出后，对方往往需要回复一个应答 RESP 类消息。注意，这些消息大多具有方向性，只能够从一端到另一端，除了两端都能够发出的消息，其余的消息不可反方向进行。并且消息体长度根据消息不同，长度不一。

按照传递与接收消息实体分类，可以分为三大类：

1） 信息资源站实体(SP)与互联网短信网关(Internet Short Message Gateway，ISMG)间的接口协议；

2） 互联网短信网关(ISMG)之间的接口协议，譬如移动各省、市之间的短信息交换通过 ISMG 之间进行；

3） 互联网短信网关(ISMG)与汇接网关(Gateway Name Server，GNS)之间的接口协议，譬如跨省之类的短信需要 GNS 的帮助指出当前 ISMG 该如何传递短信。

其中，后两方面属于移动短信息系统内部实现，对于 SP 来讲大概可以“透明”来看待，只要实现了 SP 同 ISMG 的正确交互，就可以实现接入移动网短信系统，所以我们关心的只是 SP 端的开发细节。

SP 端的开发使用到的命令如下：

1. *CMPP_CONNECT*，该消息由 SP 发送给 ISMG，CMPP_CONNECT 操作的目的是 SP 向 ISMG 注册，作为一个合法 SP 身份，此消息需要向 ISMG 发出验证信息，验证方式采用 MD5 加密方式，若注册成功后即建立了应用层的连接，否则 ISMG 会立即断开 Socket。此后 SP 可以通过此 ISMG 接收和发送短信。
2. *CMPP_CONNECT_RESP*，该消息由 ISMG 发送给 SP，ISMG 对 CMPP_CONNECT 消息的回复，无论是否验证成功。如果未通过，会在消息中包含参考信息，但 ISMG 会立即断开连接。
3. *CMPP_ACTIVE_TEST*，这个消息通信双方都可以发出，目的是在没有其他消息发送时，保持双方的通信链路的连接，避免系统认为通信通道已经关闭。每一个收到此消息的实体应当返回 CMPP_ACTIVE_TEST_RESP 消息，以“礼节性”表示自己的还在通信，维持数据连接有效性。
4. *CMPP_ACTIVE_TEST_RESP*，这个消息是通信双方都可以发出，对通信的另一端的 CMPP_ACTIVE_TEST 消息的回复。
5. *CMPP_SUBMIT*，该消息由 SP 发送给 ISMG，在正确建立了数据连接后，SP 向 ISMG 发送一个 SMS 数据包。接收到此消息后，ISMG 以 CMPP_SUBMIT_RESP 消息作为回答。如果在一定时间间隔内（移动给出的参考值 60 秒）内未得到消息回应，那么 SP 需要重新发送此数据包，以确保消息得到投递。如果重发达到 3 次后仍然得不到回应，SP 端应该考虑可能 ISMG 已经失效，应当停止发送短消息。
6. *CMPP_SUBMIT_RESP*，该消息由 ISMG 发送给 SP，同时返回一个“收条”(源 CMPP_SUBMIT 消息的 ISMG 端的标示 MSGID)给 SP，表示“ISMG 已经确认收到这条消息”。收到此消息后，SP 需要保留此“收条”，因为后面 ISMG 会最终

报告本消息是否正确发送到用户手机。那个报告就是以此消息的“收条”作为确认那一条消息的。

7. *CMPP_QUERY*，该消息由 SP 发送给 ISMG，这个查询不是查询单条消息的，是查询 SP 发送给 ISMG 的短信的业务情况。可以查总计数，还可以分类查询，基本是发起对移动 SMS 业务数据库的查询统计。
8. *CMPP_QUERY_RESP*，该消息由 ISMG 发送给 SP，ISMG 将查询的数据返回给 SP。
9. *CMPP_CANCEL*，该消息由 SP 发送给 ISMG，是 SP 发起的取消某条消息的命令消息，其中包含了之前已经发送给 ISMG 消息的“收条”以便 ISMG 可以确定是那一条消息。如果消息已经发送给用户了，那么此消息/命令会无效，ISMG 返回失败。
10. *CMPP_CANCEL_RESP*，该消息由 ISMG 发送给 SP，ISMG 返回对 CMPP_CANCEL 的回复，并告知是否删除成功。
11. *CMPP_DELIVER*，该消息由 SP 发送给 ISMG，当有 MO 或者状态报告时，ISMG 发送此消息。注意，此消息的数据可以是用户手机发送给 SP 的消息，也可是对于之前 SP 发送到 ISMG 的短信的最终状态的回复，报告短信的最终状态。
12. *CMPP_DELIVER_RESP*，该消息由 SP 发送给 ISMG，SP 回复告知收到 CMPP_DELIVER 消息。要指出 SP 报告的 CMPP_DELIVER 消息的 MSGID，以便 ISMG 知道那一条消息 SP 已经确认收到。
13. *CMPP_TERMINATE*， SP 和 ISMG 都可以主动发送该消息给对方，表示一端由于某种原因需要终止当前的数据连接。终止后，要经过重新验证之后才可以发送 SMS 数据消息。
14. *CMPP_TERMINATE_RES*，SP 和 ISMG 是都可以发送该消息给对方，通知对方本端已经做好撤除连接的准备。

4.1.5 CMPP 操作

开发工具通过界面编辑短信，发送至 OTA Server，并且在 OTA Server 发送的信息处理之后，将其传送给 USIM 卡。用户可以根据菜单选择业务，USIM 卡也可以主动发起命令，并且透明地发送短信到目的地址，或是接收来自 OTA Server 的命令。

4.1.5.1 端口

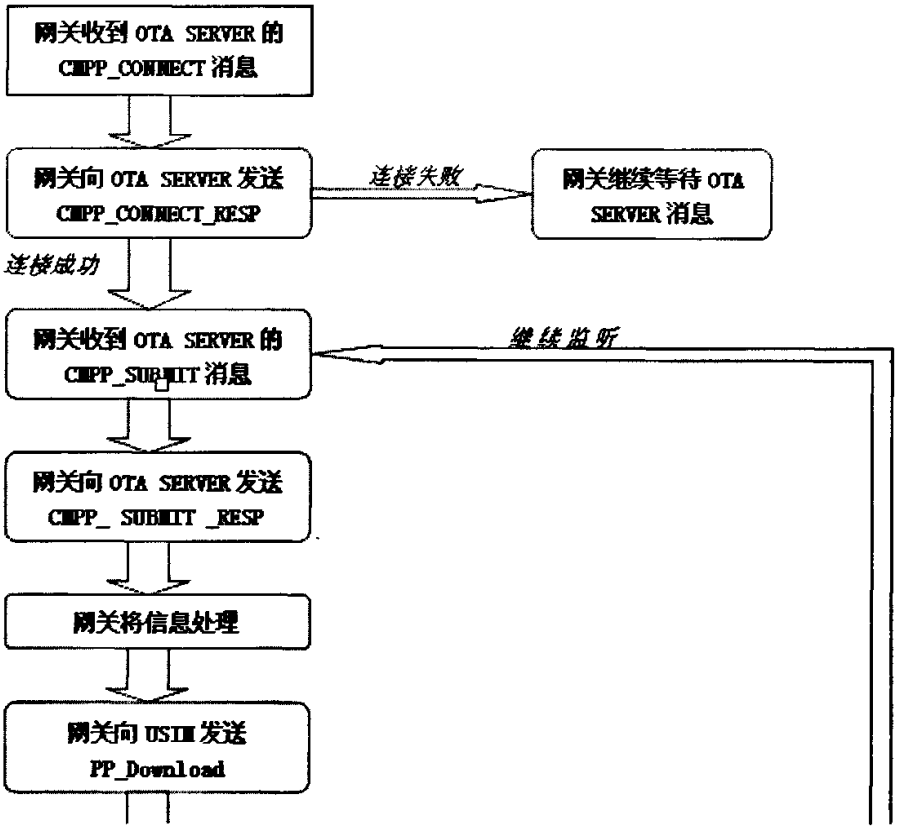
交互过程涉及到长连接/短连接，以及发送信息/接收信息，故需要定义四个端口进行不同需求的操作[5]：

表 4-1 端口应用表

端口号	应用
7890	长连接（SP 与网关间）
7900	短连接（SP 与网关间或网关之间）
7930	长连接（网关之间）
9168	短连接（短信网关与汇接网关之间）

4.1.5.2 系统逻辑流程设计

1. 信息资源站实体(SP)与互联网短信网关(ISMG)间消息处理流程（网关与 OTA Server 发送消息处理流程），详细流程见图 4-3。



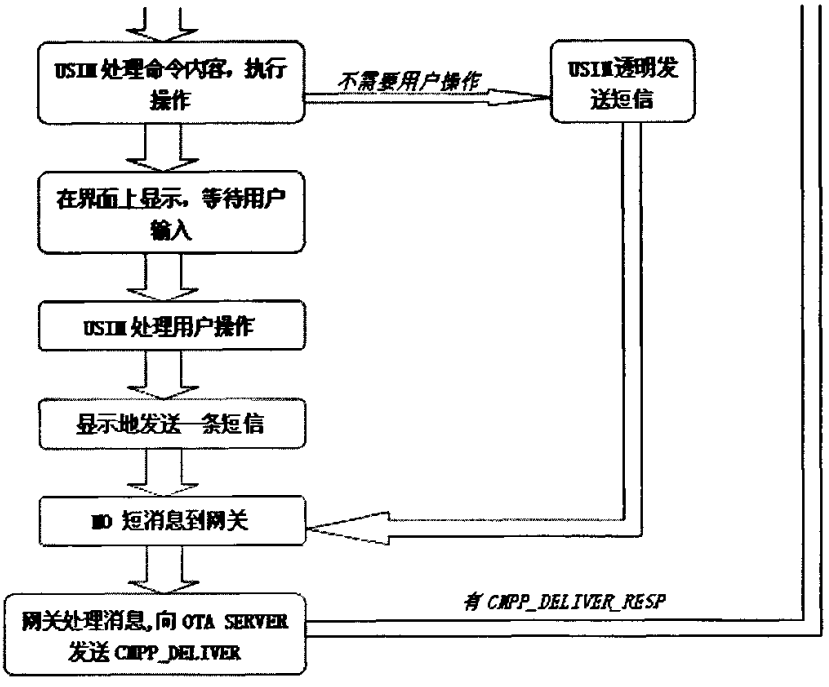


图 4-3　SP 与 ISMG 间消息处理流程图

2. OTA Server 端发送信息处理流程

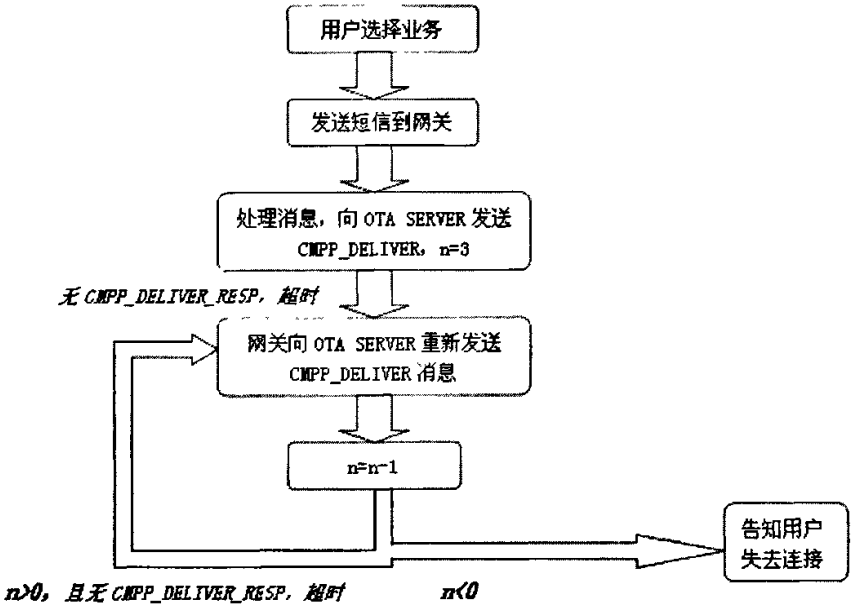


图 4-4　OTA Server 端发送信息处理流程图

3. 在连接过程中应该保持长连接状态

当信道上没有数据传输时，通信双方应每隔时间 C 发送链路检测包以维持此连接，当链路检测包发出超过时间 T 后未收到响应，应立即再发送链路检测包，再连续发送 N-1 次后仍未得到响应则断开此连接。在程序中根据协议[2]建议，取值为：C=3 分钟，T=60 秒，N=3。

在连接状态中，若在间隔时间内信道上没有数据传输，则由网关发送 CMPP_ACTIVE_TEST 命令到 OTA Server 端，同时网关准备接收 CMPP_ACTIVE_TEST_RESP 命令。

4. TETMINATE 命令

用户执行关机操作，退出操作软件或是选择相应选项后，网关向 OTA Server 发送 CMPP_TETMINATE 命令，随后断开与 OTA Server 之间的连接。

4.2 OTA 命令处理模块

OTA，即 Over－the－Air Technology，空中下载技术，是通过移动通信（GSM 或 CDMA）的空中接口对 SIM 卡数据，及其应用进行远程管理的技术。

OTA 技术的应用，使得移动通信不仅可以提供语音和数据服务，而且还能提供新业务下载。这样，应用及内容服务商可以不受平台的局限，可以不断开发出更具个性化的贴近用户需求的服务，如信息点播、互动娱乐、位置服务以及银行交易等。通过 OTA 空中下载技术，手机用户只要进行简单操作，就可以按照个人喜好把所提供的各种业务菜单利用 OTA 机制下载到手机中，并且还可以根据自己的意愿定制具体业务。

4.2.1 菜单下载业务的定义

OTA 卡菜单下载业务是指用户可以根据自己的需要，随时增加或删除自己手机卡上的移动梦网短信业务菜单，以此实现梦网服务的个性化和业务更新的实时性，同时使运营商能更方便、迅速地全面展开各项梦网短信服务。

OTA 菜单下载的实现借助于 STK 功能和短消息通道，支持空中下载的手机卡提供可行的人机接口界面供用户发起下载申请，OTA 应用下载服务器根据用户请求，以数据短消息（Data Download 模式）的形式将相应的服务下载内容发给用户手机，并将下载数据透明地传递给用户手机卡，之后手机卡对下载内容进行组织存贮，实现相应的 STK 卡菜单管理。

4.2.2 功能描述

此模块主要可以完成如下功能：

1. 支持 CMPP2.0 协议规范，可以实现短信网关连接，进行收、发短信；
2. 选择、操作 USIM 卡的 STK 菜单；
3. 接收 USIM 卡返回的 OTA 操作请求数据，并封包为 CMPP 协议中定义的数据，之后发送到 OTA Server；
4. 接收 OTA Server 发送的信息，根据 CMPP 协议解包后，取出其中数据项，通过 PP-Download 命令向 USIM 卡发送 OTA 操作和响应数据；
5. 支持 USIM 卡向 OTA Server 注册，可以完成刷新列表，菜单删除通知，菜单下载功能。

4.2.3 流程描述

从卡的角度，根据命令请求的发出与接受可以把整个流程分为卡端显示发起请求、卡端收到请求两大部分：

1. 卡端显示发起请求，详细流程见图 4-5。

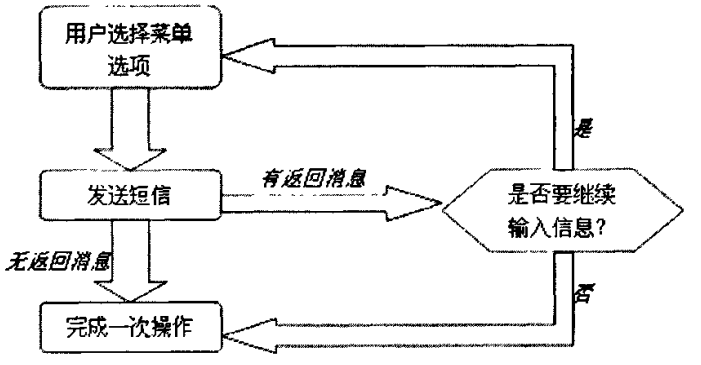


图 4 -5 卡端显示发起请求流程图

2. 卡端收到请求，详细流程见图 4-6。

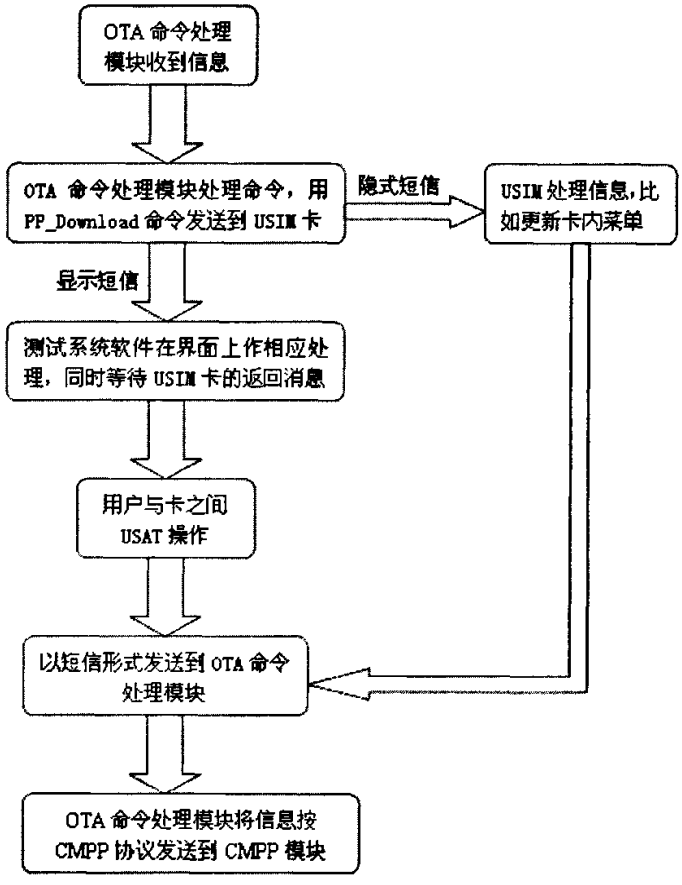


图 4-6 卡端收到请求图

4.2.3 功能详述

1. 用户卡注册

当用户首次进入 USIM 卡 OTA 菜单第一级目录时，USIM 卡自动向 OTA 应用下载服务器发送 OTA 服务注册信息。服务器收到卡端发来的注册信息后，向用户卡发送注册确认信息。卡片收到确认信息以后将不再进行注册（如未收到确认信息，用户每次进入一级菜单时都要发送注册信息，直到收到注册成功确认消息为止）。若卡片注册未成功，则不允许用户进行菜单管理（如下载、删除）。注册信息的发送不会影响用户的其他正常操作。检测通过后，服务器用新的用户注册信息覆盖原有用户注册信息，并下发注册成功确认消息。

OTA 系统数据库中的用户注册信息必须包含以下内容：

- 卡商代码：由运营商给不同 USIM 卡供应商分配统一编号；

- 协议版本号：协议版本号代表该协议版本；
- 用户标识：是否有 OTA 卡标识及业务品牌；
- 卡片发行批号：卡片发行的不同批次编号；
- 卡片可用下载空间：用户卡上的当前可用下载空间；
- 卡片序列号：用于用户识别及密钥分散；
- 用户菜单记录：用于记录用户卡上的菜单状况；
- 备份用户菜单记录：用于 OTA 菜单恢复时恢复菜单使用。

2. MO 下载

MO （Short Message Mobile Originate，SM_MO），短信发送，短信从手机用户端发送到目标 SP，具体流程如下：

1） 用户通过操作点击 USIM 卡菜单管理选项进行下载菜单请求；
2） USIM 卡判断当前卡内是否有足够的剩余空间用于下载用户选择的菜单，若卡内剩余空间不足，则提示用户相关信息后退出，否则将用户下载菜单申请发送给短消息网关；
3） 短消息网关将用户申请透明传递给 OTA 应用下载服务器；
4） OTA 应用下载服务器的接收程序接收到申请后，将申请数据交给数据处理模块；
5） 数据处理模块检查收到数据的完整性、合法性。验证未通过，则流程中止；
6） 从数据库中的 MO 菜单数据表中取得与申请数据对应的菜单数据，将数据提交给发送程序；
7） 发送程序将数据提交给短消息网关，同时将用户下载菜单的情况写入数据库的用户卡信息表中和日志表中；
8） 短消息网关将下载的业务数据以短消息的形式发送到用户手机；
9） 用户 USIM 卡接收到菜单数据短信后，首先验证菜单数据的完整性和合法性，若菜单数据未通过验证则被丢弃，反之则由用户 USIM 卡完成菜单数据的下载。

如果用户在 USIM 卡等待下载数据的中间发起另一次下载申请(卡端可让用户选择是等待上次下载完成，还是发起新申请)，则中断上一次下载流程。

3. 下载服务列表更新

服务列表更新的步骤如下：

1）用户通过操作点击 USIM 卡菜单管理选项发送列表更新请求；
2）OTA 应用下载服务器的接收程序接收到申请后，根据用户信息表将列表数据

提交给发送程序；

3）发送程序将数据提交给短消息网关，同时将用户下载菜单的情况写入数据库的用户卡信息表中和日志表中；

4）短消息网关将下载数据发送到用户手机，用户 USIM 卡接收到数据后进行循环更新列表。

列表更新是对用户卡内的下载菜单列表记录进行更新。USIM 卡接收到服务器端下发的列表更新数据后，将循环更新列表。列表空间按目录（第一级菜单）划分，每一目录下列表空间固定为 5 条，即每个目录下的下载菜单列表固定为 5 个，卡片列表总空间条数为 5 倍的卡片最大目录数。每一目录下列表更新时，仅更新该目录下列表，不能影响其他目录下列表。并且服务器按目录将列表更新分类，以 5 个列表应用为 1 页，实行分页管理。卡端用从服务器收到的当前列表页码更新卡内当前列表页码记录，并用于下次列表更新请求时使用。

USIM 卡更新列表后，已下载的应用业务可继续使用，同时已经下载的服务不应出现在下载列表里。当用户删除服务时，USIM 卡首先判断下载列表是否存在空记录，如存在，则在删除服务应用数据的同时将该服务的列表添加入下载列表；否则仅删除服务应用数据，对下载列表不做改变。

4. 菜单删除

菜单删除，即删除 OTA 菜单中的业务项，详细流程如下：

1）用户通过操作点击 USIM 卡菜单管理选项删除菜单；

2）USIM 卡会显示本目录下所有可以删除的菜单名称，用户选择要删除的项；如果用户所欲删除的业务已全部删除完毕，则跳到第 4 步；

3）USIM 卡执行删除操作，提示用户是否继续删除其它菜单业务，如果选择继续删除则回到第 2 步，否则进行第 4 步；

4）把 SIM 卡内用户删除的信息组织成服务删除通知，并且上发到 OTA 服务器；短消息网关将服务删除通知透明传递给 OTA 应用下载服务器；

5）OTA 应用下载服务器的接收程序将接收到的服务删除通知写入数据库的用户卡信息表和日志表中。

5. 下载服务的管理

服务的管理可以分为空间管理和菜单管理两大部分：

1）空间管理：USIM 卡应完成对卡内剩余空间的统计，记录用户能够实际使用的空间。在用户发起下载申请时，如果 USIM 卡检测存贮空间不足，则终止下载申请，并提示手机用户。

2）菜单管理：USIM 卡应提供合理完善的菜单界面供用户完成下载申请。USIM 卡可以提供合理的机制供用户对下载的服务项目进行组织。对于已经下载的服务，USIM 卡不允许重复下载。用户下载到 USIM 卡里的服务应能够删除。

第五章 测试系统实现

5.1 实现环境

测试系统实现的硬件环境：

- 计算机，要求至少有一个 USB 接口，并且可以支持 Windows2000 操作系统；
- 3G 手机测试卡至少一张，本系统使用大唐电信集团公司的 3G 手机测试卡；
- 智能卡读卡机至少一台，本系统使用金普斯智能卡读卡器，型号为 GemPC USB-SL。利用智能卡读卡机从智能卡中读取或向智能卡写入信息。

测试系统实现的软件环境：

- Windows2000 操作系统，因为需要使用其中的的 winscard.dll 动态链接库文件；
- Visual Basic 编程环境，简称 VB，因为它是编程效率最高的一种编程方法，另外 VB 还是最快速、最简便的方法。

5.2 WINDOWS 智能卡工具包

在测试系统的实现过程中，用到了 Windows 操作系统中的智能卡工具包[10]：winscard.dll，它是个人计算机对智能卡读取相关程序的动态链接库文件，里面的函数比较多，在测试系统中使用的有：

1. 智能卡数据库查询函数：用来查询智能卡数据库。
   - ScardGetProviderId：获取给定的智能卡的主要服务提供者的标识符；
   - SCardListCards：获取以前被某个用户引入系统的所有智能卡列表；
   - SCardListInterfaces：获取由一个给定的智能卡提供的接口的标识符；
   - SCardListReaderGroups：获取以前被引入系统的读卡机组列表；
   - SCardListReaders：获取某个读卡机组中的读卡机的列表。
2. 智能卡数据库管理函数：用来管理智能卡数据库，并使用特定的资源管理器描述表更新数据库。
   - SCardAddReaderToGroup：向一个读卡机组中添加一个读卡机；
   - SCardForgetCardType：从系统中删除一个智能卡；

- SCardForgetReader：从系统中删除一个读卡机；
- SCardForgetReaderGroup：从系统中删除一个读卡机组；
- SCardIntroduceCardType：向系统中引入一个新卡；
- SCardIntroduceReader：向系统引入一个新读卡机；
- SCardIntroduceReaderGroup：向系统引入一个新读卡机组；
- SCardRemoveReaderFromGroup：从一个读卡机组中删除一个读卡机。

3. 资源管理器描述表函数：用来建立并释放被数据库查询、管理函数所使用的资源管理器描述表。
   - SCardEstablishContext：为访问智能卡数据库建立一个描述表；
   - SCardReleaseContext：关闭一个已经建立的描述表。
4. 智能卡追踪函数：用来寻找读卡机内的卡。
   - SCardLocateCards：寻找一个 ATR 字符串与提供的智能卡名称相符的卡；
   - SCardGetStatusChange：执行块，直到智能卡可用性改变为止；
   - SCardCancel：结束未完成的操作。
5. 智能卡及读卡机访问函数：用以连接到一个特定的智能卡并与之通讯。
   - SCardConnect：连接到一张卡；
   - SCardReconnect：重新建立连接；
   - SCardDisconnect：结束一个连接；
   - SCardBeginTransaction：启动一个事务，阻止其它应用程序访问智能卡；
   - SCardEndTransaction：结束一个事务，允许其它引用程序访问智能卡；
   - SCardStatus：提供某个读卡机目前的状态。

此外智能卡子系统还为应用程序及服务提供者提供了与智能卡连结的一些方法，包括：

1）应用程序可以调用 ScardConnect 函数来连接到一个放置在给定的读卡机里的卡。这是与智能卡建立通讯的最简单的方法。

2）应用程序可以在一个给定的读卡机组中搜索一个特定的智能卡。应用程序使用智能卡的名称标识该卡，并指定一个该智能卡可能放入的读卡机组列表。资源管理器使用 ATR 字符串，在读卡机列表中搜索所有与给定智能卡相符的卡，并将该卡的状态信息返回给应用程序。智能卡子系统从不提供 CUI，也不在获取 ATR 字符串之后提供与智能卡的交互。但它们能够为用户定位在要的智能卡或卡的类型上。这导致了将一个申请映射到一个指定的读卡机，并可以进一步映射到 I/O 的定向。

3）应用程序能够申请一个支持某些给定智能卡接口的智能卡列表。应用程序可以在前面的情况中使申请服务并从一个使用 T=0、T=1 以及原始协议的卡上返回数据。其中，T=0 协议是一个异步的面向字符的半双工传输协议；T=1 协议是一个异步的 ScardTransmit 面向块的半双工传输协议。

用该列表，这使得应用程序能够通过查询智能卡的功能找到相应的智能卡，而不需要知道它们的名称。

当应用程序查找一张卡时，它提供一组可能放有指定智能卡的读卡机名称。对于每一个在该序列中的读卡机，资源管理器提供下列信息：

- 该读卡机是否能够被这个程序使用。
- 是否有卡插入该读卡机，如果有的话，它的 ATR 字符串是什么。
- 找到的智能卡 ATR 字符串是否符合所申请的智能卡 ATR 字符串。

应用程序使用返回的信息来进一步提供智能卡过滤装置，对所有找到的智能卡进行过滤，或者提示用户选择需要的智能卡。

注意，如果一个或多个读卡机列表已经被其他应用程序以独占方式打开，那么访问这些列表上的读卡机将会失败。

5.3 运行

本测试系统可以运行在 Windows2000 系统或更高版本 Windows 操作系统上。

5.3.1 手机显示界面

屏幕为一个仿真手机屏幕，在这里可以通过鼠标、键盘实现菜单选择，短消息发送，信息浏览等功能。图 5-1 中的 1、2、3 分别显示了界面初始化、第一级菜单、和第二级菜单。，

图 5-1　模拟手机界面图

5.3.2 命令显示界面

在对手机模拟界面的操作过程中，在屏幕边上有窗口可以显示 USIM 卡执行的每条代码、执行之后的结果、是否有错误发生、以及显示详细的执行过程。

```
A0 A4 00 00   02 6F 45
+++++++ EF Selected ++++.....................................PASS
9F 0F
+++++++ Send command ++++....................................PASS
A0 C0 00 00   0F
+++++++Get EF Response++++...................................PASS
00 00 00 28   6F 45 04 00
11 FF 44 01   02 00 00 90
00
+++++++send ReadBinary++++...................................PASS
A0 B0 00 00   28
+++++++Get ReadBinary Response++++...........................PASS
56 58 FF FF   FF FF FF FF
```

图 5-2　命令执行细节图

5.3.3 用户选择界面

除了可以在模拟手机上进行操作之外，在这里也可以实现对卡的操作。不过此处主要是针对单步测试过程，并且这里的执行结果用户是可以选择的，具体选择内容本文在之前有描述。

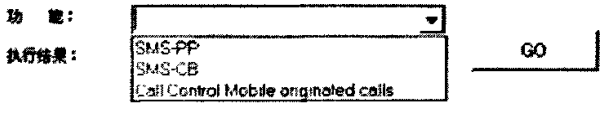


图 5-3　单步测试选择界面图

5.3.4 基本信息显示

在卡进行全面测试之前，要对卡进行一次基本信息扫描，以得到卡的基本信息，有利于对卡的全面了解。

```
------------------------------------------------------
Testing getCardReaderInfo()
读卡器型号是：Gemplus GemPC430 0
读卡器默认时钟速率是：1100kHz
读卡器最大时钟速率是：1100kHz
读卡器默认数据速率是：1400bps
读卡器最大数据速率是：7210bps
------------------------------------------------------
Testing getCardInfo()
智能卡的ATR是：3B 3D 94 00 44 4D 54 11 01 02 50 03 85 44 50 20 00
智能卡的IMSI是：08 49 06 00 96 24 16 00 41
智能卡的ICCID是：56 58 00 67 80 31 60 49 00 41
智能卡的Ifhace是：03
```

图 5-4　基本信息界面图

5.3.5 CMPP 操作界面

在网络模块中，实现了有线环境代替无线环境，图 5-5 是初始化的主界面。其中具体内容如下。

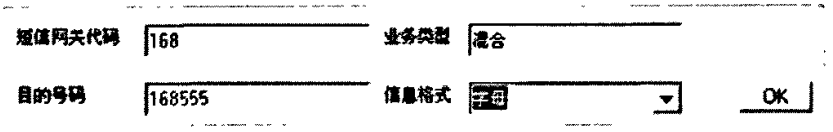
1）连接的OTA Server IP: 192.168.010.132，填入的 IP 信息是正测试系统在监听的 OTA Server 的地址。

2）OTA Port: 7777，表示测试系统通过此端口监听 OTA Server，此处端口号与协议[5]中使用的不同。

3）OTA状态：连接保持，表示目前程序与 OAT Server 之间的关系。

4）CMPP_ACTIVE_TEST次数： 5，当保持连接状态的时候，每隔固定时间要向 OTA Server 发送 CMPP_ACTIVE_TEST 命令，以继续保持长连接状态。此处表示 CMPP_ACTIVE_TEST 已经尝试发送了 5 次。

5）命令类型 [▼]
CMPP_CONNECT
CMPP_DELIVER
CMPP_SUBMIT
，表示可以执行的命令。这些命令均是 CMPP 命令，满足中国移动通信互联网短信网关接口协议（V2.0）。



6），是在选择具体命令之后，需要再进一步填写的命令细节。本框图显示的是选择 CMPP_ DELIVER 命令之后需要填写的命令细节。

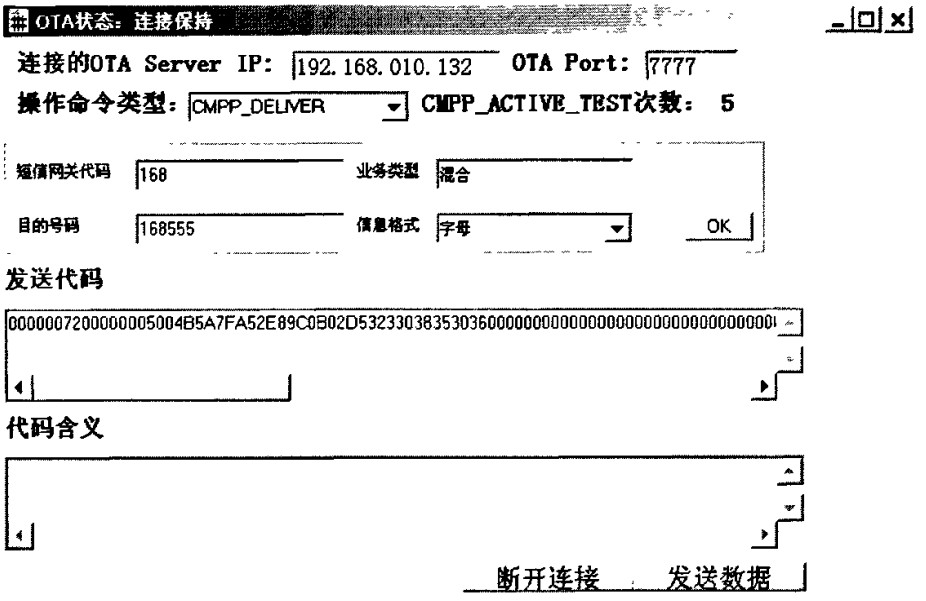


图 5-5　网络模块初始化界面图

5.3.6 OTA 命令界面

在图 5-5 中点击“OK”按钮之后，在“发送代码”下面生成图 5-6 中的字符串。点击“发送数据”按钮后，这些代码会发送到 OTA Server。

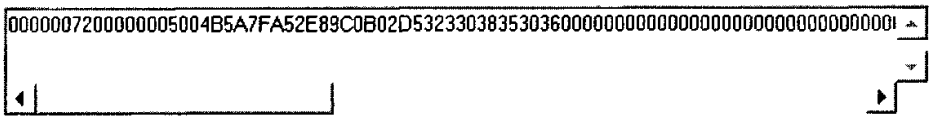


图 5-6　发送代码字符串

图 5-6 中这些字符就是将要发送的命令，此时它们是按照协议[2][3][4][5]中的要求，将信息用 16 进制的代码表示的。

数据发送之后，就可以收到 OTA Server 的响应消息，图 5-7 中的字符串就是在发送上述 CMPP_DELIVER 之后收到的响应消息。同时应在“代码含义”下方显示接收到的字符串的实际含义（由于时间关系未实现）。

接收代码

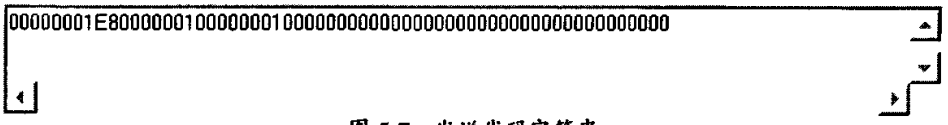


图 5-7 发送代码字符串

第六章 USAT 测试工具设计过程中遇到的问题以及解决方法

6.1 编码转换

编码方式在测试系统的实现过程中涉及比较多。通常在 APDU 中，可以采用三种编码方式来对发送的内容进行编码，它们是 7-bit、8-bit 和 UCS2 编码。

7-bit 编码用于发送普通的 ASCII 字符，它将一串 7-bit 的字符（最高位为 0）编码成 8-bit 的数据，每 8 个字符可“压缩”成 7 个；8-bit 编码通常用于发送数据消息，比如图片和铃声等；而 UCS2 编码用于发送 Unicode 字符。APDU 串的用户信息(TP-UD)段最大容量是 140 字节，所以在这三种编码方式下，可以发送的短消息的最大字符数分别是 160、140 和 70。这里，将一个英文字母、一个汉字和一个数据字节都视为一个字符。

需要注意的是，PDU 串的用户信息长度(TP-UDL)，在各种编码方式下意义有所不同。7-bit 编码时，指原始短消息的字符个数，而不是编码后的字节数。8-bit 编码时，就是字节数。UCS2 编码时，也是字节数，等于原始短消息的字符数的两倍。如果用户信息(TP-UD)中存在一个头参数(基本参数的 TP-UDHI 为 1)，在所有编码方式下，用户信息长度(TP-UDL)都等于头长度与编码后字节数之和。如果采用 GSM 03.42 所建议的压缩算法(TP-DCS 的高 3 位为 001)，则该长度也是压缩编码后字节数或头长度与压缩编码后字节数之和。

需要指出的是，7-bit 的字符集与 ANSI 标准字符集不完全一致，在‘0x20’以下也排布了一些可打印字符，但英文字母、阿拉伯数字和常用符号的位置两者是一样的。用上面介绍的算法收发纯英文短消息，一般情况应该是够用了。如果是法语、德语、西班牙语等，含有“å”、“é”这一类字符，则要按上面编码的输出去查表，具体格式请参阅 GSM 03.38 中的规定。

UCS2 编码是将每个字符(1-2 个字节)按照 ISO/IEC10646 的规定，转变为 16 位的 Unicode 宽字符。在 Windows 系统中，特别是在 2000/XP 中，可以简单地调用 API 函数实现编码和解码。如果没有系统的支持，比如用单片机控制手机模块收发短消息，只好用查表法解决了。

还有一处也是需要相当注意的地方：在 CMPP 模块中，进行测试系统与 OTA Srever 之间的通信时。这里的数据传递不需要经过特殊处理，是按照字符形式，直接传递就可以。

6.2 字符串长度

在测试系统与卡进行交互操作的过程中，字符串长度这个参数格外重要。因为它不仅告诉我们一整条命令的长度，以便我们可以将数据完整取出，而且还在每条数据中间也会有大量的字符串长度参数出现，它们分别属于不同的功能参数。比如在菜单项选择中，每一个菜单项均有一个字符串长度参数，来保证其可以准确翻译。但是由于目前不同卡商的卡，多多少少存在一些与 3GPP 规范不完全符合之处，在字符串长度这里的问题比较明显。

协议规定字符串长度表示的内容在小于 128 时，使用两位的 16 进制代码表示即可；但是当大于 128 时，就要使用 4 位 16 进制的数字表示，前两位为‘81’，后面为实际长度。有的卡是按照协议要求的，有的没有。这样就给测试系统批量执行带来了难处，所以此部分暂时未做。

6.3 显示菜单顺序

从卡中读出的菜单信息是由菜单项 ID，菜单内容，以及还有可能包含菜单项的图标分别组成的。菜单项 ID 是菜单中某一项在同级菜单中的唯一标识，菜单内容是显示给用户的菜单操作名称。

因为卡是将这三项信息分别放在了三个字段中表示，而菜单项是需要按照菜单项 ID 的顺序递增排列，所以在处理的时候要特别注意它们的对应关系。否则很容易出现选中项目 1，而执行项目 2 的情况。这样的问题在程序调试的过程中也不容易发现，还有菜单项 ID 不是连续的数字。

结合代码我的处理方法是，建立一个空数组，将菜单项 ID，菜单内容，以及菜单项图标按照“菜单项 ID***菜单内容***菜单项图标”的格式处理之后，再按照菜单项 ID 进行递增顺序存储。所有的菜单项在生成以后，需要按照一定顺序保存在程序中，以后对菜单的操作就不再是需要 USIM 卡进行建立，而是直接从程序中读出来。

6.4 进制转换问题

在卡、程序、OTA Server 的信息传递中，以及在命令流程的详细执行过程中，都会遇到进制转换问题。在显示的时候，使用 2 位长度的 16 进制数表示相应信息；USIM 卡发送与接收的信息是 0 到 255 的整数表示的代码；在主动式命令信息填写的时候，会用到相当多的 2 进制数据，这些需要转换为 16 进制数以后才可以发送出去。

在操作过程中用户填写的数据均是 10 进制的，另外程序中存在 2 进制，10 进制，

16 进制相互转换的函数，可以对相应数据进行处理，在显示命令或者是参数的时候按照多进制的显示要求进行了相应处理。在程序中传递、显示的数据均是 2 位 16 进制的字符串，在仅有 1 个字节长的时候添加一个‘0’字节。这样会使得界面显示的数据整齐，便于查找和比较数据。

6.5 APDU MODE 下发送和接收短消息的注意事项

APDU 串表面上是一串 ASCII 码，由‘0’～‘9’、‘A’～‘F 这些数字和字母组成。它们是 8 字节的十六进制数，或者 BCD 码十进制数。APDU 串不仅包含可显示的消息本身，还包含很多其它信息，如 SMS 服务中心号码、目标号码、回复号码、编码方式和服务时间等。

发送和接收的 APDU 串，结构是不完全相同的。

1．发送。例如 SMSC 号码是+8613800250500，对方号码是 13811858840，消息内容是“Hello!”。从手机发出的 PDU 串可以是：08 91 68 31 08 20 05 05 F0 11 00 0D 91 68 31 18 81 85 48 F0 00 00 00 06 C8 32 9B FD 0E 01。对照规范，具体分析见表 6-1。

表 6-1 发送消息时 APDU 字符含义

分段	含义	说明
08	SMSC 地址信息的长度	共 8 个八位字节(包括‘91’)
91	SMSC 地址格式(TON/NPI)	用国际格式号码(在前面加‘+’)
68 31 08 20 05 05 F0	SMSC 地址	8613800250500，补‘F’凑成偶数个
11	基本参数(TP-MTI/VFP)	发送，TP-VP 用相对格式
00	消息基准值(TP-MR)	0
0D	目标地址数字个数	共 13 个十进制数(不包括‘91’和‘F’)
91	目标地址格式(TON/NPI)	用国际格式号码(在前面加‘+’)
68 31 18 81 85 48 F0	目标地址(TP-DA)	8613811858840，补‘F’凑成偶数
00	协议标识(TP-PID)	是普通 GSM 类型，点到点方式
00	用户信息编码方式(TP-DCS)	7-bit 编码
00	有效期(TP-VP)	5 分钟
06	用户信息长度(TP-UDL)	实际长度 6 个字节
C8 32 9B FD 0E 01	用户信息(TP-UD)	“Hello!”

2．接收。例如 SMSC 号码是+8613800250500，对方号码是 13811858840，消息内容是“你好！”。手机接收到的 PDU 串可以是：08 91 68 31 08 20 05 05 F0 84 0D 91 68 31 58 81 27 64 F8 00 08 30 30 21 80 63 54 80 06 4F 60 59 7D 00 21。对照规范，具体分析见表 6-2。

表 6-2 接收消息时 APDU 字符含义

分段	含义	说明
08	地址信息的长度	共 8 个八位字节(包括‘91’)
91	SMSC 地址格式(TON/NPI)	用国际格式号码(在前面加‘+’)

68 31 08 20 05 05 F0	SMSC 地址	8613800250500，补‘F’凑成偶数
84	基本参数(TP-MTI/MMS/RP)	接收，无更多消息，有回复地址
0D	回复地址数字个数	共 13 个十进制数(不包括‘91’和‘F’)
91	回复地址格式(TON/NPI)	用国际格式号码(在前面加‘+’)
68 31 18 81 85 48 F0	回复地址(TP-RA)	8613811858840，补‘F’凑成偶数个
00	协议标识(TP-PID)	是普通 GSM 类型，点到点方式
08	用户信息编码方式(TP-DCS)	UCS2 编码
30 30 21 80 63 54 80	时间戳(TP-SCTS)	2003-3-12 08:36:45 +8 时区
06	用户信息长度(TP-UDL)	实际长度 6 个字节
4F 60 59 7D 00 21	用户信息(TP-UD)	“你好!”
分段	含义	说明

注意事项：

- 地址信息的长度中是需要包括‘91’信息的；
- 号码和时间的表示方法，不是按正常顺序排列的，而且要以‘F’将奇数补成偶数；
- 号码的数字是十进制数字的直接转换，不用作任何处理，最后一位的时候加一个‘F’即可；
- 时间是按年、月、日、时、分、秒和时区的顺序，也是用十进制数字直接处理的；
- 目标/回复地址数字个数中不包括‘91’和‘F’；
- 用户信息编码方式在发送与接受过程中，使用的地编码方式不同。

6.6 TERMINAL RESPONSE 使用细节

TERMINAL RESPONSE[6]命令结果中存在一个“结果的附加信息”项，对于部分命令要求命令结果中的附加信息。对于一般结果‘20’、‘21’、‘26’、‘34’、‘5’、‘37’、‘38’、‘39’和‘3A’，ME 必须提供一个明确的原因值作为附加信息。对于其它的一般结果，ME 可选择提供附加信息，若不提供附加信息，则数据对象的长度仅需包含一般结果的长度。

1. 文本串，仅在 GET INKEY，GET INPUT 命令的响应中要求在文本串中提供由用户输入的一个字符或字符串。

表 6-3 文本串参数表[6]

字节	描述	长度
1	文本串标记：0D 或 8D	1
2 到(Y-1)+2	长度 (X)	Y
(Y-1)+3	数据编码方案	1
(Y-1)+4 to (Y-1)+X+2	文本串	X-1

2. 项目标识符，仅在 SELECT ITEM 命令的响应中要求，提供由用户选择的项目标识符。

表 6-4 项目标识符参数表[6]

字节	描述	长度
1	项目标识符标记：10 或 90	1
2	长度 = '01'	1
3	项目选择的标识：01~FF (空项目标识符为 '00')	1

3. 位置信息，仅在 PROVIDE LOCAL INFORMATION 命令的响应中要求，由 ME 提供请求的本地信息。

表 6-5 位置信息参数表[6]

字节	描述	长度
1	位置信息标记：13 / 93	1
2	长度 = '07'	1
3 - 5	MCC（移动国家代码）和 MNC（移动网络代码）	3
6 - 7	LAC（位置区代码）	2
8 - 9	Cell ID Value（当前服务小区的 ID 号）	2

4. 呼叫控制响应，仅在主动式命令 SET UP CALL 和 SEND SS 的响应中要求，提供响应数据作为对 ENVELOPE 的响应。

表 6-6 呼叫控制响应参数表[6]

字节	描述	长度
1	呼叫控制响应标记：27/A7	1
2 到(Y-1)+2	长度(X)	Y
(Y-1)+3 到(Y-1)+X+2	呼叫控制响应	X

5. 定时器标识，仅在 TIMER MANAGEMENT 命令的响应中要求，在定时器标识数据中声明定时器的标识符。

表 6-7 定时器标识参数表[6]

字节	描述	长度
1	定时器标识标记：24/A4	1
2	长度= '01'	1
3	定时器标识符（标识一个定时器）	1

参考文献

[1].智能卡研发技术与工程实践，人民邮电出版社，李翔编著

[2].3GPP TS 11.11 "Specification of the Subscriber Identity Module –Mobile Equipment(SIM-ME) interface(V8.13.0:Rel99)"

[3].3GPP TS 11.14 "Specification of the SIM application toolkit for the Subscriber Identity Module–Mobile Equipment (SIM-ME) interface(V8.17.0):Rel99"

[4].STK 卡梦网短信业务菜单 OTA 下载实现方案(二阶段)

[5].中国移动通信互联网短信网关接口协议（China Mobile Peer to Peer, CMPP）（V2.0）

[6].中国移动 USAT 技术规范(1.0)

[7].IC 卡的技术与应用，电子工业出版社，王卓人，邓普均，刘宗祥编著

[8].智能卡技术，清华大学出版社，王爱英主编

[9].3GPP 03.04 Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS); Point-to-Point (PP) (GSM 03.40 version 6.0.0)

[10].智能卡技术与应用，电子工业出版社，段丽斌编著

[11].移动应用开发——短消息业务和 SIM 卡开发包，人民邮电出版社， Scott B.Guthery & Mary J.Cronin 著，田敏 黄翔 等翻译

[12].3GPP TS 31.111 "USIM Application Toolkit(USAT)(3.13.0:Rel99)"

[13].3GPP TS 22.038 "USIM/SIM Application Toolkit(USAT/SAT); service description"

[14].3GPP TS 51.011 "Specification of the Subscriber Identity Module – Mobile Equipment(SIM-ME) interface(V4.15.0:Rel-4)"

[15].3GPP TS 51.014 "Specification of the SIM application toolkit for the Subscriber Identity Module–Mobile Equipment (SIM-ME) interface(V4.15.0):Rel-4"

[16].GSM 03.38 "Digital cellular telecommunications system(Phase 2+); Alphabets and language-specific information"

[17].3GPP TS 03.48 "Security mechanisms for the SIM application toolkit; stage 2(V8.9.0:Rel99)"

[18].3GPP TS 23.048 "Security mechanisms for the (U)SIM application toolkit;

stage 2(V4.5.0:Rel-4)"

[19].3GPP TS 23.040 V6.7.0 (2006-03)3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Technical realization of the Short Message Service (SMS) (Release 6)

[20].3GPP TS 31.111 V7.2.0 (2005-12) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) (Release 7)

[21].3GPP TS 24.011 V6.1.0 (2005-06) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface (Release 6)

致 谢

首先，我要诚挚地感谢我的指导老师——刘杰、范春晓教授在这几年里对我的悉心指导！感谢他们给我这么好的学习机会，感谢这几年对我的关心和鼓励，感谢对我学习和课题研究的指导！

其次，在研究课题的过程中得到了周鹏老师的详细指导。在论文完成过程中还得到了刘杰老师的指导，有了他们的认真和热心，我的这篇论文才得以顺利完成。他们渊博的学识，严谨的治学态度、开阔的视野和豁达乐观的人生态度使我受益匪浅。

此外，我还要感谢实验室的其它同学，大家团结协作相互配合的精神深深的打动了我。我们实验室是一个团结的集体，在所有项目上大家都是相互配合，互相支持。在此向实验室的每位成员表示谢意！

最后，还要感谢李听颖，她在我学习过程中给了我极大的帮助和关心。