IT先锋系列丛书

移动应用开发
——短消息业务和SIM卡开发包

MOBILE APPLICATION DEVELOPMENT
WITH SMS AND THE SIM TOOLKIT

Scott B. Guthery
Mary J. Cronin 著
田敏 黄翊 等译
白建军 审校

McGraw Hill Education

人民邮电出版社
POSTS & TELECOM PRESS

IT 先锋系列丛书

移动应用开发
——短消息业务和 SIM 卡开发包

Scott B.Guthery
Mary J.Cronin 著

田 敏 黄 翊 等译
白建军 审校

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

移动应用开发：短消息业务和SIM卡开发包 /（美）格斯里（Guthery, S. B.）著；田敏，黄翊译. —北京：人民邮电出版社，2003.9
（IT先锋系列丛书）
ISBN 7-115-10833-1

I. 移… II. ①格… ②田… ③黄… III. 移动通信—通信技术 IV. TN929.5
中国版本图书馆CIP数据核字（2003）第076569号

IT先锋系列丛书
移动应用开发
——短消息业务和SIM卡开发包

◆ 著 Scott B.Guthery Mary J.Cronin
译 田 敏 黄 翊 等
审 校 白建军
责任编辑 梁 凝

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
读者热线 010-67129258
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：800×1000 1/16
印张：13.25
字数：279千字 2003年9月第1版
印数：1-4 000册 2003年9月北京第1次印刷
著作权合同登记 图字：01-2002-2459号
ISBN 7-115-10833-1/TN·1960

定价：23.00元

本书如有印装质量问题，请与本社联系 电话：（010）67129223

版 权 声 明

内 容 提 要

本书主要介绍 SIM 卡编程环境所需要的完整应用技术。内容包括：如何在应用环境中设计、建立和集成 SMS 短消息应用；如何创建能够充分利用 SIM 卡功能的代码；如何在 3G 电话中使用微浏览器和微 Web 服务器；如何在现代网络中建立具有前导性的移动商务应用；如何从服务器或膝上电脑上发送和接收 SMS 短消息；如何使用接口和其他必需的组件；如何为公司网络及 VPN 创建安全的无线应用。

本书的主要读者对象为移动通信应用软件开发人员，SIM 卡应用程序设计员及大专院校相关专业师生。

译 者 序

谁能想到，在短短两年时间内短消息的应用竟然发展得如此神速！

现在，在全球范围内，每个月有超过 200 亿条 SMS 消息流量，而且这个数字还一直在增长。使用手机发送和接收短消息已经成为一种全球性的文化现象，更是电信业的一个新的利润增长点。

从技术上讲，短消息的实现很复杂么？根本不！可以说非常简单，无非是在手机的 SIM 卡里加载了一段很短的“程序”。可见受欢迎的技术并不一定必须很复杂。开发短消息这样的应用就是简单但又非常受欢迎的技术，它为人们的生活和工作提供了方便和效率，甚至能够为商业团体节省成本，带来利润。

现在，提起 SIM 卡，恐怕几乎所有人都听说过。但是，关于如何在 SIM 卡上开发移动应用，特别是像短消息业务的应用，了解的人可能不多。本书就是详细介绍如何使用 SIM 卡的开发包开发移动应用的一本好书。

从 SMS 和 SIM 卡的基本原理到使用各种开发包进行高级应用开发，从简单而丰富的理论介绍到大量有趣而充实的应用实例，作者始终试图用通俗的语言从原理和使用的角度，完整介绍如何使用 SMS 和 SIM 卡开发包进行移动应用开发。无疑，这对于从事移动通信业务和电信业务的技术人员、市场人员和管理人员，以及进行程序开发的程序员，甚至相关专业的在校学生来说都有非常好的参考价值。

本书主要由田敏、钟读杭和黄翊翻译，白建军审校全书并最后统稿。由于时间紧迫，加之译者水平有限，书中难免有很多翻译不确切的地方，恳请广大读者批评指正。

致　谢

国际上 SMS 和 SIM 卡标准以及它们的互操作应用平台的发展需要来自多个国家的努力及各种各样的观点的支持，因此，本书主要介绍参与标准化进程的众多人员的技能和经验也就不足为奇。我们非常感激那些阅读过本书章节的早期版本、迅速回答复杂问题、无私地共享他们早期的一些决策的收集材料和文档的人们，这些文档为形成今天的 SMS 和 SIM 卡标准以及为指明下一代移动应用的发展方向做出了很多贡献。我们在这里列出一些，但并非全部。感谢 3GPP 终端组和 ETSI 智能卡平台（Smart Card Platform，SCP）标准体系的全体同事，他们为标准化所做出的工作使这本书的出版成为可能，也感谢各种新闻组和 Listserv 列表里的用户，包括 alt.technoloy.smartcard 和欧洲无线。

书中所阐述的运营商和公司如何使用 SIM 卡和 SMS 应用的示例，主要源于很多管理者和参与者花费大量时间对各种问题做出的回答、提供的数据、给予的详细解释以及对这些示例进行仔细回顾的早期草稿。特别感谢 Zruich 的 Atraxis 工作组的 Anselmo A.Mazzoleni 和 Swisscom 公司的 Pawl Aebi 为完成 Atraxis 示例的书写所给予的帮助；感谢 Den mark 的 Sonofon 的 Thomas Bruun Pedersen 给予的广泛接见及对 Sonofon 示例的深入探究；感谢智能信任的 Jarkko Rossi、Lars-Erik、Sellin 和 Werner Freystätter 关于移动商务安全在技术和商业上的复杂性的观点和解释，也感谢他们对草稿的多次更改和阅读；感谢 Sonera 的 Ari-pekka kitinoja 和 Setec 的 Jouni Heinonen 所给予的关键背景细节和解释；我们还要感谢智能信任的 Anders sellin 为策划示例所给予的重要帮助以及对他众多 SIM 卡应用领域里的多个示例前景的介绍。

这本书的最终稿刚出来，就有 3 位专家花费时间阅读了全部章节并给出了很有价值的意见和建议，他们分别是 Nigel Barnes、Jean-Francois Rubon 和 Kristian Woodsend，非常感激他们。

在整个研究和写作的过程中，我们召集了一些同事来提供背景知识并帮助弄清楚标准和应用实施的一些特殊点，在众多响应这次邀请的人中，特别感谢 David Birch、Peter De Vijt、Bertrand du Castel、David Everett、Tony Guilfoyle、Colin Hamling、Mark Kamers、Roger kehr、Tim Jurgensen、Hans-Joachim Kuobloch、Michael Meyer、Pierre Paradinas、David Pecham、Patrice Peyret、Jochaim Posegga、Fred Renner、Ekouard Richard、Wolfgang Salge、Lars-Erid Sellin、Gerry Smith、Jean-Jaclues Vandewalle、John Wood 以及最后的但也同样重要的 Klans Vedder。

书中引用的表格和插图经过了 ETST、Atraxis、Setec 和智能信任等组织的允许，Sonoton 进一步增强了本书的可读性，这里对他们的帮助表示感谢。

向那些在整个过程中支持我们的研究、写作和更正的人们，以及 Mobile-Mind 公司的全

体员工，特别对 Dan Eichenwald、Peter Laing、Scott Marks、Scott Olihovid 和 Perry Spero，表示真挚的敬意。我们很真诚地告诉所有人，没有你们日复一日的帮助，我们无法完稿，诚挚地感谢非常优秀和具有耐心的 Marjorie Spencer 编辑，以及对这本书一直拥有信心的我们的代理 Rob Robertson。

最后，我们充分认识到，即使有了最大的支持和各位专家的建议，在 SMS 和 SIM 卡应用这个快速变化的领域，肯定会在已出版的书中有一些不恰当的地方，希望读者提出宝贵的意见和建议，以使我们能够在下一版进行改正。

Scott B.Guthery
sguthery@mobile-mind.com

Mary J.Cronin
mcronin@mobile-mind.com

前　言

GSM 的成功史即是 SIM 卡的成功史。每个用户都需要一个 SIM 卡，离开它就不能得到任何服务。这不像在其他的系统中，智能卡（Smart Card）内的“微计算机”只是提供一种用户可用可不用的附加服务。到目前为止，在全球有着 6 亿用户的 GSM 系统是使用智能卡的最大应用系统，GSM 也使智能卡工业从幼儿状态发展到成熟状态。GSM 同智能卡大规模生产的到来有非常紧密的联系，它对 SIM 卡需求的不断增长不仅大大地推动着微计算机本身在技术上的发展，也在整体上推动着智能卡的操作系统、应用程序以及编程接口的发展。

然而，电信业只是在过去的几年才开始普遍认识到 SIM 卡为 GSM 的成功所做的重要贡献。GSM 刚诞生时，SIM 卡的目的只是在移动通信中提供一个史无前例的安全保证，SIM 卡也把手机从签名承诺和安全方面“解放”出来，这第一次创建了一个全球性的终端市场。

今天，SIM 卡所能提供的远远不仅这两项功能。SIM 卡应用程序开发包（Toolkit）和解释器（Interpreter）的标准化同 SIM 卡硬件平台的发展一起创建了一个不断进步的并且使网络运营商（Network Operator）和服务提供商（Service Provider）能够进行判断、控制的安全增值服务平台。内容（指内容服务）是一个不可思议的词，在将来会更是如此。

这本书是第一本全面介绍 SMS 相关技术问题的书籍，包括对基本的 SIM 卡开发包和解释器的详细介绍。它把那些技术细节同现实应用中的具体例子结合在一起，成为一本拥有技术背景的市场人员的好参考资料，这也是开发包和解释器所需要的，即在网络运营商和服务提供商的高层引起更多的市场关注。很多人知道 WAP，但是谁又听说过开发包和解释器，更别说知道怎样以一种创新的态度使用它们赚钱了。基于手机的 WAP 服务同基于 SIM 卡的开发包和解释器提供的服务并不互相排斥，而是能够以一种最佳的方式得到互补。

事实是这本书毕竟已经问世，阐明了多个专利方法拥有一个标准的好处。开发包和解释器已被 ETSI 和 3GPP 定为 SIM 卡和 USIM 卡的标准。它们是基于方法的标准，GSM 的发展历史清晰地表明，只有基于方法的标准才能在有多个提供者的环境必须的系统成员之间提供高级别的互操作性，以及长期的成功所必需的多个不同专利方法的独立性，我希望本书能够传播与那些强大工具有关的知识，从而扩大 SIM 卡作为提供增值服务内容平台的渗透力。

我想本书肯定也能够引起很多关于开发包和解释器的技术及市场方面的有趣和有争议的讨论。有关 SIM 卡的标准化进程一开始我就参与了，相信它的未来决不仅仅只是一

种安全设备。我也期盼这些讨论，它们将会作为移动通信智能卡平台的 UICC 领域的新推动力。

Dr. Klaus Vedder
Giesecke & Devrient
Chairman ETSI EP SCP（Smart Card Platform）
Chairman 3GPP TSG-T3（USIM）
E-mail：klaus.vedder@gdm.de

目　录

第 1 章　SMS 和 SIM 卡入门 ····· 1
1.1　基础知识和定义 ····· 2
1.2　网络环境中的 SMS 和 SIM 卡 ····· 4
1.3　协议栈 ····· 5
1.4　标准的作用 ····· 7
1.5　后续章节预览 ····· 10
1.6　小结 ····· 11

第 2 章　基本的 SMS 通信 ····· 12
2.1　连接到手机 ····· 12
2.2　与手机进行通信 ····· 13
2.3　与网络通信 ····· 15
2.4　你好，移动世界 ····· 16
2.5　小结 ····· 25

第 3 章　SMS-SUBMIT 和 SMS-DELIVER 详解 ····· 26
3.1　编码规则和手机的号码 ····· 27
3.2　SMS-SUBMIT ····· 28
3.3　协议标识符 ····· 31
3.4　数据编码模式 ····· 32
3.5　链接短消息 ····· 33
3.6　“有邮件到达” ····· 34
3.7　应用端口寻址 ····· 35
3.8　SIM 卡开发包安全 ····· 35
3.9　增强的消息服务 ····· 36
3.10　声音、图像和动画 ····· 37
3.11　Internet E-mail ····· 40
3.12　SMS-DELIVER ····· 40
3.13　小结 ····· 42

第 4 章　SMS 集成 ····· 43

第 5 章　SMS Brokers ····· 54

第 6 章　SMS 在机场后勤中的应用 ····· 65
6.1　SMS 个案研究：Atraxis ····· 65
6.2　工程背景 ····· 66
6.3　主要的技术难点 ····· 66
6.4　设计和实现过程 ····· 67
6.5　地面行为 ····· 68
6.6　项目性能评估 ····· 70
6.7　商业成果评估 ····· 70
6.8　小结 ····· 71

第 7 章　SIM 卡 ····· 72
7.1　智能卡 101 ····· 74
7.2　SIM 卡的发展过程 ····· 77
7.3　你是谁 ····· 79
7.4　SIM 卡标准的发展 ····· 80
7.5　SIM 卡应用程序开发包的出现 ····· 83
7.6　SAT API ····· 85
7.7　USAT 解释器 ····· 86
7.8　小结 ····· 87

第 8 章　SIM 卡开发包 API：主动命令和事件下载 ····· 88
8.1　主动命令 ····· 90
8.2　SIM 卡开发包命令细节 ····· 94
8.2.1　应用命令 ····· 94
8.2.2　智能卡主动命令 ····· 96
8.2.3　通用的通信命令 ····· 97
8.2.4　系统命令 ····· 97
8.3　事件下载 ····· 98
8.4　小结 ····· 102

第 9 章　SMS 消息的端到端安全 ····· 103

9.1 安全参数指示器 …… 104
9.2 加密密钥标识和密钥标识 …… 106
9.3 开发包应用参考 …… 107
9.4 计数器 …… 107
9.5 填充计数器 …… 108
9.6 冗余校验（RC）、加密校验和（CC）或数字签名（RDS） …… 108
9.7 安全 SMS 消息例子 …… 108
9.7.1 接收证明 …… 110
9.7.2 发送消息和响应的对应 …… 111
9.8 小结 …… 112

第 10 章 智能信任微浏览器和 3GPP USAT 解释器 …… 113
10.1 更多的一些有关 SIM 卡开发包的历史 …… 113
10.2 智能卡字节码解释器的简短历史 …… 114
10.3 Sonera 的智能信任 WIB …… 117
10.4 3GPP USAT 解释器 …… 122
10.5 使用 USAT 解释器的远程过程调用 …… 126
10.6 小结 …… 128

第 11 章 发展中的 USAT 解释器 …… 129
11.1 商业驱动力 …… 129
11.2 技术概览 …… 130
11.2.1 从 SMS 开始 …… 130
11.2.2 从 WAP 到集成门户 …… 132
11.2.3 与微浏览器集成 …… 133
11.2.4 向移动银行和移动商务进军 …… 133
11.3 从用户的角度 …… 134
11.4 实现中的挑战和策略 …… 135
11.5 Bottom-Line Benefits …… 136
11.6 学到的经验 …… 137

第 12 章 USAT 虚拟机与 SIM 卡开发包程序 …… 138
12.1 各种各样的虚拟机 …… 139
12.2 虚拟机体系结构 …… 141
12.3 来自微软的 USAT 虚拟机 …… 142

12.4 实时旅行例子 …… 146
12.5 Java 卡 SIM 卡 …… 155
12.6 USAT 虚拟机程序的安装 …… 156
12.7 小结 …… 157

第 13 章 安全移动商务的智能签名 …… 158
13.1 从移动客户开始 …… 159
13.2 智能签名特性 …… 160
13.2.1 表格（Form）和模板（Template） …… 160
13.2.2 密钥和签名身份识别码（PIN） …… 160
13.2.3 菜单设计 …… 160
13.2.4 改变服务提供商 …… 161
13.3 使用智能签名的移动认证和信任 …… 163
13.3.1 产生事务所需的信任关系 …… 165
13.3.2 使能事务所需的信任关系 …… 166
13.3.3 证书权威机构 …… 167
13.4 智能签名的商业使能者 …… 168
13.4.1 操作中的智能签名 …… 169
13.4.2 安装阶段的智能签名 …… 169
13.5 管理大规模的智能签名试验 …… 171
13.5.1 试验背景 …… 171
13.5.2 关键的参与者 …… 171
13.5.3 收入模型 …… 172
13.5.4 智能信任部件的价格 …… 172
13.5.5 移动信任层次中的安全性 …… 172
13.5.6 试验性投放的教训与经验 …… 173
13.5.7 客户经历的重要性 …… 173
13.5.8 商业模式的含义 …… 174
13.5.9 智能信任商业策略的含义 …… 174
13.6 智能签名的未来 …… 174

第 14 章 ETSI 智能卡平台 …… 176
14.1 使用访问控制列表管理数据共享 …… 177
14.2 将访问控制列表和文件关联起来 …… 179
14.3 对访问控制规则编码 …… 180

14.4 访问模式 TLV …… 181
14.5 密钥引用 …… 182
14.6 密钥引用的布尔表达式 …… 183
14.7 密钥引用语义 …… 184
14.8 密钥引用的认证 …… 186
14.9 应用激活和并发执行 …… 187
14.9.1 应用目录和应用激活 …… 187
14.9.2 应用选择 …… 189
14.9.3 并发应用执行 …… 189
14.10 小结 …… 190

附录 SMS 和 SIM 卡标准 …… 191

第1章 SMS和SIM卡入门

在全球，无线技术的发展超过了任何其他技术，包括 Internet。2003 年有超过十亿人使用无线电话或者 PDA（Personal Digital Assistant，个人数字助理）进行声音或数据通信。有 3 个因素驱动着这种显著的增长，同时也是编写本书的初衷：

（1）廉价的 SMS（Short Message Service，短消息业务）在全球范围内的可用和流行。

（2）GSM 电话中的 SIM 卡技术逐渐发展成为一个标准的、安全的 GSM 和下一代网络的应用平台。

（3）人们通过手机进行通话以外的应用需求。

首先，让我们迅速浏览一下，SMS 和 SIM 卡如何为无线应用的增长做出贡献，随后讨论读者可以从本书学到哪些内容。

每月发送的短信数量从 1999 年 7 月的大概 10 亿条增长到了 2001 年 7 月的 200 亿条，而在 2001 年，总的短信交换数量达到 2000 亿条。这些相互发送的短信囊括了从个人用户之间发送的简单文本问候或者问题，到无线服务商提供的新闻和信息服务，甚至是第三方提供的更多高级应用，比如，从一个公司的销售数据库或者移动银行获取数据。这些文本和其他短信服务发展的一个原因就是现在无线运营商（Wireless Carrier）把 SMS 视为收入的重要来源。这导致的另一个结果就是几亿用户已经适应并期望得到更多基于 SMS 的服务和创建个性化的和可信任的应用，开发者需要一个标准的和安全的应用平台，于是 SIM 卡应运而生。

SIM 卡是一种被设计成安全、稳定地存储用户密码的智能卡，它所存储的密码用来标识 GSM 用户到网络的连接并跟踪这些用户的行为，只要他们在服务区，只要移动设备不关机，SIM 卡就一直维持着到网络的连接，这种可以定位并能认证的连接就是用户能够在全世界各网络之间漫游的原因，并且从提供商的角度看，非常重要的是 SIM 卡保持跟踪并记录用户的网络使用和漫游行为，从而能够准确地收费。

在不中断通信的情况下，保证 SIM 卡能够做到把用户的连接从一个网络移交给另一个网络的唯一方法就是把它的所有功能都建立在一个非常详细的国际标准体系之上。这个标准涵盖了从设备的物理尺寸和芯片特征到它如何处理和保存接收的信息等方面，每一个 GSM 设备制造商和服务提供商都遵循这些标准。任何人开发和 SIM 卡相关的应用也必须熟悉相关标准并保特同步发展。本书详细描述一些最重要的标准，并为读者介绍完整的标准文档和更新的在线资源。

本章的后面将会提到，SIM 卡也是向更快和更强的“下一代”无线网络发展的基础。因为 2001 数字网络被称为第 2 代网络（模拟无线网络为第一代），它的升级被称为 2.5G（从现在的速度和性能来讲是一个非常大的跨越）和 3G。虽然世界各地实施下一代网络的技术和时

间表各不相同，但各地的服务提供商们都认识到，在网络升级的过程中和升级以后，保持 SIM 卡和 SMS 应用正常工作的重要性，因此，SIM 卡还要管理数据在不同级别的网络和不同物理位置之间的漫游。另外，基于现有 SIM 卡标准的应用也将会处于一个很有优势的位置，以能够充分利用 3G 网络出现所带来的更高的传输速率和多媒体传递能力。

网络提供商、移动设备制造商和其他的服务提供商都认为应用是无线数据交换持续增长最重要的驱动力。提供商们正在寻找新的招人喜爱的应用来从他们拥有的网络中获得更多的收入，并增加用户的使用量和“忠诚”度。他们看到个人用户也在寻找能够让自己从手机或无线 PDA 得到更多服务的应用。也看到商业机构需要能够让移动雇员更加高效地工作，并使他们能更方便地接触移动客户的应用。关于究竟谁应该开发这样的应用有不同的看法。一些运营商倾向于自己完成开发工作，而其他的则选择同第三方开发者合作或者寻求 SIM 卡移动设备商提供应用，不管怎样，应用的需求正在持续增长。

被很多人看作是实现移动应用最快途径的无线应用协议（Wireless Application Protocol，WAP），对网络运营商来讲只是类似于“唤醒呼叫”（wake-up call）的一种方法。当无线通信全进行语言传输时，网络运营商能够控制手机的任何方面。WAP 的出现使很多众所周知的基于 Web 的服务，像 yahoo.com 和几百个刚启动的 WAP 站点，提供下载程序到移动手持设备上的功能并控制显示屏和按键。无线运营商到处寻找，最终发现他们真正能够控制的只有 SIM 卡，一个嵌于手机内部的只能提供安全而不支持应用的芯片。后面将会讨论这种计算机如何提供一个应用程序编程接口，称为 SIM 卡应用程序开发包（SIM Application Toolkit，SAT）以及其他的开发工具，像第 10 章中的 SIM 卡微浏览器（Micro-Browser），但是，读者应该明白现今的 SIM 卡只是一种没能得到充分利用来支持丰富的移动应用的开发平台。

同时，应用程序开发者，特别是那些善长于创建 SMS 和基于 SIM 卡的应用程序的开发人员非常短缺。很难找到开始使用 SMS 和 SAT 的足够信息，更难找到详细的特定应用开发示例。本书提供了关于相关命令、标准及编程技术的渐进的介绍性知识，这些知识将带领读者从基本的 SMS 应用开始一直到学会使用高级的 SAT 功能。如果想学到更多关于 SMS 和 SIM 卡开发的知识，就从这里开始吧！

1.1 基础知识和定义

SMS 是 Short Message Service 的缩写。SMS 是向手机发送短信和用手机接收短信的一个途径。“短”意味着信息的最大长度不能超过 160 字节。根据 GSM 协会的规定，每一个短信用拉丁字母表示时最长不超过 160 个字符，而用非拉丁字母，比如阿拉伯字母和汉字表示时最长不超过 70 个字符。

短信可以由文本字符组成，这样，它就可以被人们阅读和书写。在欧洲和亚太地区，SMS 文本信息已经成为人们常用的一种无线通信方式，在北美也正逐渐受到人们的欢迎。短信也可以由任意 8 位的字节序列组成，这种情况下，它可能是在一端由计算机生成并在另一端由