第3章 移 动 支 付

教学目标与要求

- 掌握移动支付的概念;
- 掌握移动支付的类型;
- 掌握移动支付的接入方式;
- 了解移动支付的功能、流程;
- 了解移动支付的安全保障技术。

知识架构

导入案例

安全障碍移动支付发展[①]

用户普遍存在对移动支付安全性的担忧。据赛迪顾问调查显示，交易安全是中国移动支付用户最关注问题，如图 3.1 所示。

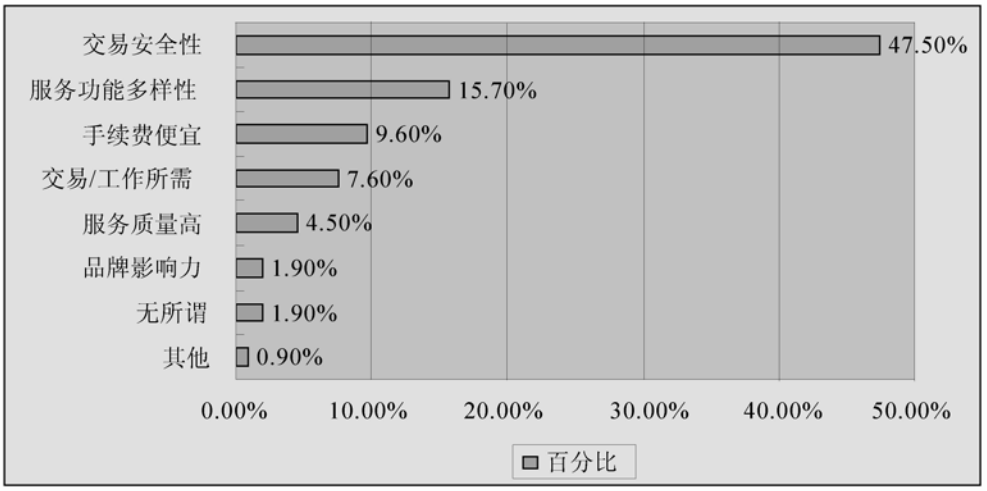

图 3.1　移动支付调查

更不利的是，见表 3-1，在中国，用户对移动支付安全性的信任度，与年龄成反比，在职业分布中也只有学生给予了较高评价。这就意味着开发难度较低的细分市场，却是价值较低的群体。或许这也解释了众多的移动支付业务似乎只是移动公司和金融服务公司的一项复杂的额外业务，没有人把它作为重点业务来做，离真正大范围的推广还有一定差距。

表 3-1　不同年龄手机用户对移动支付交易安全性评价

年龄段	18 岁以下	18～25 岁	26～35 岁	36～50 岁	50 岁以上
安全性	50%	35%	20%	18%	12%

什么是移动支付？移动支付和手机支付有何不同？我国目前移动支付的运营情况和支付流程如何？采用了哪些安全措施？本章将试图回答这些问题。

3.1　移动支付概述

截至 2009 年 8 月，中国作为世界第一大手机市场，手机用户已超过 6.7 亿，手机已经渗透到社会生活的方方面面，另外，随着中国 3G 牌照于 2009 年年初的发放，移动支付业

① 资料来源：http://www.ccidconsulting.com/import/channel/detail.asp?Content_id=7306。

务将成为移动运营商新的利润增长点，也将成为用户对移动功能需求的热点，存在着巨大的潜在市场，将更受关注。

3.1.1 移动支付相关概念

1. 移动支付

对移动支付(Mobile Payment，M-Payment)的概念业界存在不同的观点，主要差别存在于以下两个方面。

1) 移动支付的工具

部分学者认为移动支付工具包括手机、PDA、移动 PC 等移动设备，另一部分学者认为移动支付工具就是手机。

2) 移动支付的支持网络

部分学者认为移动支付通过移动通信网络实现支付，另一部分学者认为移动支付通过无线通信网络进行支付。

综合上述学者们的观点，移动支付可以从广义和狭义两个方面进行界定，狭义的移动支付主要指利用手机通过移动通信网络进行支付(即手机银行支付)；广义的移动支付除包括手机支付外，还包括采用其他移动通信设备所进行的支付方式。本书采用广义的移动支付的概念，但是，目前我国各银行提供的移动支付还局限于狭义移动支付方式，即手机银行。

综上所述，移动支付就是利用移动设备通过无线通信网络转移货币价值以清偿债权债务关系的一种支付方式，其中“移动设备”包括手机、PDA、移动 PC 等。对于手机银行支付来说，移动支付方式仍沿用原有支付账户进行支付，而其他移动通信设备仅是新的支付载体。与网上银行支付相比，移动支付主要面向个人用户。

手机是目前移动支付中使用最普遍的移动设备，利用手机进行支付的支付方式通常称为手机支付。手机支付实质上就是把具有支付功能的智能卡安置在手机中，手机只是一个支付智能卡的载体。手机支付最早出现在美国，但是美国和欧洲的移动运营商却都没有给予太多重视与关注；相反，在日本和韩国，手机支付的发展变得最为迅速；无论是在业务量上，还是在业务模式上，我国的手机支付还处于发展的初期。

2. 手机银行

手机银行就是通过移动通信网络与移动通信技术实现手机与银行的连接，通过手机界面操作或者发送短信完成各种金融服务的电子银行创新业务产品，是手机支付的一种实现方式，也是目前移动支付中使用最普遍的一种支付方式。手机银行作为一种结合货币电子化与移动通信的服务，不仅可以使人们随时随地处理多种金融业务，而且极大地丰富了银行服务的内涵，使银行能以便利、高效而又较为安全的方式为客户提供传统和创新服务。

手机银行其实并非是新生事物，早在 2000 年 5 月工商银行、中国银行就推出基于 SIM 卡(Subscriber Identity Module，客户识别模块，也称为智能卡、用户身份识别卡)技术的手机银行，后来建设银行推出基于 BREW(Binary Runtime Environment for Wireless，无线二进制运行时环境)技术的手机银行，目前各大银行基本都推出了基于 WAP2.0(Wireless

Application Protocol，无线应用协议)先进技术的手机银行，客户利用手机通过上网进入自己的账户进行账户查询、交易、缴费等操作。随着 3G 时代的开启，手机银行上网速度将会得到很大提升，第四代手机银行离人们已经不远了。

3. 手机钱包

2003 年 8 月，中国移动与中国银联合资成立了北京联动优势科技有限公司，联合各大银行共同推出了一项全新的移动电子支付通道服务——“手机钱包”[①]，将手机与钱包的功能合二为一，通过把客户的手机号码与银行卡等支付账户进行绑定，使用手机短信、语音、WAP 、K-Java、USSD 等操作方式，随时随地为拥有中国移动手机的客户提供移动支付通道服务。使用该通道服务可完成手机缴费、手机理财、移动电子商务付费等个性化服务，具体包括：查缴手机话费、动感地带充值、个人账务查询、手机订报、购买数字点卡、电子邮箱付费、手机捐款、远程教育、手机投保、公共事业缴费等多项业务。

根据联动优势公司数据，公司手机钱包的用户数在 2006 年 6 月已经拥有了 1 000 万注册量，而活跃用户接近一半，在国内的手机支付市场已经占据了 50%的市场份额。到了 2008 年 12 月，手机钱包注册用户已经超过了 5 000 万。

3.1.2 移动支付的类型

按照不同的标准，移动支付可以分为不同的类型。

1. 小额支付和大额支付

根据移动支付交易金额的大小分为小额支付和大额支付。

小额支付指单笔交易金额在 100 元以下的移动支付业务，通常是指购买移动内容的业务，例如：视频下载、游戏点卡等的购买。而大额支付是指交易金额较大的支付行为，即单笔交易大于 100 元的支付业务，如在线购物等。

2. 近距离支付和远距离支付

按照传输方式的不同，移动支付可以分为近距离支付和远距离支付，或者称为现场支付与远程支付。

近距离支付不通过移动网络，使用近距离无线通信技术(例如：红外线、射频识别、蓝牙等技术)进行支付，包括接触式支付和非接触式支付。消费者在购买商品或服务时，即时通过移动设备(主要是手机)向商家进行支付，支付的处理在现场进行，支付完毕，消费者即可得到商品或服务。这种支付方式需要手机终端内置 NFC(近距离通信)芯片，并且植入用户信息、银行卡号等信息，通常应用于商场、超市、便利店的支付。

远距离支付是指通过无线移动网络进行接入的服务。消费者在购买商品时，可以用短信、WAP 或客户端的方式将支付信息传递到支付平台的后台服务器，支付平台在银行账户中扣除相应的费用，并且向商家发出支付确认信息，商家再向使用者确认，完成交易支付。通常用于网上消费。

① 资料来源：移动支付门户网站(http://www.umpay.com)。

3. 移动运营商代收费和银行卡绑定收费

根据手机是否与银行卡绑定，移动支付分为移动运营商代收费和银行卡绑定收费。移动运营商代收费是指移动运营商为商户提供服务，用户通过手机账户进行商品的购买，全额由移动运营商从其手机账户中扣除，再同金融机构进行结算。由于金融机构的管制，目前此种方式在我国仅限于小额支付。

银行卡绑定收费是指银行为用户提供信用，将用户银行卡账号同手机号连接起来，费用从用户的银行账户中扣除。

4. 手机—手机、手机—移动 POS 机、手机—专用设备

按与商家的交互方式不同，移动支付分为：手机—手机、手机—移动 POS 机、手机—专用设备 3 种类型。

手机—手机类移动支付指收款方是与银行联网的商城、超市，付款方通过手机银行支付消费款项，双方均通过手机银行得到结算结果的通知。此方式主要适用于有固定营业人员的消费场所，如出租车费用的支付。

手机—POS 机类移动支付是指收款方是与银行联网的商城、超市等，付款方通过手机银行支付消费款项，收款方通过移动 POS 机接受收款信息。此方式适用于大型商场、超市等。

手机—专用设备类移动支付是指收款方装备了红外线、蓝牙等专用设备。此方式适用于小型商店、摊位等不固定的营业场所。

3.1.3 移动支付价值链构成与运营模式

移动支付属于典型的技术驱动型业务，这类业务成功的基础是建立一个基本成型的价值链和合理的商业运营模式。

1. 移动支付的价值链构成

移动支付的价值链主要由金融机构、电信运营商、商家、消费者、移动设备提供商、移动支付服务提供商等多个环节构成，如图 3.2 所示。只有建立并完善移动支付价值链，才能使价值链中各成员获得最大的利益，实现多赢，从而推动我国移动支付市场的健康发展。

在价值链构成中，电信运营商的主要角色是搭建移动支付平台，为移动支付提供通信渠道。电信运营商掌握着消费者资源，是连接金融机构、服务提供商以及商家和消费者的通道。

金融机构同电信运营商一样，也掌握了大量的用户资源，拥有较强的讨价能力和资金支持。

移动设备提供商为电信运营机构和消费者提供移动通信设备，并提供移动支付解决方案。

移动支付服务提供商是银行和电信运营商之间沟通的桥梁，同时为消费者和商户提供交易平台。实际上电信运营商有时也是服务提供商。

商家在移动支付的价值链中基本上属于从属地位，它提供产品和服务。

消费者是移动支付服务的最终使用者，消费者的使用习惯和接受程度是决定移动支付发展的重要因素。

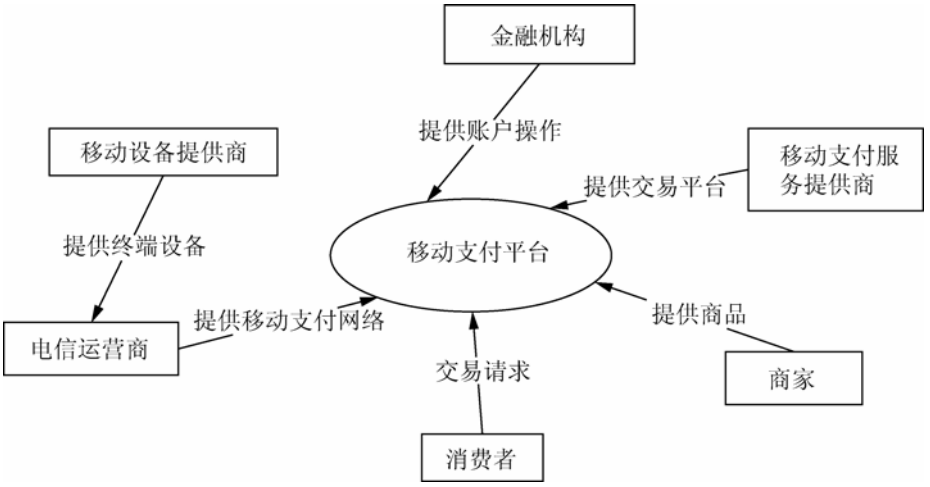

图 3.2 移动支付价值链构成[①]

2. 移动支付商业运营模式

移动支付商业运营的主要模式有以下几种：以金融机构为主导的运营模式、以移动运营商为主导的运营模式、以第三方支付服务提供商为主导的运营模式、银行与移动运营商合作的运营模式。

1) 以金融机构为主导的运营模式

提供支付服务的金融机构主要是银行。在该种运营模式下，银行独立提供移动支付服务，消费者和银行之间利用手机借助移动运营商的通信网络传递支付信息。移动运营商不参与运营管理，只负责提供信息通道。用户将手机与银行账户进行绑定，直接通过语音、短信等形式将货款从消费者银行账户划转到商家银行账户，完成支付，如图 3.3 所示。

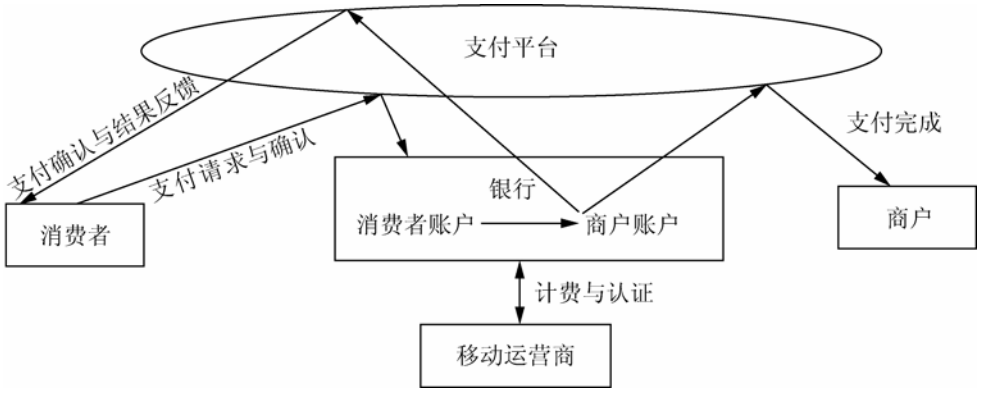

图 3.3 以金融机构为主导的移动支付运营模式[②]

在这种模式中，银行的收益主要来自以下方面。

(1) 手机银行账户上的预存金额，可以增加存款额度。

① 资料来源：韩刚．移动支付产业链研究．优秀硕士论文，2007。

② 作者自制。

(2) 对移动运营商、商户的移动支付业务利润分成。

(3) 降低银行支付渠道的经营成本(如网点、ATM)。

(4) 通过移动支付业务激活银行卡的使用，巩固和扩展客户群。

在该种运营模式下，各银行只能为本行用户提供手机银行服务，移动支付业务在银行之间不能互联互通；各银行都要购置自己的设备，通过与移动运营商搭建专线等通信线路，自建计费与认证系统，因而会造成较大的资源浪费；对终端设备的安全性要求很高，用户需要更换手机或 STK(SIM Tool Kit)卡。

2) 以移动运营商为主导的运营模式

这种运营模式以移动运营商代收费业务为主，银行完全不参与其中。消费者对其话费账户预先充值，当采用手机支付形式购买商品或服务时，将话费账户作为支付账户，交易费用直接从话费账户中扣除。这样货款支付先由电信话费进行扣除，最后由商家和移动运营公司进行统一结算。例如中国移动公司推出的“移动影音书刊俱乐部”购物的支付方式，日本移动运营商 NTT DoCoMo 推广的 i-mode Felica 手机电子钱包服务等。以移动运营商为主导的移动支付运营模式如图 3.4 所示。

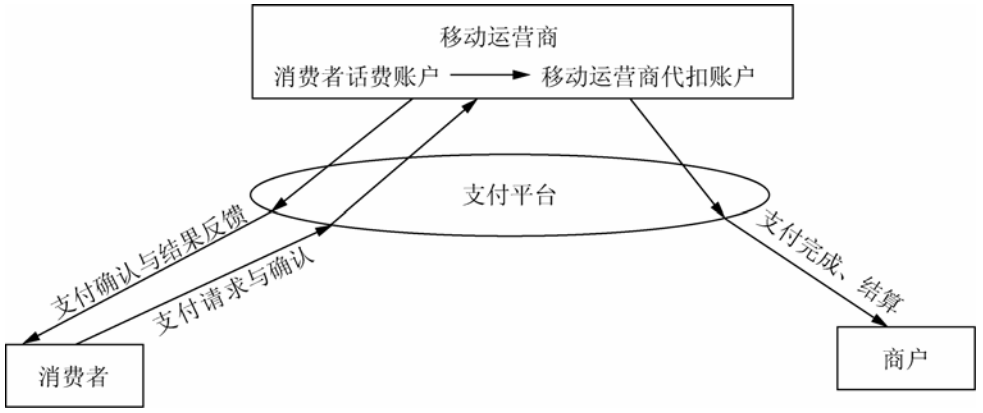

图 3.4 以移动运营商为主导的移动支付运营模式

在这种运营模式下，移动运营商主要从以下几方面获得利益。

(1) 服务提供商(即商户)的佣金。

(2) 带来基于语音、SMS(Short Messaging Service)、WAP(Wireless Application Protocol)的移动支付业务，增加业务收入。

(3) 移动支付业务可以刺激用户产生更多的数据业务需求，同时稳定现有客户，并吸纳新用户。

在这种运营模式下，移动运营商直接与用户交流，不需要银行参与，技术实现简单；但移动运营商需要承担部分金融机构的责任，如果发生大额交易将与国家金融政策发生抵触；而且无法对非话费类业务出具发票，税务处理复杂。因此一般只能用于小额支付。

3) 以第三方支付服务提供商为主导的运营模式

这里的第三方支付服务提供商指独立于银行和移动运营商，利用移动通信网络和银行的支付结算资源进行支付的身份认证和支付确认的机构。第三方支付服务提供商可以是银联，也可以是别的手机支付平台，它们需要构建移动支付平台，并与银行相连完成支付，同时充当信用中介，并且为交易承担部分担保责任。货款通过第三方提供的移动支付账号

进行划转。如通过上海捷银支付、联动优势科技的移动门户支付、手付通等平台进行的支付。以第三方支付服务提供商为主导的移动支付运营模式如图 3.5 所示。

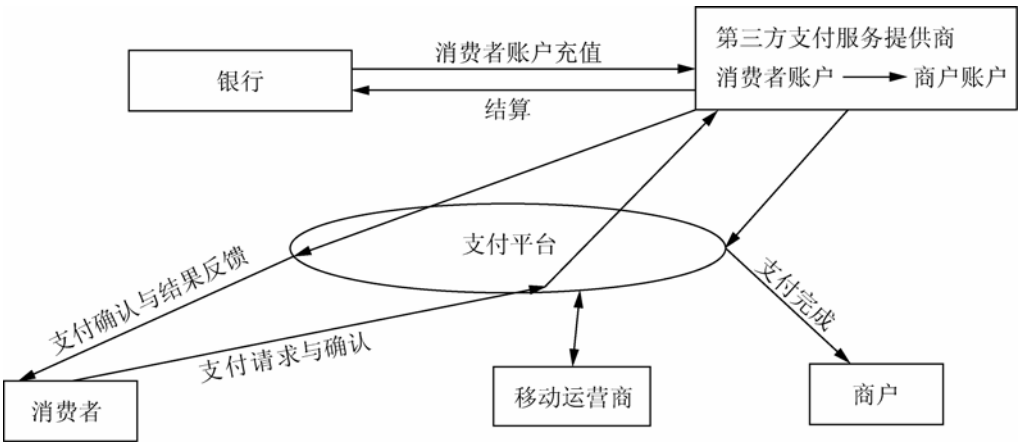

图 3.5 以第三方支付服务提供商为主导的移动支付运营模式

在该种模式中，第三方支付服务提供商的利润主要来源于向移动运营商、银行和商户收取的信息交换佣金。

该种运营模式具有以下特点。

(1) 银行、移动运营商、第三方支付服务提供商、商户之间分工明确、关系简单。

(2) 第三方支付服务提供商发挥着“插转器”的作用，将银行、移动运营商等各利益群体之间错综复杂的关系简单化，从而大大提高了商务运作的效率。

(3) 实现了跨行支付。

(4) 第三方支付服务提供商可以平衡移动运营商和银行之间的关系。

(5) 对第三方支付服务提供商在技术能力、市场能力、资金运作能力方面都要求很高。

4) 银行与移动运营商合作的运营模式

银行和移动运营商发挥各自的优势，在移动支付技术安全和信用管理领域强强联手，综合了以金融机构为主导和以移动运营商为主导的两种运营模式，如图 3.6 所示。

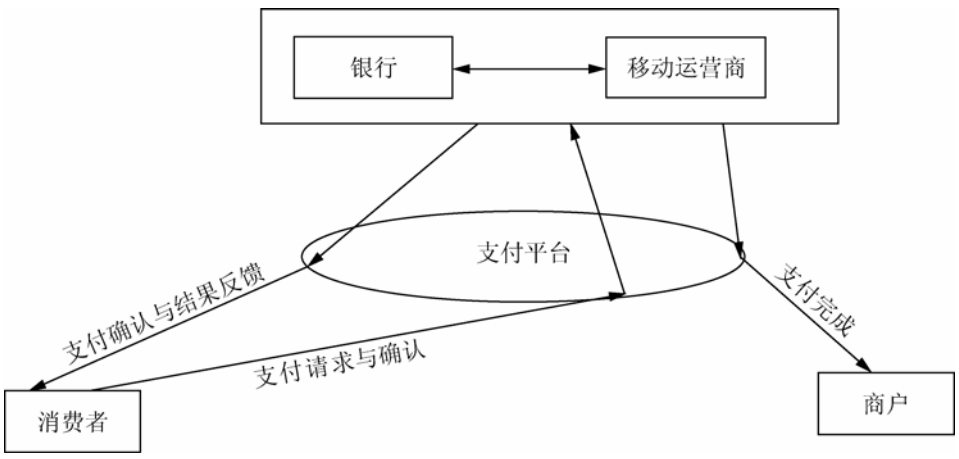

图 3.6 银行与移动运营商合作的运营模式

在这种模式下，移动运营商与银行关注各自的核心产品，形成一种战略联盟关系，合作控制整条产业链；在信息安全、产品开发和资源共享方面合作更加紧密；运营商需要与各银行合作，或与银行合作组织建立联盟关系。

随着中国人民银行即将对电子支付服务提供商实行“牌照制”，移动支付的市场秩序将得到规范和整顿。在产业利益的驱动下，最好的运营模式将是以银行和移动运营商紧密合作为基础，以第三方支付服务提供商的协助支持为推动力的整合商业模式。

3.1.4 移动支付发展现状与面临的主要问题

进入 2009 年，3G 为移动支付业务带来了良好的发展契机和空间，电信运营商和各大金融机构纷纷在移动支付领域开疆拓土。移动支付已经成为“3G 时代应时而生的宠儿”。

1. 我国移动支付的发展现状

(1) 3 大电信运营商在“手机支付”领域展开激烈竞争，我国移动支付进入以非接触式移动支付为主要特征的第三代移动支付阶段。

中国联通于 2009 年 5 月在上海启动了移动支付业务，推出了可刷公交卡的联通 3G 手机，预装目前国际领先的 NFC(非接触式通信)芯片，内置公交卡账户，相当于将市民熟悉的公共交通一卡通“缩微”进了手机中，使用方式和公交卡一样，用户在乘公交车、轨交、出租车时，直接“刷手机”扣费。

中国移动于 2009 年 7 月推出一种全新的 SIM 卡，将 NFC 芯片与 SIM 卡融合，实现电子支付和数据下载等多种功能。用户只要用手机接近读卡器，即可实现小额支付。同时，手机卡账户将和用户银行账户捆绑，一旦手机卡金额花完，可通过短信将银行账户资金转入手机卡内。目前，在上海、重庆等城市，中国移动的用户已经可以通过手机像刷公交卡一样刷卡乘车，亦能像刷银行卡一样在自动售货机购买可乐或在超市购物，甚至还可以直接利用手机购买电影票、火车票或飞机票。

中国电信上海公司推出天翼 3G“移动支付”业务，为用户提供账单支付、手机充值、公用事业费缴费、订购商品服务、自助金融、刷手机消费等手机自助支付服务。

在运营商早期提供的移动支付业务中，基于短信或语音交互绑定后台账户模式的移动支付被认为是移动支付的第一代；基于 WAP 和 Java 方式、通过网络进行支付的模式被认为是移动支付的第二代。上述通过 3G 手机、非接触式的移动支付模式则被认为是移动支付的第三代，这也是目前全球范围内大规模使用的一种移动支付模式。

(2) 移动支付成为金融机构的一大核心关注点。目前，各大银行都开通了以手机银行为代表的移动支付功能，而且不断升级手机银行业务，开展手机银行优惠活动。工商银行、交通银行、建设银行、农业银行、兴业银行等都对原有手机银行进行了系统升级，不仅可以支持普通 WAP 手机用户，而且推出了 3G 版手机银行。建设银行、中信银行、招商银行等也有着功能设计完备的手机银行，开通手机银行的用户，几乎可以完成所有的个人银行非现金业务。各家银行在手机银行的安全性方面也都采取了各自的安全保护方式。例如：建设银行的手机银行为客户身份信息与手机号码建立了唯一绑定关系，加上登录密码的验

证与控制，建立了客户身份信息、手机号码、登录密码三重保护机制，构建了手机银行业务独特的安全特性。为防止有人恶意试探别人密码，系统设置了密码错误次数日累计限制，当达到限制时，将设置该客户手机银行服务为暂停状态。其他银行也在手机银行交易密码上做了双重保证，并且交易限额上也有限制。兴业银行还有图片附加码保护功能。招商银行则设计了图形验证码机制，防止程序自动试探密码，还有密码错误次数过多自动锁定账户，以保证用户安全。

除各大银行以外，中国银联与瀚银科技合作推出了“手付通”，该产品基于自主开发的中国银联新一代移动支付技术，可通过 POS 及 3G 无线网络，用装有手付通 SD 卡的手机实现移动支付的功能。

(3) 移动支付产业论坛促进移动支付产业的发展。2009 年 7 月 24 日，2009 中国移动支付产业论坛在北京开幕，参会各方就移动支付中的技术问题、信息安全问题、产业链各方的合作问题进行了充分的沟通和探讨，这无疑对我国移动支付的发展具有很大的推动作用。

2. 我国移动支付面临的主要问题

现阶段我国移动支付还处在起步阶段，要大规模地普及推广，还面临诸多问题，下面列举其中的几个方面。

(1) 法律制度与行业规范尚待完善。目前中国在电子支付领域的法律体系尚未完善，移动支付参与方的责任与分工缺少明确的法律描述，在行业运营方面也没有可靠的行业操作规范。

(2) 信用与信息安全问题严重。垃圾短信、电话诈骗和资费陷阱等问题导致移动增值服务的诚信度较低，使用户对移动支付的安全性存在疑虑。

(3) 存在成本问题。由于移动支付可能需要安装客户端软件，或使用特定的支持 NFC 技术的终端，这一方面需要用户进一步学习相关操作知识，另一方面存在手机更换成本。如果不能向用户提供足够的优惠服务，将很难吸引用户由现金支付或银行卡支付转向移动支付。

(4) 商业模式难定。目前，3 大主流运营商和主流银行机构都希望以自己为中心建立商业模式，客观上影响了移动支付产业的发展步伐。

3.2 移动支付流程与安全

前面已经提到，按照传输方式的不同，移动支付可以分为远距离支付和近距离支付，如图 3.7 所示[①]。我国移动支付目前采用比较多的是远距离支付技术。不同的支付技术具有不同的支付流程。

① 资料来源：杨坚争．电子商务安全与电子支付．163 页，北京：机械工业出版社，2007。

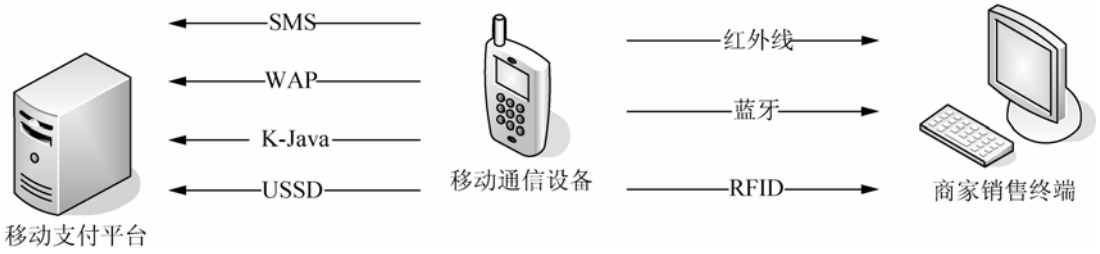

图 3.7　移动支付的两种传输方式

3.2.1　移动支付远距离支付技术及流程

按照移动支付远距离支付接入方式的不同，移动支付可以分为以下 4 类。

(1) 基于短消息(SMS)的方式，其中包括基于 STK 的支付接入方式。

(2) 基于 USSD 的方式。

(3) 基于 WAP 协议的方式。

(4) 基于 K-Java 的方式，其中包括基于 BREW 的支付接入方式。

1. 基于短消息方式的支付

国内提供基于 SMS 移动支付的典型是中国工商银行，工商银行在 2004 年正式在全国范围内推出基于短信的手机银行服务，为个人网上银行用户提供增值服务。

在以金融机构为主导的移动支付运营模式中，用户必须将手机原有的 SIM 卡换成 STK(SIM Tool Kit，用户识别应用工具)卡，STK 卡与 SIM 卡一样都能够在普通手机上使用，但是 STK 卡具有更高的存储量，能够运行应用软件。基于 STK 卡的支付方式与基于 SMS 的移动支付流程相似。中国银行、建设银行、招商银行等都曾提供过 STK 手机银行，但在随后的发展中，多数都被其他类型的手机银行所代替。

1) 短消息业务

短消息分为两类：一类是点到点短消息(SMS)，另一类是校区广播短消息(CBS)，一般意义上提到的短消息主要指的是点到点短消息。

短消息(Short Message Service，SMS)业务是一种在数字蜂窝终端上发送或接收长达 140B 字符消息，并具有存储和转发功能的服务。短消息并不是直接从发送人发送到接收人，而始终通过 SMS 中心进行转发。如果接收人处于未连接状态(可能电话已关闭或超出服务范围)，则消息将在接收人再次连接时发送。

点对点短消息既是一种基本电信业务，又可以作为信息服务业务的数据传输载体提供增值业务，如信息点播服务及远程数据操作业务。由于短消息需在短消息中心存储转发，所以实时性较弱。

短消息业务以较低的延迟支持国际漫游，因此特别适合多用户寻呼、E-mail、语音邮件通知和消息类业务等应用，但具体提供给用户的各种功能和相应的收费在很大程度上仍依赖于网络运营商所提供的服务水平。已经有大量的应用可以使用计算机来接收和发送短消息。

2) 基于 SMS 的移动支付流程

主要采用的是点到点短消息模式，这种方式广泛在欧洲和亚洲使用，基于 SMS 支付方式的支付流程如图 3.8 所示。

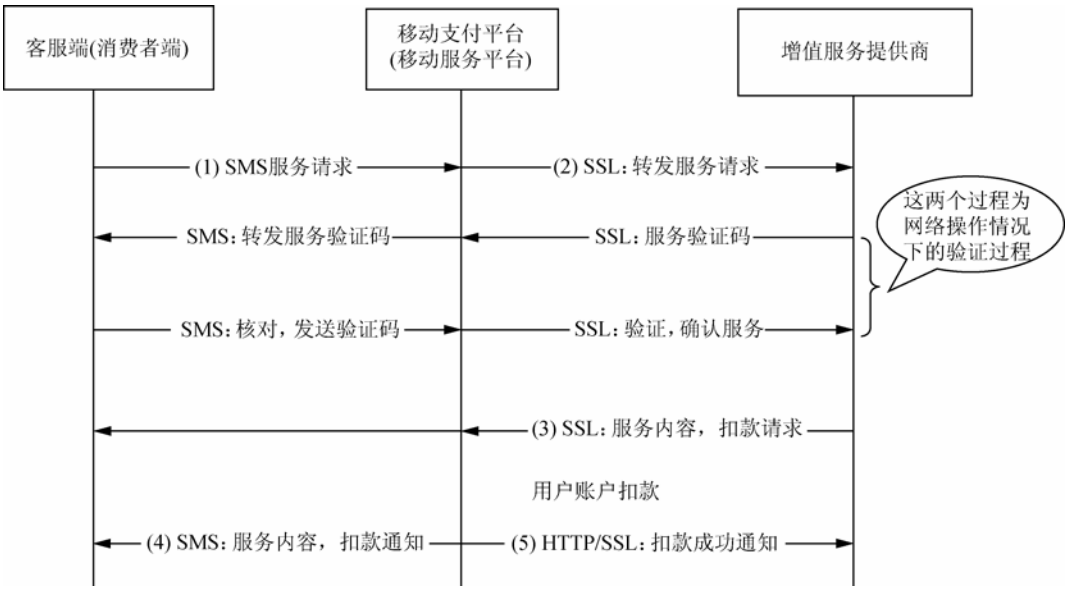

图 3.8 基于 SMS 支付方式支付流程[①]

(1) 用户通过短消息形式向移动支付平台请求内容服务。

(2) 移动支付平台收到请求内容后认证用户的合法性及账户余额，如果合法则向增值服务提供商请求内容，不合法则返回相应错误信息。

(3) 增值服务提供商收到移动支付平台的内容请求后，认证移动支付平台的合法性，如果合法，则增值服务提供商发送请求的内容给移动支付平台，否则返回相应错误信息。

(4) 移动支付平台从用户的账户中扣除相应费用，然后把收到的内容转发给用户，同时告诉用户付款结果。

(5) 移动支付平台通知增值服务提供商转账成功。

在 SMS 系统中，费用从用户的话费中扣除，账户的处理由移动支付平台来完成，银行不参与，因此 SMS 系统仅适合于小额的信息服务。SMS 方式移动支付的安全性主要由短消息的安全性决定。这种方式的优点是费用低廉、节省成本，符合手机使用群体以低成本享受高质量服务的期望。

2. 基于 USSD 方式的支付

1) USSD 简介

USSD(Unstructured Supplementary Services Data，非结构化补充业务数据)是基于 900/1800MHz 数字蜂窝移动网络的一种应用，遵循 GSM 02.90，GSM 03.90，GSM 04.90

① 资料来源：邓方民．移动支付安全机制研究，2006。

标准。它是一种面向连接的基于会话的数据业务，在使用上与 SMS 非常类似。用户可以在移动终端上按照规定的格式编辑 USSD 字符串，然后发起 USSD 请求。USSD 在非通话状态下使用独立专用控制信道，每个 USSD 会话占用一个专用控制信道，传输速度约 600B/s；在通话状态下使用快速随机控制信道，传输速度约 1 000B/s。USSD 第一阶段规范只支持移动台发起的 USSD 操作，且只支持一次交互，因此只适合简单的业务；第二阶段规范引入了对网络发起的 USSD 操作的支持，允许移动平台与网络间的持续会话。

USSD 是继短消息业务后在 GSM 移动通信网络上推出的又一新型增值业务。USSD 业务与 SMS 的主要区别在于 SMS 采用的是存储转发方式，而 USSD 业务系统采用的是面向连接、提供透明通道的交互式会话方式，是会话类业务的理想载体，具有响应速度快、交互能力强、可靠性高的特点，特别适合开展支付型、交易型的业务(如银行转账、股票彩票业务、移动电子商务小额交易等)。大多数普通 GSM 手机支持 USSD 功能，可使手机用户在不换卡的情况下，采用菜单方式访问各项 USSD 业务，有利于减低用户操作难度。

2) 基于 USSD 接入方式的移动支付流程

基于 USSD 接入方式的移动支付流程如图 3.9 所示。

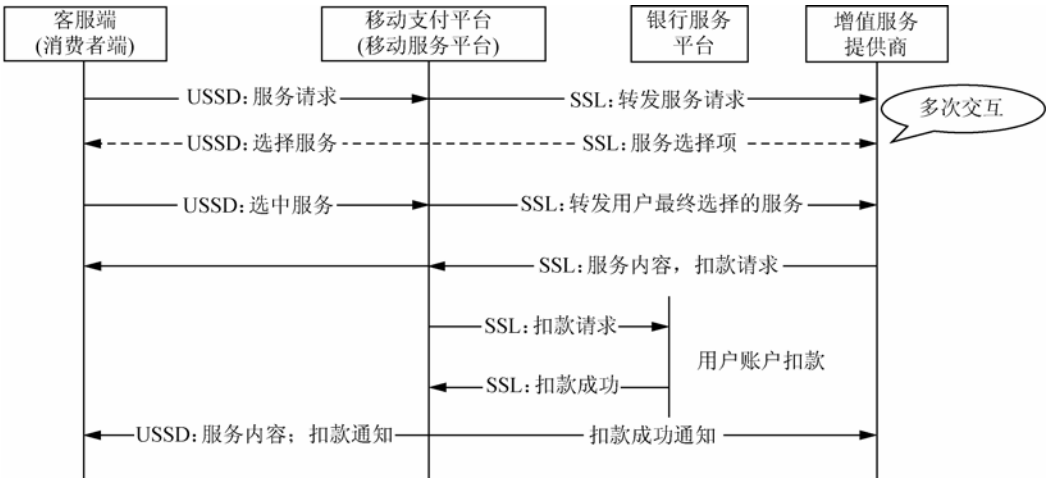

图 3.9 基于 USSD 接入方式的移动支付流程[①]

3. 基于 WAP 方式的支付[②]

目前，我国几乎所有银行都在着力提供 WAP 方式的手机银行，其中发展成效最好的当数中国建设银行。早在 2000 年建设银行就已携手中国移动共同探索手机银行服务的研发，相继提供了 STK 手机银行、BREW 手机银行(类似于 K-Java 手机银行)，2005 年与中国联通合作在业内首次推出联通 WAP 手机银行。该手机银行功能可形象地表述为“手机理财+手机支付+手机电子商务”，它是国内首个大规模推出支持在线交易的金融服务，让我国手机银行服务的发展有了一次跳跃式的进步。随后又在 2006 年与中国移动合作推出移动 WAP 手机银行。

① 资料来源：邓方民．移动支付安全机制研究，2006。

② 资料来源：王雨．WAP 移动支付体系结构研究，2004。

1) WAP 简介

WAP(Wireless Application Protocol，无线应用协议)由一系列协议组成，用来标准化无线通信设备。WAP 将 Internet 和移动电话技术结合起来，使随时随地访问丰富的互联网络资源成为现实。WAP 服务是一种手机直接上网，通过手机 WAP“浏览器”浏览 WAP 站点的服务，可享受新闻浏览、股票查询、邮件收发、在线游戏、聊天等多种应用服务。通过 GPRS 网络接入 WAP，可充分发挥接入时延短(2s 接入)、速率高、永远在线、切换方便等优点。

WAP 由 WAP 论坛(WAP Forum，网址为 http://www.wapforum.com)发布，WAP 论坛由爱立信、摩托罗拉、诺基亚以及 Unwired Planet 创建于 1997 年 6 月。WAP 论坛的成员目前占据着超过 90%的全球手机市场，同时又是领先的基础设施提供商、软件提供商及其他机构。正是由于 WAP 论坛成员有广泛的代表性，其制定的 WAP 规范具有多厂商设备可以互操作的特点，所以 WAP 有望成为业界广泛接受和使用的无线信息网络连接方式。WAP 标准和其他技术文档可以直接从 WAP 论坛上下载。

WAP 无线应用协议的产生使移动设备能够直接访问国际互联网上的资源，WAP 可以支持目前使用的绝大多数无线设备，包括移动电话、FLEX 寻呼机、双向无线电通信设备等。目前，WAP 已经成为移动通信业中的一大热点，WAP 具有以下特点。

(1) WAP 是公开的全球无线协议标准，并且是基于现有的 Internet 标准制定的。

(2) WAP 提供了一套开放、统一的技术平台。WAP 定义了一套软硬件的接口，实现了这些接口的移动设备和网站服务器可以使人们像使用 PC 一样，使用移动电话收发电子邮件甚至浏览 Internet。

(3) WAP 定义了一种 XML(Extensible Markup Language)语法，被称做 WML(Wireless Markup Language)；WML 是专门为小屏幕和无键盘手持设备服务的语言。

(4) WAP 协议可以广泛地运用于 GSM、CDMA、TDMA、3G 等多种网络。

(5) 为保持现有的巨大移动市场，WML 用户的界面直接映射到现有的手机界面上。

2) WAP 应用体系结构

WAP 的应用模型是基于 WWW 的客户/服务器结构(即 B/S 结构)，客户方通过浏览器向 Internet 上的服务器请求以标准格式表示的 Web 页面内容；该模型还针对无线和移动环境的特点对内容格式、通信协议等方面进行了优化和扩展；可以利用现有的大量应用开发工具(如 Web 服务器、XML 工具等)。

WAP 的目标是利用其在 Internet 上的对等 Web 结构，使内容提供商和移动设备之间的通信比在单独使用情况下更有效和省时。因此 WAP 应用结构非常类似于 Internet 结构。一个典型的 WAP 应用系统如图 3.10 所示。

图 3.10 WAP 应用体系结构

在一个 WAP 应用系统中包括以下 3 种实体。

(1) 具有 WAP 用户代理功能的移动终端。典型的移动终端是 WAP 手机，它相当于 Internet 中的 PC，在它的显示屏上运行有微浏览器(Micro-Browser)，用户可以采用简单的选择键来实现 WAP 服务请求，并以无线方式发送和接收所需的信息。WAP 终端使用 WML(Wireless Markup Language，无线标记语言)显示各种文字图像数据。

(2) WAP 网关。WAP 网关(即 WAP 代理)实现了 WAP 协议栈(WSP，WTP，WTLS 和 WDP)与 Internet 协议栈之间的转换；利用信息内容编码/解码器(Content Encoders And Decoders)把 WAP 数据压缩编码，减少了网络数据流量，最大限度地利用无线网络缓慢的数据传输速率。同时，WAP 还采用了错误校正技术，确保网络浏览和数据过程不会因无线通信线路质量的变化而受到影响。

(3) 应用服务器。支持 WAP 的 Web 网站就存放在应用服务器上，服务器中存有用 WMLScript 及 WML 编写的 WAP 应用，这些应用可以根据 WAP 移动终端的需要而被下载，在不需要时可以从 WAP 终端中卸载。

WAP 应用系统的基本工作过程如下：WAP 移动终端上 WAE(Wireless Application Environment)用户代理将编码后的 HTTP 请求通过无线接口，经由无线通信网络发送给 WAP 网关，网关解码请求后将其转换为标准的 HTTP 请求提交给内容服务器(即应用服务器)。响应消息从内容服务器返回到 WAP 网关后，网关再对响应信息进行编码并返回给移动客户端，WAE 用户代理负责解释并显示响应数据。

3) WAP 安全机制

WAP 环境的安全机制包括 WIM、WIMScript、WTLS、WPKI 4 个安全标准。

(1) WIM。WIM(WAP Identity Module)是安装在 WAP 设备里的微处理器芯片，能够保存一些关键信息(如 PKI 公钥和用户的私钥信息)，WIM 通常使用智能卡实现。

(2) WIMScript。WIMScript(WAP Script Crypto API)是 WIMScriptLib 库提供的应用编程接口，包含密钥产生、数字签名，以及处理一些常用的 PKI 对象的函数。

(3) WTLS。WTLS(Wireless Transport Layer Security)是基于互联网中的 TLS 的传输层安全协议。WTLS 能够实现对通信参与方的认证，对 WML 数据加密，并能保证 WML 数据的完整性。WTLS 针对无线设备通信的低宽带特性进行了优化。

(4) WPKI。WPKI(Wireless Application Protocol PKI)为无线应用协议的 PKI，是传统 PKI 在无线应用环境中的优化扩展。详细内容参见本节安全部分。

4) WAP 移动接入方式的支付流程

WAP 移动支付接入方式的支付流程如图 3.11 所示。从移动客户端开始，经过商家、支付网关并最后到达银行端；银行经过验证、处理后，向商家及移动终端发出反馈说明本次交易状态。其中银行与商家不进行直接通信，而是通过商家在银行注册的支付网关进行转发；对于移动终端，则由银行向其发送签名消息来完成通知过程。

具体而言，WAP 移动接入方式的支付流程可以分为 5 个阶段。与有线交易不同的是，移动客户在整个交易过程中并不是一直处于连接状态，移动终端向商家提供订购信息后便断开网络连接，等待从银行发来的支付确认签名短信。这种做法有效地节约了无线网络的带宽，也从经济上为客户节省了开支，是目前一种可取的办法。

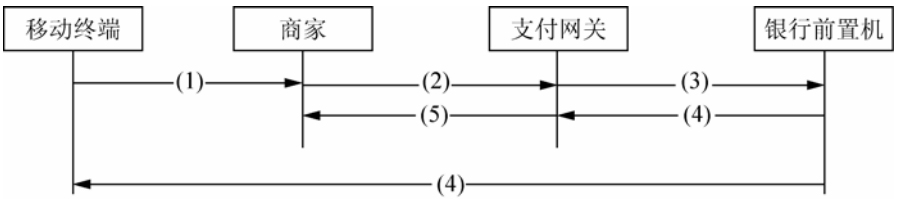

图 3.11　WAP 移动接入方式支付流程

交易过程从移动终端用户开始，可能有以下两种情况。

(1) 网上购物。客户从商家主页获取商品信息并做出选购，当商家发回确认信息后，再由客户生成交易数据。

(2) 直接支付。客户不需要浏览商家网站，而只是进行一种简单的支付行为。例如，客户可能到某个超市进行购物，付款时发现身上没带现金，也没带银行卡，因此，客户选择移动支付方式，从商家获得代表本次交易的交易号，并将交易号、金额、商家账号等信息输入移动设备后向商家服务器提出支付请求。

不论哪种情况，真正的支付流程以商家向客户端发送支付确认为标志，以上述直接支付情况为例，支付流程图的各步骤具体含义如下。

(1) 客户端移动设备访问商家服务器，并与商家 WAP 网关建立安全连接。

(2) 商家提供未支付的交易查询，保证客户能够通过交易序列号查询出本次交易所需支付的金额。

(3) 商家向支付平台发出连接请求，支付平台收到请求后向其发送自己的数字证书。如果商家验证支付平台证书通过，则将数据以平台的公钥加密，将交易数据以及商家自己的证书发送给支付网关。支付网关利用商家证书验证商家身份，如果通过验证，则证明商家身份合法，可以进行通信；否则，发出警告并断开连接。

(4) 银行前置机是整个交易流程的最后一个处理环节，并且是银行内部系统的外部接口。银行前置机根据支付平台传过来的支付请求信息生成本行内部使用的命令，操纵内部数据库，完成转账过程。

(5) 支付结果反馈。完整的反馈过程由银行端发起，银行端会同时向支付平台及客户端发送支付确认消息。由于支付平台及客户端在银行均有注册，所以可以根据对象的不同使用其公钥进行加密，并附加上保证数据完整性的数字签名进行反馈。

4. 基于 K-Java 方式的支付[①]

国内提供 K-Java 方式手机银行服务的典型代表是兴业银行和工商银行上海分行。兴业银行 K-Java 手机银行提供的服务主要包含两大类：外汇和银证。与基于短信方式的手机银行相比，基于 K-Java 方式的手机银行界面更友好、输入/输出更方便，网络传输更快；而与基于 WAP 方式的手机银行相比，则存在必须先下载客户端的劣势。

1) K-Java 及其规范

K-Java 即 J2ME(Java To Micro Edition)，是 Sun 公司专门用于嵌入式设备的 Java 软件。

① 资料来源：邓方民．移动支付安全机制研究，2006。

利用 K-Java 编程语言为手机开发应用程序，可以为手机用户提供游戏、个人信息处理、电子地图、股票等服务程序。J2ME 致力于消费产品和嵌入式设备的最佳解决方案，其遵循“对于各种不同的装置而造出一个单一的开发系统是没有意义的事”这个基本原则，将所有的嵌入式装置大体上区分为两种：一种是运算功能有限、电力供应也有限的嵌入式装置(例如 PDA、手机等)；另外一种是运算能力相对较佳并且在电力供应上相对比较充足的嵌入式装置(例如冷气机、电冰箱等)。针对这两种嵌入式设备引入了两种规范：把上述运算功能有限、电力有限的嵌入式装置规范为 Connected Limited Device Configuration(CLDC)规格；而另外一种装置则规范为 Connected Device Configuration(CDC)规格。

2) 基于 K-Java 接入方式的移动支付流程

基于 K-Java 接入方式的移动支付流程如图 3.12 所示。

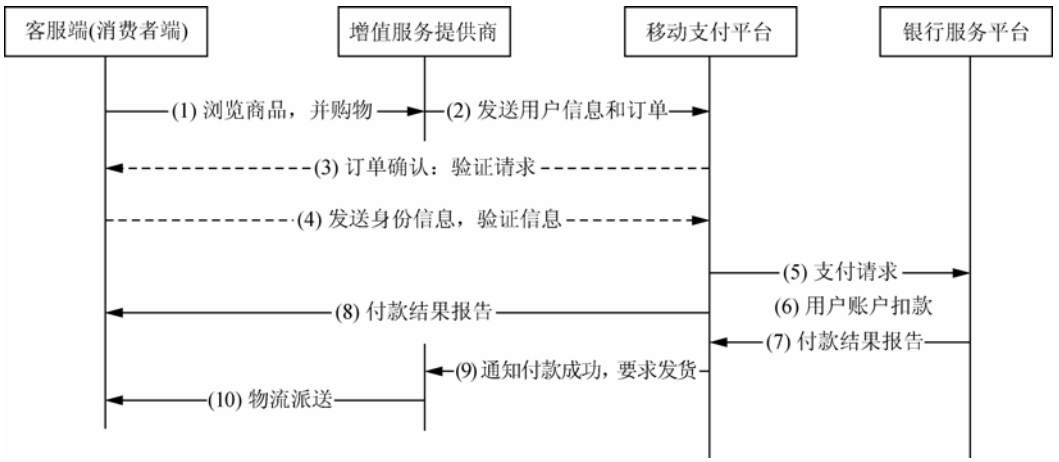

图 3.12　K-Java 接入方式支付流程

(1) 用户挑选商品后，由商家服务人员录入所买商品的详细信息，并按固定格式形成订单。用户核对完订单后告诉服务人员手持设备的号码。

(2) 商家对该订单和手持设备(如手机号)加密、签名后通过安全 Internet 通道(SSL)发送给移动支付平台。

(3) 移动支付平台收到消息后确认消息的来源，如果消息确实来自指定商家则对消息处理(如加密签名)后发送给移动用户。

(4) 用户收到移动支付平台发来的消息后，进行验证，输入 PIN 码，同意使用移动支付系统，然后确认所买的商品、消费额、商家标示及消息来源，如果消息正确，则同意支付。消息处理后传送给移动支付平台。

(5) 移动支付平台确认消息正确后向银行发起转账请求。

(6) 银行处理支付。

(7) 移动支付平台收到转账成功的消息。

(8) 用户收到电子发票或收据。

(9) 商家收到支付成功的通知。

(10) 商家为客户提供服务。

3.2.2 移动支付近距离支付技术

在近距离支付中，常采用的支付技术有红外线技术、蓝牙技术及射频识别技术 3 种。目前，基于 RFID 的非接触式移动支付正在逐步取代蓝牙、红外线等非接触式移动支付技术成为非接触式移动支付的新宠。

1. 红外线

红外线(Infrared Rays)是一种光线，是波长为 750nm～1mm 的电磁波，由于它的波长比红色光(750nm)还长，超出了人眼可以识别的(可见光)范围，所以是不可见光线。

红外线由德国科学家霍胥尔于 1800 年发现，又称为红外热辐射(Infrared Radiation)，它的频率高于微波而低于可见光，通常把波长为 0.75～1 000 μm 的光都称为红外线，并可以按照波长继续细分为 3 部分，即近红外线，波长为 0.75～1.50 μm；中红外线，波长为 1.50～6.0 μm；远红外线，波长为 6.0～1 000 μm。红外线具有普通光的性质，常常被用做近距离视线范围内的通信载波。

红外线传输是一种点对点的无线传输方式，传输对象间不能离得太远，要对准方向，且中间不能有障碍物，几乎无法控制信息传输的进度。目前红外线应用于移动支付主要是在日本和韩国。

2002 年 7 月，韩国的 HarexInfo Tech 开始对基于红外线非接触式移动支付系统的测试，该系统名为 ZOOP，用户可以通过手机中的“手机钱包”进行支付，具体的支付流程如图 3.13 所示[①]。

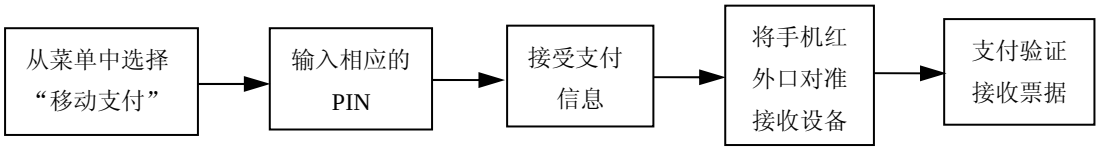

图 3.13 ZOOP 手机支付流程

2. 蓝牙

蓝牙技术(Bluetooth)是一种无线数据与语音通信的开放性全球规范，它以低成本的近距离无线连接为基础，为固定与移动设备通信环境建立一个特别连接，同时形成一种个人身边的网络，使得身边各种信息化的移动便携设备都能无缝地实现资源共享。蓝牙以 WLAN 的 IEEE 802.11 标准技术为基础，使用全球通用并且无须申请执照的 2.45GHz 无线频带。系统设计通信距离为 10cm～10m，如增大发射功率，其距离可长达 100m。

近年来，世界上一些权威的标准化组织，也都在关注蓝牙技术标准的制定和发展。越来越多的设备厂商和驱动厂商支持蓝牙，蓝牙已逐渐成为较为普及的一种无线近距离通信技术。在短距离技术应用方面，蓝牙技术正逐步超越红外技术，成为手机中的主要传输技术。

2001 年，爱立信与 EurocardAB 在瑞典开始测试基于蓝牙的移动支付系统，具有蓝牙

① 资料来源：诺达咨询，本书作者翻译。

支付功能的手机与 Eurocard 账号进行了绑定，其交易流程如图 3.14 所示[①]。

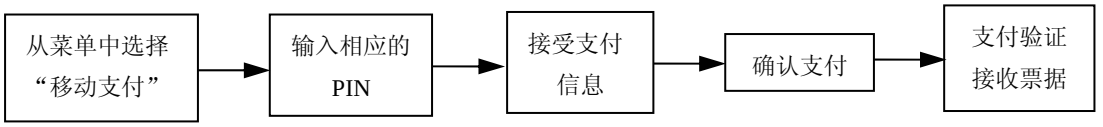

图 3.14　Eurocard 手机支付流程

3. RFID

RFID(Radio Frequency Identification)即射频识别技术，射频识别技术是 20 世纪 90 年代开始兴起的一种自动识别技术，射频识别技术是一项利用射频信号通过空间耦合(交变磁场或电磁场)实现无接触信息传递并通过所传递的信息达到识别目的的技术。

RFID 产品的工作频率有低频、高频和超高频，根据频率可以定义符合不同标准的不同产品，不同频段的 RFID 产品有不同的特性。

RFID 是 20 世纪 90 年代兴起的一项自动识别技术。与传统识别方式相比，RFID 技术无须直接接触、无须光学可视、无须人工干预即可完成信息输入和处理，操作方便快捷。

采用 RFID 技术的支付流程与采用蓝牙技术的移动支付流程类似。

3.2.3　移动支付面临的安全问题与技术保障

移动支付涉及支付用户资金的安全和相关信息的保密等问题，开展移动支付要面对来自移动通信系统和互联网的安全风险，这给移动支付提出了更高的安全要求。

1. 移动支付面临的安全问题

移动支付中面临的安全问题主要存在于 3 个方面：无线链路、服务网络和终端。具体而言，主要包括以下问题。

1) 窃听

窃听是最简单的获取非加密网络信息的形式，这种方式可以同样应用于无线网络。由于无线网络本身的开放性特点，以及短消息等数据一般都是明文传输，这使得通过无线空中接口进行窃听成为可能。攻击者通过窃听有可能了解支付流程，获取用户的隐私信息，甚至破解支付协议中的秘密信息。

2) 重传交易信息

攻击者截获传输中的交易信息，并把交易信息多次传送给服务网络。多次重复传送的信息有可能给支付方或接收方带来损失。

3) 终端窃取与假冒

攻击者有可能通过窃取移动终端或 SIM 卡来假冒合法用户，从而非法参与支付活动，给系统和交易双方造成损失。通过本地和远程写卡方式，攻击者还有可能修改、插入或删除存储在终端上的应用软件和数据，从而破坏终端的物理或逻辑控制。

4) 中间人攻击

如果攻击者设法使用户和服务提供商间的通信变成由攻击者转发，那么该中间人可完

① 资料来源：诺达咨询，本书作者翻译。

全控制移动支付的过程，并从中非法牟利。

5) 交易抵赖

当移动支付成为普遍行为时，就可能存在支付欺诈问题。用户可能对发出的支付行为进行否认，也可能对花费的费用及业务资料来源进行否认。随着开放程度的加强，来自服务提供商的抵赖可能性也会有所增加。

6) 拒绝服务

破坏服务网络，使得系统丧失服务功能，影响移动支付的正常运行，阻止用户发起或接受相关的支付行为。

2. 移动支付安全需求

移动支付应对支付本身、支付所涉及的内容进行恰当的保护，确保交易双方的合法权益不受非法攻击者的侵害。通常，移动支付应满足下面几个方面的安全需求。

1) 秘密性

秘密性是指防止合法或隐私数据为非法用户所获得，即在移动支付过程中，即使非法用户获得用户的交易信息也无法知晓信息内容，从而无法使用。

2) 完整性

完整性是指维护信息的一致性，即移动支付的交易信息在生成、传输、储存和使用过程中不发生人为或非人为的非授权篡改。

3) 不可抵赖性

不可抵赖性是指移动支付交易的各方无法在事后否认曾对交易信息进行的生成、签发、接受等行为，是对移动支付交易各方真实同一性的安全要求。

4) 可认证性

移动支付应提供完备的身份认证，确保交易双方是可以信任的，即确保服务间的相互身份认证，防止欺诈行为的产生。

5) 可用性

可用性是指保障交易信息资源随时可提供服务的特性，即移动支付各方的授权用户可以随时访问所需交易信息。可用性是信息资源服务功能和性能可靠性的度量，涉及物理、网络、系统、数据、应用和用户等多方面的因素，是对信息网络总体可靠性的要求。

3. 移动支付的安全技术保障

为解决移动支付面临的安全问题，满足移动支付安全需求，从管理上来说，一般采用限额控制(即设定一定的支付限额)和签约机制(如部分银行客户在享受手机银行服务时需与银行签订服务协议)；从技术上来说，一般采用访问控制技术使支付中的交易信息不被非法用户获取和篡改，采用身份认证技术实现对交易各方的身份认证，采用数字签名技术实现信息的保密等。与一般的网络传输相比，移动支付安全在身份认证技术和数字签名技术上具有新的特点。

1) 移动支付身份认证技术

在移动电子商务中，每一次交易活动都会涉及不少于两个交易实体之间的对话，所以移动支付安全性的一个关键方面就是能否对交易实体的身份进行认证。

(1) 移动支付身份认证体制的要求。一个安全的身份认证体制至少需要满足下列要求。

① 互相认证性：服务提供者和用户的相互认证。

② 可确认性：已定的接受者能够校验和证实信息的合法性、真实性和完整性。

③ 不可否认性：消息的发送者对所发的消息不能抵赖，有时也要求消息的接受者不能否认所收到的消息。

④ 不可伪造性：除了合法的消息发送者之外，其他人不能伪造合法的消息。

为了满足上述安全需求，身份认证体制往往需要引入可信的第三方，这样，身份认证主要由用户实体、提供信息服务的网络和可信的第三方 3 个方面组成。

对于传统应用领域，如有线电子商务，认证体制往往采用认证中心(CA)作为可信的第三方来发放和管理数字证书。数字证书是一种数字信息附加物，由证书权威机构颁发，该证书证明发送者的身份并提供加密密钥。PKI(Public Key Infrastructure)提供了与加密和数字证书相关的一系列技术，成为有线电子商务等领域身份认证或访问控制安全模块的首选。

移动支付应用领域的身份认证技术因为移动环境和移动终端的特殊性而提出了更高的要求。在无线通信环境下，PKI 无法实现无线终端和有线设备之间的互通，同时，移动终端计算能力非常有限以及数据流速率低的特点，也使得传统的 PKI 体制无法成为移动安全支付的合理解决方案。WPKI(Wireless Public Key Infrastructure，无线公钥基础设施)，即无线 PKI，是 PKI 结合移动环境特点的产物。WPKI 的出现和发展，为解决移动安全支付的身份认证问题提供了合适的选择。

(2) 无线公钥基础设施技术。WPKI 并不是一个全新的 PKI 标准，它是传统的 PKI 技术应用于无线环境的优化扩展。它采用证书管理公钥，通过第三方可信机构——认证中心(CA)验证用户的身份，从而实现信息的安全传输。

在移动支付过程中，存在着无线网络和有线网络之间的连接问题。无线应用协议(WAP)解决了这个连接问题，但在其实现过程中需要 WPKI 的支持。

WPKI 的工作流程主要包括两个部分，一是完成 WPKI 证书的发放，二是实现 WAP 的安全连接，如图 3.15 所示。

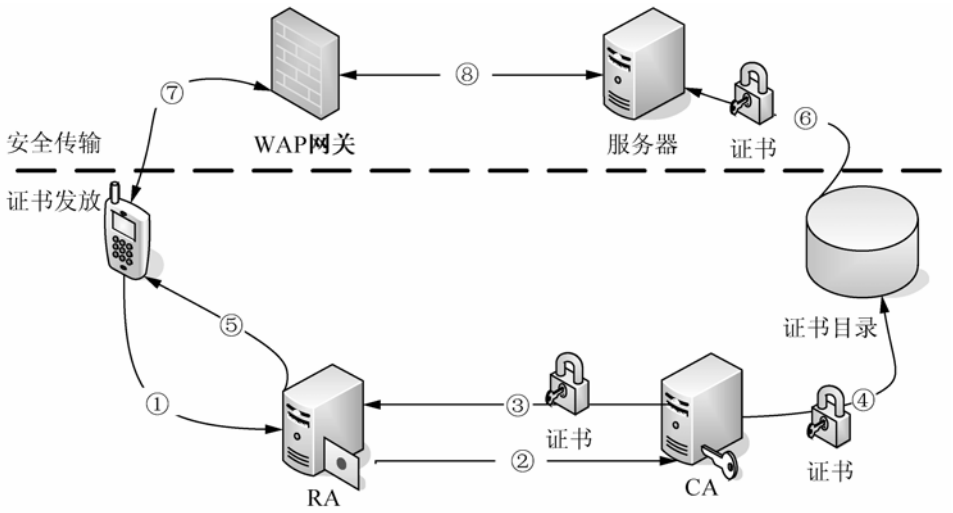

图 3.15　WPKI 工作流程图[①]

① 资料来源：李峰．移动支付安全研究，优秀硕士论文，2008。

① 用户向注册中心(RA)提交证书申请。

② RA 对用户的申请进行审查，审查合格将申请发给认证中心(CA)。

③ CA 为用户生成一对密钥并制作证书，将证书交给 RA。

④ CA 同时将证书发布到证书目录中，供有线网络用户查询。

⑤ RA 保存用户的证书，针对每一份证书产生一个证书 URL，将该 URL 发送给移动终端。

⑥ 有线网络服务器下载证书列表备用。

⑦ 移动终端和 WAP 网关利用 CA 颁发的证书建立安全连接。

⑧ WAP 网关与有线网络服务器建立连接，实现移动终端和有线网络服务器安全信息传送。

除了上述工作流程之外，WPKI 体系还规定了其他内容，包括证书的格式，证书的撤销和更新机制等，这些内容与对应的有线环境下所采用的 PKI 体系的内容是一致的。

WPKI 不仅可以用于移动支付，还可以用于电子邮件等其他移动电子商务领域。现在对 WPKI 技术的研究是 WAP 研究的热点，美国、日本和欧洲各国的 WPKI 体系均具备自己完整的协议体系，并且已经在无线数据业务中得到实际应用，国内的一些厂商也正在着手 WPKI 技术的研究和开发，而且也取得了一定程度的进展。但是，WPKI 还存在不少问题，需要进一步的研究，主要包括证书、交叉认证技术、桥接技术和弹性 CA 技术等问题，还没有得到很好解决。

总之，WPKI 是移动支付的关键安全技术，在无线领域具有很广阔的应用前景，但是 WPKI 目前的认证方案还不是系统级的安全认证，需要进一步深入研究。

2) 移动支付数字签名技术

在移动支付应用领域，移动支付所需要采用的数字签名技术除了需要满足数字签名的基本条件之外，还需要结合移动安全支付中移动终端计算能力和存储能力弱的特点，选取更加合适的公钥密码算法。椭圆曲线密码体制算法正好能满足这些要求。

椭圆曲线数字签名协议的实现过程包括两个主要步骤：密钥的产生和签名的生成与确认。假设商家和移动支付平台两个主体要实现数字签名，商家在密钥产生之前，必须选定一个 7 元组 $T=(q, FR, a, b, G, n, h)$作为椭圆曲线域的参数，并确保其有效。其中 q 代表有限域 Fq；FR 为域表示法；a，b 是方程中的系数；G 为基点；n 为大素数并且等于点 G 的阶；h 是小整数，称为余因子。

然后，进行以下步骤的操作。

(1) 密钥的产生。商家随机选择区间[1，$n-1$]内的一个随机或伪随机数 d；计算 $Q=dG$ 此时，商家的公钥是 Q，私钥是 d。

商家的公钥 Q 和私钥 d 生成之后，还必须经过特定的算法或协议进行公钥和私钥的有效性证明，才能够正确地进行签名的生成与确认。

(2) 签名的生成和确认。

商家拥有了特定的域参数 7 元组 $T=(q, FR, a, b, G, n, h)$和有效的密钥对(d, Q)之后，就可以利用自己的私钥 d 对消息进行数字签名。

移动支付平台必须首先得到域参数 $T=(q, FR, a, b, G, n, h)$和商家的公钥 Q，并对其有效性进行确认，然后利用商家的公钥 Q 对接收到的消息签名进行确认。

椭圆曲线数字签名协议无论在安全性方面还是在实现效率方面，都具有其他签名算法不可比拟的优势，具有广泛的应用空间。在安全性方面，椭圆曲线数字签名协议的安全性基于椭圆曲线离散对数问题和单向散列函数的安全性，比其他公钥密码算法要高得多。在实现效率方面，椭圆曲线数字签名协议所使用的运算是一些简单的位运算，其运算速度比较快，运行效率比较高。

3.3 移动支付举例

目前，工农中建四大国有银行和很多股份制银行都开通了以手机银行为代表的移动支付功能。下面将介绍招商银行的手机银行情况[①]。

招商银行手机银行目前版本为 WAP 版，登录网址为 http://mobile.cmbchina.com，系统介绍可参见网址 http://mobile.cmbchina.com/MobileWap。

3.3.1 招商银行手机银行概况

1. 招商银行手机银行客户及使用成本

要成为招商银行手机银行 WAP 版的客户，需要满足以下两个条件。

1) 在招商银行办理一卡通或信用卡个人卡

“一卡通”是招商银行向社会大众提供的、以真实姓名开户的个人理财基本账户(也就是大家熟悉的储蓄卡、借记卡)，它集定活期、多储种、多币种、多功能于一卡。当然，上述客户也可以注册为招行一网通用户，“一网通”用户是招行一网通系列网站、社区、各专业系统联合推出的一种新型用户模式。“一网通用户”可关联多张招商银行卡及存折，关联卡折个数不限。“一网通”用户一经注册，就可在一网通全系统中通行使用，包括招行个人银行大众版、手机银行、信用卡俱乐部、商城、房城、社区等，无须在各系统中再次分别注册。登录时只需输入一网通用户的“网银密码”，即可管理所有关联卡。注册了一网通用户，原有银行卡、存折登录方式仍有效。

2) 手机支持 WAP 1.1 或更高版本的 WAP 协议

注意：有的手机不支持 WTLS 安全协议，将无法使用招商银行手机银行 WAP 版。

满足上述条件的客户无须注册，直接登录 http://mobile.cmbchina.com，就可以使用招商银行手机银行 WAP 版。

使用招商银行手机银行，用户仅需要向移动运营商支付访问手机银行所产生的网络流量费用。除此之外，招商银行不收取任何其他服务费用。

目前手机上网的费用已经在普通大众可接受的水平之内。例如，登录一次招行手机银行的流量约 6KB，做一次交易查询的流量约 10KB，做一次转账的流量约 6KB，平均每笔交易的流量不到 10KB。以广东移动 GPRS 标准资费方式(1 元 1MB 流量)计算，一次交易的成本约 0.01 元。

① 资料来源：中国招商银行网站(http://www.cmbchina.com)。

移动互联网业务正在成为移动运营商一个重要的利润增长点，为了迅速推动移动互联网业务的普及和成长，移动运营商不断降低手机上网费用，这将是一个长期的趋势。

2. 招商银行手机银行功能

招商银行手机银行以稳步发展、保障安全为前提，以满足广大招行客户需求为宗旨，以实现让用户 7×24 小时随时随地享受优质银行服务为目的，提供了可靠、便捷的掌上金融服务——招商银行手机银行 WAP 版。

招商银行手机银行提供以下功能。

1) 一卡通功能

持有招商银行一卡通的客户可以享受招商银行手机银行的以下功能。

(1) 账户管理：账户查询、交易查询、密码管理、挂失。

(2) 自助转账：转一卡通、转信用卡、转存折、转他行账户、定活互转、银证转账。

(3) 投资管理：基金、证券。

(4) 自助缴费：缴手机费、缴电话费、缴其他费用。

(5) 网上支付：网上支付交易查询、网上支付额度管理。

2) 信用卡功能

持有招商银行信用卡个人卡的客户可以享受招行手机银行的以下功能。

(1) 账户管理：账户查询、已出账单、未出账单、密码管理。

(2) 还款管理：自动还款设置、还款明细查询。

(3) 网上支付：网上支付功能申请、网上支付交易查询、网上支付额度设置。

(4) 卡片管理：卡片额度调整。

(5) 自助缴费：缴手机费、缴电话费、缴其他费用。

(6) 积分管理：积分查询。

3) 理财助手

(1) 提醒服务：每日基金净值短信提醒管理、日程安排及短信提醒管理。

(2) 工具箱：包含一些实用工具(该功能即将推出)。

为保证安全，对某些功能，招商银行会要求客户到柜台办理相关协议手续。

3. 招商银行手机银行安全措施

手机银行作为一种新兴渠道的银行服务产品，其安全性一直是用户关注的重点。对客户来说，安全风险主要包括资金盗用的风险和信息泄漏的风险，招商银行手机银行 WAP 版通过以下措施来确保客户资金与信息的安全。

1) 招商银行保障客户资金安全的措施

招商银行手机银行的资金转出功能有严格限制，必须要客户本人到柜台去办理转账协议才能转账至某个特定的账户，不允许转出资金至未签订协议的账户。因此，客户不需要担心使用手机银行导致资金被盗用的风险。

2) 招商银行保障客户信息安全的措施

敏感信息泄漏是发生风险的开端，招行针对以下几种窃取信息方式采取了相应的安全保障措施。

(1) 截获网络传输数据。招商银行手机银行采用 SSL 安全协议进行高强度的数据加密传输，即使网络传输的数据被截获，也无法解密和还原。

(2) 散布木马。散布木马是 PC 和互联网上最普遍，也是最有效的信息窃取方式，与此相比，手机在抵御木马方面具有先天的优势。首先，手机操作系统平台具有封闭性、复杂性和多样性特征，不同手机生产厂商采用的操作系统平台不同，即使同一个厂商的不同型号手机也可能使用不同的操作系统，而且操作系统的接口一般是不公开的。其次，移动通信网络也具有封闭性和复杂性特征。这些特性将对木马的生存和传播起到极大的遏制作用，要制作一个有生命力且具有广泛传播特性的手机木马，难度相当大，甚至是不可能的。

(3) 网络钓鱼。网络钓鱼是指作案者通过各种途径诱使客户访问虚假网站、虚假网址并主动输入敏感信息的信息窃取方式。在互联网上，每天都有成千上万的虚假网站诞生，也有成千上万的虚假网站关闭，网络钓鱼主要还是利用了一些客户容易上当受骗的心理弱点。

由于移动通信网络的封闭性，通过手机进行网络钓鱼的风险大大降低，但还是会存在。预防虚假网站主要还是要靠客户主动识别，不轻易相信他人，不访问来历不明的网址。如果客户能做到这些，就能远离网络钓鱼的风险。

(4) 手机被他人操作。招商银行手机银行在登录时要提供登录名、网银密码，如图 3.16 所示。即使手机被他人操作，不知道密码也将无法登录。

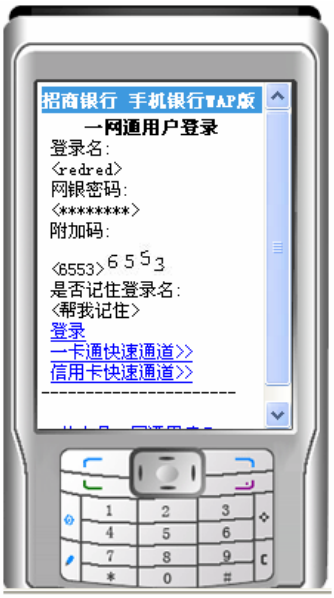

图 3.16　招行手机银行一网通用户登录

一方面，当用户退出手机银行或关闭手机浏览器后，手机内存中临时存储的账户、密码等信息将自动清除，不会在手机上保存。另一方面，如果用户打开手机银行，超过一定的时间未操作，银行后台系统将自动注销登录。因此，客户不用担心手机丢失或手机被他人操作会造成手机银行信息泄漏的风险。

3) 招商银行手机银行其他安全措施

除上述两方面的安全措施外，招商银行为手机银行还采取了以下安全措施。

(1) 网银密码、账户密码双重保护。招商银行手机银行全面支持一网通用户登录，在登录时会验证网银登录密码，在转账等交易时会验证取款密码或其他账户密码。这样，招商银行手机银行在账户密码之外又多了一层网银密码的安全屏障，客户账户更安全。

(2) 图形验证码机制，防止程序自动试探密码。在登录手机银行时，要求用户输入图形验证码，可以有效防止程序自动试探密码的风险。

(3) 密码错误次数过多自动锁定账户。对登录、转账等涉及密码输入的功能操作，如果密码输入连续错误次数过多，系统会在当天自动锁定账户。

(4) 账户号码保护机制。招商银行手机银行对用户关联的账户号码采取了特别的保护机制，账户号码以部分屏蔽的方式显示，真实的账户号码不在网络上传输，也不会发送到客户手机，有效地保障了客户账户号码的安全。

3.3.2 招商银行手机银行使用流程

招商银行手机银行使用非常简便，使用流程如图 3.17 所示。

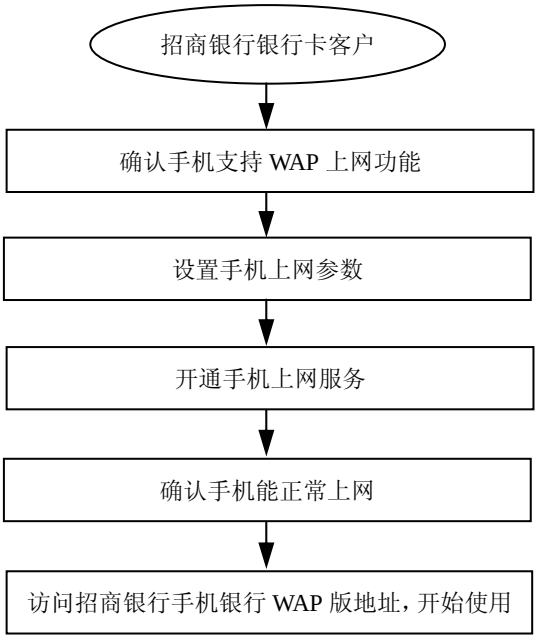

图 3.17 招商银行手机银行使用流程

1. 客户设置手机以支持 WAP 上网

1) 确认手机支持 WAP 上网功能

可以通过以下方式来确认手机是否支持手机上网功能。

(1) 查看手机上是否有浏览器的相应菜单选项。

(2) 查阅购机时附带的产品说明书。

(3) 访问手机生产商官方网站，查询手机规格说明。

2) 设置手机上网参数

一般手机在出厂时均已设置好上网参数，不需要再自行设置。如果手机没有默认设定上网连接参数，需要为手机浏览器新建一个连接并设定连接参数。GPRS 上网参数应按以下方式设置。

(1) 主页：招商银行(http://www.cmbchina.com)。

(2) 网关(代理服务器)地址：10.0.0.172。

(3) 网关(代理服务器)端口号：80 或 9201 或 9202 或 9203(各手机型号可能不同，要选择不同的支持安全连接的端口号)。

(4) 用户名和密码为空。

3) 开通手机上网服务

一般情况下，客户不需要主动申请手机上网服务，移动运营商会自动开通。如果客户设置了上网参数仍无法上网，或者需要更改计费类型，可以直接与运营商联系。

4) 确认手机能正常上网

可以选择手机浏览器的主页菜单，或直接输入运营商门户网站地址(参见 2)的主页项目)，如果能正常显示网页，说明手机已能正常上网。如果不能上网，可以直接与运营商联系。

如果手机可以上网，却无法访问招商银行手机银行，则有可能是手机不支持 WTLS 安全协议，也有可能是设置的上网参数不正确，可以尝试将网关(代理服务器)端口号改为 80 或 9201 或 9202 或 9203。

如果在登录页面看不到验证码图片，则可能是手机浏览器选项中禁止了图片显示。

2. 开始使用

招商银行手机银行 WAP 版的访问地址为 http://mobile.cmbchina.com，可以通过以下方式开始使用。

(1) 在招商银行网站上选择发送地址短信，则招行服务器会发送地址短信到客户手机，客户收到短信后提取其中的 URL 地址并访问。

(2) 在手机浏览器上手动输入上述地址并访问。

为了以后使用方便，可以在手机上将该地址加为书签。

本 章 小 结

随着信息技术的发展，移动支付将越来越受到人们的关注和青睐，其应用也将越来越广泛。

移动支付是通过移动设备转移货币价值以清偿债权债务关系的一种支付方式，其作为一种服务产品，并不完全是一种新的支付方式，对手机银行支付来说，仍沿用原有支付账户进行支付，移动通信设备仅是一种新的支付载体。移动支付包括广义和狭义两种概念。与移动支付密切相关的两个概念是手机银行和手机钱包。根据不同的分

类标准，移动支付具有不同的分类，其中，按照传输方式将移动支付分为远距离支付和近距离支付是比较常用的一种分类方式。

移动支付属于典型的技术驱动型业务，这类业务成功的基础是建立一个基本成型的价值链和合理的商业运营模式。移动支付的价值链主要由金融机构、电信运营商、商家、消费者、移动设备提供商、移动支付服务提供商等多个环节构成。移动支付商业运营的主要模式有 4 种：以金融机构为主导的运营模式、以移动运营商为主导的运营模式、以第三方支付服务商为主导的运营模式、银行与移动运营商合作的运营模式。

远距离移动支付的接入方式主要包括基于短消息（SMS）方式、基于语音（IVR）方式、基于 USSD 方式、基于 WAP 协议方式、基于 K-Java 方式；近距离移动支付的接入方式主要包括红外线、蓝牙、射频识别技术。我国移动支付目前应用的主要是远距离移动支付技术，对每种远距离移动支付技术都有特定的支付流程。

移动支付中面临的安全威胁主要包括无线链路威胁、服务网络威胁和终端威胁，解决这些问题需要达到秘密性、完整性、抗否认性、可认证性和可用性安全目标。为此，管理上一般采用限额控制和签约机制；技术上一般采用访问控制技术使支付中交易信息不被非法用户获得和篡改，采用身份认证技术实现对交易各方的身份认证，采数字签名技术实现信息的保密等。WPKI 和椭圆数字签名技术是适合移动支付特性的安全技术。

目前，工农中建四大国有银行和很多股份制银行都开通了以手机银行为代表的移动支付功能。招商银行的手机银行 WAP 版是一个典型的移动支付例子。

关键术语

移动支付；手机银行；SMS；WAP；身份认证；数字证书

习　　题

一、选择题

1．移动支付中使用的移动设备不包括(　　)。

A．手机　　B．固定电话和小灵通

C．移动 PC　　D．PDA

2．与网上银行支付相比，移动支付主要面向(　　)。

A．企业用户的大额支付　　B．企业用户的小额支付

C．个人用户的各类支付　　D．个人用户的小额支付

3．以下(　　)不属于移动支付远距离支付技术。

A．基于短消息(SMS)方式　　B．基于 WAP 方式的支付

C．基于 K-Java 方式的支付　　D．蓝牙

4．下列(　　)不属于移动支付商业运营的主要模式。

A．以金融机构为主导的运营模式

B．以移动运营商为主导的运营模式
C．银行与移动运营商合作的运营模式
D．以移动设备提供商为主导的运营模式

5．在移动支付中，下述(　　)不是安全问题主要存在的方面。
A．无线链路　　B．服务网络　　C．金融机构　　D．终端

二、简答题

1．简述移动支付、移动银行的概念。
2．简述移动支付的分类。
3．简述远距离移动支付的接入方式及其相应的支付流程。
4．移动支付面临哪些主要安全问题？
5．移动支付有哪些安全需求？
6．简要列举移动支付安全策略。
7．什么是 WPKI 技术？
8．结合自己手机银行支付的经历，谈谈所用的手机银行具有哪些功能，采取了哪些安全技术。

三、讨论题

登录中国工商银行网站(http://www.icbc.com.cn)，了解其手机银行的功能、安全措施，与招商银行手机银行进行对比。

案例分析

手机支付存在安全漏洞有巨大欺诈风险[①]

全球调查结果显示，利用手机和短距离无线传输技术付款的“非接触式”移动支付服务将在今后几年内迅速发展。但美国专家 2008 年 5 月 19 日警告，这种方式迄今存在严重安全漏洞，带来巨大欺诈风险，甚至可能是欺诈者今后“最大的犯罪机会”。

所谓“非接触式”移动支付，是指通过手机和读卡器等设备间的无线数据传输完成支付交易，这使手机具有银行卡的功能。

手机支付以简单易行、避免现金交易等优点获得不少人青睐。全球各大手机运营商已开始开发这一业务的商机，旅行社、零售商和银行等也推出手机支付服务。英国市场调研机构“朱尼珀研究”的一项最新调查结果显示，手机将日益成为现金、信用卡和借记卡的替代物。至 2011 年，预计全球 5200 万消费者将采用移动技术为日常消费品和服务付费。今后 3 年的手机支付总额预计为 118 亿美元。

2009 年，中国 3 大电信运营商纷纷推出内置 NFC(非接触式通信)芯片的 3G 手机，标志着我国移动支付进入以非接触式移动支付为主要特征的第三代移动支付阶段。

手机支付业务发展潜力很大，但美国软件安全技术专家格雷格·戴伊提醒说，这种方式存在巨大的数据安全漏洞。他认为，人们不久便能用手机做任何事，用手机短信交停车罚单，甚至用手机从事在线银行交易，一些狡猾的数据偷窃罪犯将出现在这一不接触式交易舞台；尽管手机付费目前大多仅限小额交易，

① http://article.pchome.net/content-627648.html。

但欺诈者可能会采取“细水长流”的策略。如果他们从每个手机用户那里拿走 5 美元，累计下来就能获得一大笔钱。

戴伊认为，手机支付方式主要安全漏洞之一在于大部分手机没有安全软件的保护，同时绝大部分消费者安全意识不足。迈克菲公司等机构联合开展的一项调查结果显示，至少 79％的消费者明知手机上的信息处于毫无保护状态，但仍然使用手机交易，15％的人不清楚手机安全保护程度。这项调查涉及英国、美国和日本的 2 000 名手机用户。

戴伊说：“无线空间是今后欺诈者最大的机会，主要原因之一在于许多人仍然只把电话看做通信设备，而不是他们必须要加以信息安全保护的设备。”

问题：目前，我国正处于采用非接触式移动支付的开始阶段，社会各界对新一代移动支付的前景非常看好，对这种一动支付方式，你是否同意戴伊的观点？目前应该从哪些方面来预防和降低潜在的欺诈风险？