移动商务支付网关的设计与实现

摘要

论文的目标是设计与实现一个移动商务支付网关，从而解决移动商务交易过程中的电子支付问题，为移动商务的快速健康发展提供了一个安全可靠的支付平台。

本文首先介绍了移动商务的概念及其分类，探讨基于 WAP 协议的移动互联网应用模型，提出了在目前网络条件下切实可行的移动商务解决方案。其次，论文对支付理论及其相关密码学技术做了全面介绍，自主设计了简洁的电子支付协议，并且利用 Kailer 逻辑对其安全性予以证明。最后，论文对支付网关设计与实现过程中的关键部分做了详细的阐述。

关键字：移动商务 支付 协议 网关

Design and Implementation of Mobile-Commerce Payment Gateway

Abstract

The thesis is devoted to design and implement an m-commerce payment gateway to solve the problem of electronic payment in the process of m-commerce transaction and provide a secure payment platform for m-commerce. It contains the architecture, algorithms and protocols of the gateway as followed.

Firstly, in chapter 1 the thesis makes an introduction and classification of m-commerce in mass. On the base of WAP application model, an m-commerce solution scheme for current mobile network is brought forward in chapter 2. Secondly, the thesis makes a complete introduction of electronic payment theory and related cryptography technology in chapter 3. In chapter 4 a simple but secure electronic payment protocol designed by myself is described in details. In the end, the description of key part of design and implementition of payment gateway is presented in chapter 5 and chapter 6. In chapter 7, the prospect of WAP application and m-commerce is discussed.

Key Word: m-commerce payment protocol gateway

第一章 引言

本章首先对移动商务的概念作了简单定义，并且根据移动商务行为发生环境(Environment)的差异对其进行分类，确定了论文中所探讨的支付网关系统所处的移动商务环境类型与范围，最后简要描述了整篇论文的组织结构。

1.1 背景介绍

1.1.1 移动商务

20世纪90年代以来，有两种技术得到了广泛应用，它们直接影响了全世界亿万人的生活，大大地改变了人类的生活方式，这就是互联网和移动通信。随着互联网络与移动电话这两种技术的日益成熟及其应用的飞速发展，使用具有移动数据业务功能的手机上网逐步进入了人们的日常生活。手机用户在任何时间、任何地点都可以进入范围广泛的互联网服务领域，轻松点击手中的移动电话就能成功获取信息、互相交流、实施电子商务等事务。

移动商务是移动化、电子化的网络商务活动。移动化是指商务行为不受时间和空间的约束；电子化包括数据、资料、资金的电子化；网络化包括信息传递和资金流通的网络化，比如网上购物、网上订票、网上交费等。

1.1.2 移动商务交易环境

MeT根据移动商务交易发生的环境将移动商务交易划分为三类:远程商务环境（Remote Environment）、本地商务环境（Local environment）、个人商务环境（Personal Environment）。本节将向读者简要介绍这三种移动商务交易环境。

1.1.2.1 远程商务环境（Remote Environment）

在远程环境中，移动终端（PTD）和内容服务器通过公共陆地移动通信网（PLMN,比如GSM等）建立连接。使用WAP终端通过移动运营商的WAP网关接入到英特网，WAP网关作为代理服务器将WAP协议转换为英特网协议。内容提供商的服务器也可以拥有自己的WAP网关而非移动运营商的公共WAP网关。

在两种网关配置方案中，传输层安全如何实现有一些细微的差别。当很多

内容服务器同时使用一个公共 WAP 网关时，在 PTD 和 WAP 网关之间使用 WTLS 协议，而在 WAP 网关和内容服务器之间使用 TLS/SSL，因此传输层安全在 WAP 网关中存在有断点，无法保证 PTD 和内容服务器之间的端到端安全；第二种情况中，由于每个内容服务器都有属于自己的 WAP 网关，所以在 PTD 和 WAP 网关之间能够保证端到端安全。

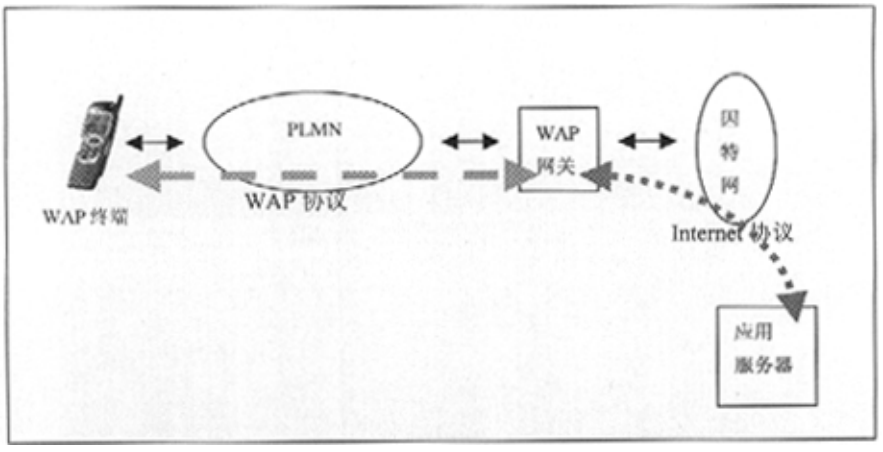

图 1-1 远程商务环境

1.1.2.2 本地商务环境（Local Environment）

在本地环境中，用户使用移动终端（PTD）通过短距离的无线技术（蓝牙等）接入到局域网发起移动商务交易，交易数据依次通过局域网、因特网，最后发送到应用服务器。在移动终端中实现 BlueTooth 承载的 WAP 协议栈，用户就能够通过 WTLS 提供服务器认证和建立安全会话，从而保障交易的安全性。

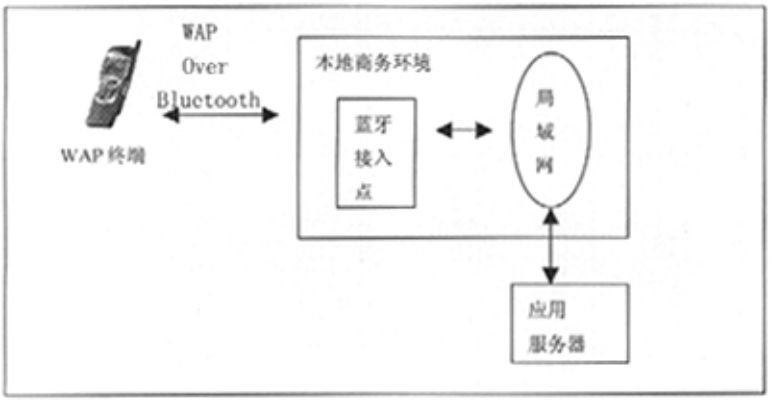

图 1-2　本地商务环境

1.1.2.3 个人商务环境（Personal Environment）

个人商务环境情况下，用户在申请业务证书和对交易数据进行签名操作等需要个人化信息的过程中使用移动终端(PTD)。移动终端仅仅被作为对交易数据签名和对用户身份认证的工具，而使用其它通信设备（比如 PC 机）进行移动商务交易数据的传输和处理。使用这样的解决方案，支付者无需在那些公共的通信设备（比如公共场合中的 PC 机）上保留个人化信息（签名密钥等），从而提高了移动商务交易的安全性。

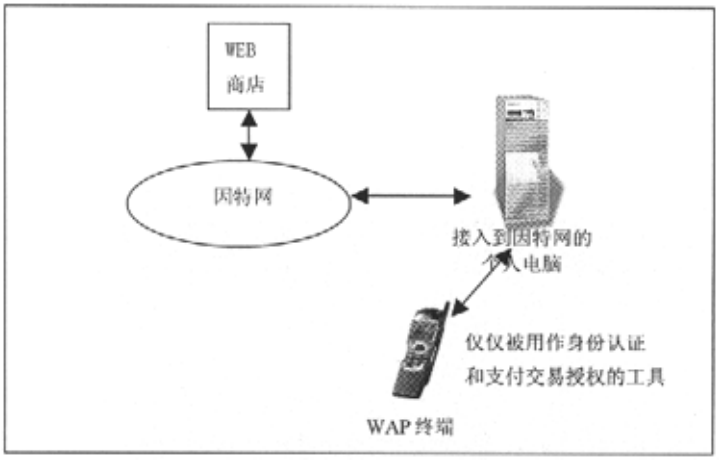

图 1-3　个人商务环境

1.1.3 移动商务体系结构

一个完整的电子商务系统安全体系结构包括 4 层：网络基础设施、电子商务安全基础设施（PKI、CA）、安全电子支付网关系统和电子商务应用系统。网络层基础设施完成信息的传送；电子商务安全基础平台主要是以 PKCS#7，X.509 证书和 LDAP 为基础，提供 CA 证书发放、认证功能；安全支付网关作为支撑层提供对各种业务应用系统的安全在线支付功能；最后实现了不同业务逻辑的各种业务应用系统。

移动电子商务支付网关是电子商务系统的重要组成部分，它是指支付者、商家和金融机构之间使用电子手段交换商品或者服务，即把新型支付手段（包括电子现金（E-CASH）、信用卡（CREDIT CARD）、借记卡（DEBIT CARD）、智能卡等）的支付信息通过网络安全传送到银行或相应的处理机构，来实现电子支付

的过程。

1.2 目标与范围

WAP1.0 规范成为移动互联网业界标准后，WAP 应用的开发和部署成为人们关注的热点。然而，由于 WAP1.0 版本对数据安全性的支持不够以及使用电话拨号接入方式对数据传输速率的限制，造成了 WAP 应用类型单一，仅仅表现为提供简单信息 WAP 网站，因此 WAP 应用的研究与开发走入了低谷。

WAP2.0 规范极大完善了对数据安全性的支持，同时越来越多移动终端厂商开始推出 WAP2.0 规范兼容手机；GPRS 业务的开通使得 GSM 网上的无线数据传输速率超过 110Kpbs。这些变化使得移动商务应用数据在无线互联网传输中的可靠性和安全性都大大提高，这就解决了移动商务应用的最基本的问题——信息安全传输。

因此，当前移动商务长足发展的关键在于能否提供一个多功能、多渠道的移动商务交易安全认证平台，在对支付者、商家和金融机构的多方认证基础上，实现安全电子支付行为。电子商务在线支付在国外成熟的金融法律制度下已经得到了一定的发展，国外主流移动设备商已经提出许多先进的移动商务解决方案，而我国是市场经济不大发达的发展中国家，金融法律还有待完善，信用卡制度还有待发展，所以如何建设符合中国国情的移动商务支付支撑系统是一个值得探讨的问题。

本文通过深入分析远程商务环境下(Remote Environment)的移动电子商务应用模式，并根据我国移动通信发展现状，设计与实现了一个移动电子商务支付网关系统。

1.3 论文组织结构

论文主体由七部分组成。第一章《引言》主要阐述了移动商务的基本概念，论文的目的与组织结构；第二章《WAP 基本概念与应用模型》是 WAP 协议的体系结构和 WAP 编程模型的概览；支付网关相关技术与理论在第三章《电子支付相关理论的分析和研究》中深入讨论。第四章《支付网关系统关键技术的研究和实现策略》中所介绍的简单电子支付协议是整个支付网关系统的理论基础。第五章《支付网关总体设计》涉及支付网关系统设计过程中的几个不同阶段，介绍了支付网关的功能要求、需求分析和软件体系结构等方面的内容。第六章《支付

网关系统实现》介绍了开发过程中采用的软件、硬件平台，系统的设计规范和实现过程中涉及的关键算法与相关通信规范等内容。第七章《结束语》探讨了基于WAP 构架的移动电子商务的发展前景，总结了支付网关系统需要进一步改进的地方。

第二章 WAP 基本概念与应用模型

本章简要介绍了 WAP 协议的体系结构和 WAP 应用模型，从而使读者易于理解 WAP 环境中移动商务支付网关的设计与实现思路。

2.1 WAP 基本概念

WAP（无线应用协议）是无线终端和互联网之间进行通信时使用的开放性全球标准。它由一系列协议组成，用来标准化无线通信设备，定义用户访问内容的组织格式，以及通信使用的协议等。利用 WAP 技术，无论你在何地、何时，只要需要信息，你就可以打开你的 WAP 手机，享受丰富多彩的网上信息或者网上资源，如：新闻、天气预报、股市行情、经济动态、电子商务、网上银行等。

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等。这些设备相对于台式个人计算机而言，CPU 功能和电池容量有限，内存和显示屏较小，输入不便。WAP 也可以支持目前存在的各种移动网络，如 GSM、CDMA、PHS 等，并考虑了对未来第三代移动通信系统的支持。相对有线网络，无线网络的带宽、连接可靠性及网络的可预测性都相对较低，网络时延也比有线网络大。

考虑到以上的限制和不利因素，WAP 充分借鉴了 Internet 的思想，并加以一定的修改和简化。一个典型的 WAP 应用系统定义了三类实体：

- 具有 WAP 用户代理功能的移动终端(Client)。典型的终端为 WAP 手机，它相当于 Internet 中的 PC 机。在它的显示屏上运行有微浏览器(microbrowser)，用户可以采用简单的选择键实现 WAP 服务请求，并以无线方式发送和接收所需的信息。WAP 移动终端使用 WML 无线标记语言显示各种文字、图像或数据。

- WAP 网关。包括协议网关--实现 WAP 协议栈(WSP、WTP、WTLS 和 WDP)与 Internet 协议栈之间的转换；信息内容编解码器(Content Encoders and Decoders)--把 WAP 数据压缩编码，以减少网络数据流量，最大限度地利用无线网络缓慢的数据传输速率。

• Web 服务器。服务器中存有用 WML 或 WMLScript 编写的 WAP 内容和应用。

2.2 WAP 协议体系结构

WAP 是一个世界性的组织 WAP Forum 长期努力的产物，其目的是要成为无线数据应用的业界标准，目前的最新版本是 1.2 版，而更新的版本已完稿正提交讨论中。WAP 是一个分层的协议簇，在设计时参考了 HTTP、TCP/IP 等协议，并努力适合于在窄带、时延长的传输环境中运行。

图 2-1 是 WAP 协议体系结构及其与 Internet/WEB 的对应关系。各协议层的具体介绍不在本文范围内。但要指出：WAP 与下层数据传输的机制是无关的；WTLS（Wireless Transport Layer Security）是一个可选的协议层。

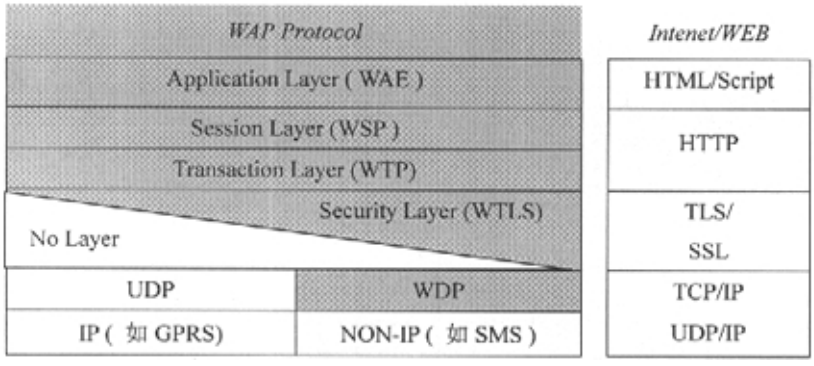

图 2-1 WAP 体系结构及与 WEB 应用的比较

2.3 WEB 和 WAP 应用模型的比较

WAP 编程模型和 WWW 编程模型非常相似。对熟悉 WWW 编程模型的人来说，理解 WAP 基本原理是一件很容易的事。

在 WWW 编程模型中，用户发起一个页面请求，请求参数中包括所请求页面的 URL。Web 浏览器将解析这个 URL 并向 Web 服务器发送一个 HTTP 或 HTTPS GET 请求。Web 服务器接收到该请求后对其进行解析，如果请求是合法的，服务器将把 URL 指定的静态页面的内容或 CGI 程序的输出作为 HTTP 的响应返回给 Web 浏览器。响应的内容部分是用 Web 浏览器可识别的 HTML 语言书写的。浏览器收到响应后将其内容显示在用户界面上（通常为计算机屏幕）。

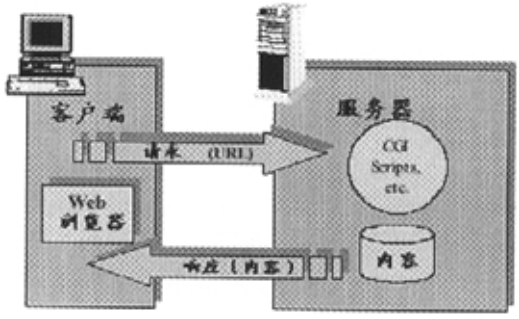

图 2-2 WEB 应用模型

WAP 应用模型（图 2-3）与 WEB 的应用模型类似，但还是有一些区别的：

在 WAP 用户终端和内容服务器之间必须有一个 WAP 网关，而 WWW 应用模型中网关或代理服务器的存在并不是必须的。WAP 网关的主要工作是将用户终端侧的 WAP 协议和内容服务器侧的 HTTP 协议互相转换，从而实现用户终端和内容服务器的通信。同时，WAP 网关在将来自内容服务器的 WML 和 WMLScript 文件送到用户终端之前，必须对它们进行编译，转换成传输效率更高的二进制格式，而 WWW 应用模型中消息以文本格式传送，传输效率低下。

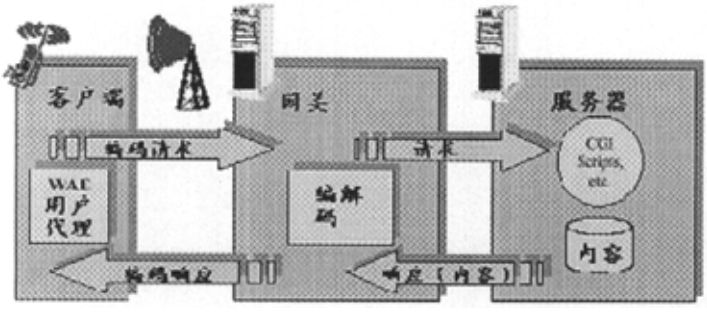

图 2-3 WAP 应用模型

为便于理解 WAP 应用模型，在此先澄清几个名词概念。图 2-3 在用户终端和内容服务器（web server 或 content server）之间也许还有一个或多个网关（gateway）或代理服务器（proxy）。网关为内容服务器充当中间层。网关最常见的应用是防火墙。用户终端通信时意识不到网关的存在，也就是说，网关

对用户终端来说是透明的。

和网关一样，代理服务器也是用户终端和服务器的中间层。但与网关不同的是，代理服务器需要代表客户端向服务器发送请求。因此，代理服务器通常必须既能发送请求又能应答请求。代理服务器一般都具有缓存功能，可以缓存来自内容服务器的响应消息，用户若在消息的有效时限内再次对其发出请求，代理服务器将直接从缓存中调出该消息，而不是再向内容服务器发出请求，这样就降低了响应时间。客户端必须知道其代理服务器的地址，也就是说，代理服务器对用户终端来说是不透明的。

2.4 WAP 应用模型分析

下面我用一个简单的例子来说明 WAP 编程模型的处理过程：

用户发出 URL 请求，用户终端对此 URL 解析后产生一个 GET 请求；用户终端先将请求转换成二进制的格式，再通过无线网络将 GET 请求发送到 WAP 网关；WAP 网关接收到请求消息后，将该信息转换成基于文本的 HTTP 的 GET 请求，然后转给 URL 所指的服务器。URL 所指的服务器将接收请求，处理并发回响应；相应地，WAP 网关接收来自内容服务器的响应，并将响应转换成简化的二进制格式，然后通过无线网络将其发送到用户终端，用户终端接收到响应后，分析信息体，并在用户 WAP 终端上显示。

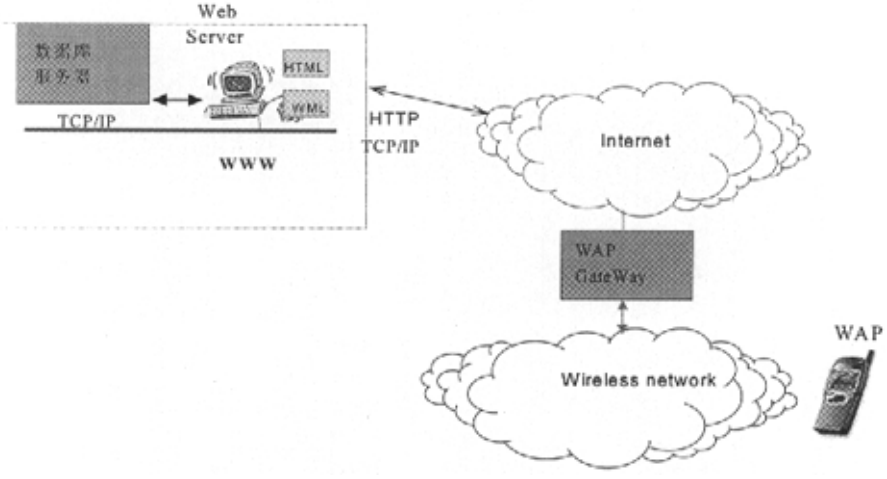

图 2-4　WAP 应用体系结构

因为 WAP 论坛尽可能地使用现成的标准，所以 WAP 和 WEB 编程模型是十分类似的，这给开发者带来了非常明显的好处：可以使用现有的 WEB 知识来创建 WAP 应用。许多现有的 Web 软件开发工具都可用于 WAP 应用的开发。例如，现有的 CGI 工具、ASP 和 PHP 工具不必做任何改动就可以直接用于 WAP 应用的开发。如果已经有基于 WEB 的应用，可以保留现有数据库、内容、应用逻辑和应用编程接口，从而节省开发投资和开发周期。

2.5 WAP 应用安全方案

2.5.1 WTLS 和 SSL 的区别

WTLS 是 WAP 协议栈中的一个可选层，具体应用时可根据业务安全性要求及承载网络特性决定是否选择该层功能。WTLS 的功能类似于 WWW 中的 TLS 1.0，可为高层提供数据完整性校验、加密解密、身份鉴别和其他安全保护功能。但他们之间还是有一些差别的，如：

- WTLS 在一般 UDP 这类不可靠信道之上工作，因此每个消息里要有序列号，协议里也要靠它来处理丢包，重复等情况。拒绝服务攻击也因此变得更加容易。
- WTLS 建立的安全连接是在 WAP 网关和手持设备之间，WAP 网关和 Web server 之间如果也要保密，需要再采用 SSL，加密的信息在 WAP 网关中会恢复成明文，即在这种模型中无法实现端到端的加密。
- WTLS 协议里增加了一种 key_refresh 的机制，当传递了一定数量数据包后，双方通过同样的算法将自己的密钥做一下更新。付出了很小的代价，安全性得以增强。
- 根据需求，WTLS 的实现应提供 3 类不同级别的安全服务。请求的服务类是可根据参数配置的，也可以通过程序设置。由于只有当 WAP 手机能够存储数字证书时，WTLS 才能支持第三类的安全，所以本支付网关系统需要 WAP2.0 兼容手机、WIM 卡和实现了 WTLS 第三类安全功能的 WAP 网关的支持。

2.5.2 WTLS 端到端的安全

WAP 通信是靠 WAP 协议栈中的 WTLS 安全层进行身份认证和数据加密从而解决通信安全问题，而 WAP 协议通信从手机出发到 WAP 网关就结束了，所以安全的通信到 WAP 网关也就结束了，因此不是真正端到端的安全。即使从 WAP 网关到内容提供商再用 SSL 加密，通信数据在 WAP 网关处也变成了明文。对安全性有很高要求的内容/应用提供商，如银行，如果采用这种部署结构，则需建

立对移动运营商（即 WAP 网关）的信任，对于象 WAP 手机银行这样需要绝对保证安全性的业务，这种结构的安全漏洞显然是不能接受的。为了解决这个问题，实现端到端的可靠性，有如下解决方案（以手机银行业务为例）：

2.5.2.1 第一代解决方案

在 WAP 协议发展还不完善，不能从协议上解决问题时，只能从系统部署上想办法。为了使 WAP 协议运行到银行的系统范围内，可在银行系统内部部署 WAP 网关，用户将手机中的网关 IP 地址设置为银行网关 IP 地址即可使 WAP 协议运行到银行；另外，银行也可根据自身情况考虑部署拨号接入服务器 RAS。该方案在某些地方已有部署。

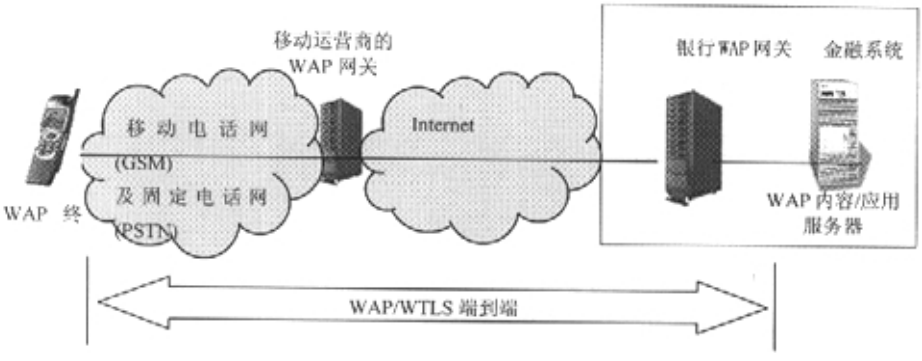

图 2-5 WTLS 安全解决方案一

第一代方案的优点：

- 在 WAP 协议本身发展未完善时通过系统部署实现端到端的安全性。
- 银行独立于移动运营商即可开展 WAP 手机银行业务。

第一代方案的缺点：

- 对 WAP 协议的发展没有考虑和准备。
- 对用户要求较高，用户需对手机进行复杂设置和切换，会极大降低用户对该业务的接受程度。
- 不符合现有的广泛部署的 WAP 部署模型。

由上可见，第一代方案是在 WAP 协议发展初期为解决安全问题提出的方案，没有充分考虑 WAP 协议的进展，对用户使用亦不方便。现实情况是：几乎每个用户手机都设置了移动运营商的网关地址（甚至有的手机出厂时就已设置好移动运营商的网关），用户对一般站点的浏览也都是使用该设置。但 WAP 手机银行

为保证端到端安全性又必须设置银行的 WAP 网关地址，得到安全性却损失了方便性。如果每次访问银行站点都要用户改变设置，肯定会使用户不胜其烦，极大地挫伤其使用 WAP 手机银行业务的积极性，于业务推广很不利。在此，安全性和方便性形成了一对矛盾。

2.5.2.2 第二代解决方案

WAP 规范的最新发展（主要是端到端安全传输协议和无线代理协议的成熟）为手机银行等既要求安全性又方便性的应用提供了最新解决方案。该方案可以在不改变现有 WAP 系统部署结构、不要求用户设置银行的网关 IP 地址的情况下支持端到端安全性。其原理是：银行部署支持 WAP 代理协议 WPP 的“企业代理服务器”即 EP ，用户仍用移动运营商的网关设置访问任何站点，包括银行站点。但在访问银行敏感信息时（图中①②），银行站点返回一个要求手机临时改变设置的信息，使手机临时自动将网关设置为银行网关（图中③④），实现端到端安全性（图中⑤），过后访问其它站点时手机将恢复原设置，这些过程都不需用户的直接参与，自动完成。

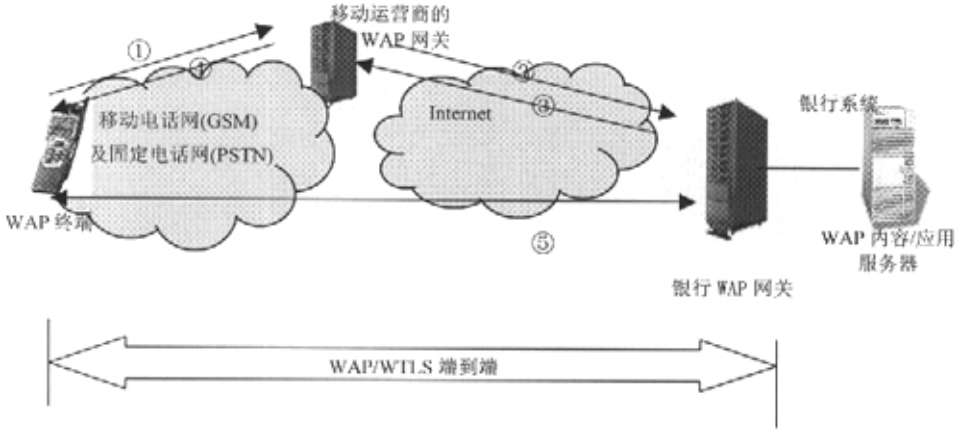

图 2-6 WTLS 安全解决方案二

第二代方案的优点：

- 利用 WAP 协议本身的发展完善解决端到端的安全性。
- 用户操作非常方便，不必对银行站点作特别设置，为了安全目的进行的临时设置转换在用户不参与的情况下自动完成，同时满足了安全性和方便性这一对通常是矛盾的要求。

- 符合现有的广泛部署的 WAP 系统模型。

第二代方案的缺点：

- 手机、移动运营商网关和银行网关都需支持端到端安全的无线代理协议，系统才能按此模式运行，因此协调面较大，完全部署还需时日。

由上可见，第二代方案能同时满足安全性和方便性的要求，唯一问题是要多方配合才能投入实际运行，事实上 Phone.com 提出的无线代理协议始终没有得到其它厂商的认同，使得第二代方案无法得到推广。

第三章 电子商务支付理论的分析

本章所阐述的内容是整篇论文的理论基础。在信息安全方面，主要介绍了公钥和私钥密码学技术、密码学协议，以及公开密钥基础设施；在支付理论方面，主要介绍了电子支付方式、电子支付协议，支付手段；最后介绍了两个国外移动设备厂商提出的移动商务系统的整体解决方案。

3.1 无线公开密钥基础设施(WPKI)

WAP PKI 是 WAP 论坛与 Met 共同制定的规范，它重用了现有的 PKI 标准，根据 WAP 环境的特定需求，增加了 WAP PKI 的定义以及 WAP 证书等一系列新的规范。

3.1.1 密码学基础

按作用不同分类，数据加密技术主要分为数据传输、数据存储、数据完整性的鉴别等，以下分别对几种常用的密码学技术做简单的介绍。

3.1.1.1 常规密钥密码体制

所谓常规密钥密码体制，即加密密钥与解密密钥是相同的。在早期的常规密钥密码体制中，典型的有替代密码，其原理可以用一个例子来说明：将字母 a，b，c，d，…，w，x，y，z 的自然顺序保持不变，但使之与 D，E，F，G，…，Z，A，B，C 分别对应(即相差 3 个字符)。若明文为 student 则对应的密文为 VWXGHQW（此时密钥为 3）。由于英文字母中各字母出现的频度早已有人进行过统计，所以根据字母频度表可以很容易对这种代替密码进行破译。

作为对称密钥密码体制的代表，DES 算法原是 IBM 公司为保护产品的机密于 1971 年至 1972 年研制成功的，后被美国国家标准局和国家安全局选为数据加密标准，并于 1977 年颁布使用。ISO 也已将 DES 作为数据加密标准。DES 对 64 位二进制数据加密，产生 64 位密文数据。使用的密钥为 64 位，实际密钥长度为 56 位（有 8 位用于奇偶校验）。解密时的过程和加密时相似，但密钥的顺序正好相反。DES 的保密性仅取决于对密钥的保密而算法是公开的，DES 内部复杂的结构是至今没有找到破译捷径的根本原因。

3.1.1.2 公开密钥密码学体制

在网络应用中一般采取两种加密形式：对称密钥和公开密钥体制，采用何种加密算法则要结合具体应用环境和系统，而不能简单地根据其加密强度来作出判断。因为除了加密算法本身之外，密钥合理分配、加密效率与现有系统的结合性，以及投入产出分析都应在实际环境中具体考虑。

公开密钥（public key）密码体制出现于 1976 年。它最主要的特点就是加密和解密使用不同的密钥，每个用户保存着一对密钥 ？公开密钥 PK 和秘密密钥 SK，因此，这种体制又称为双钥或非对称密钥密码体制。在这种体制中，PK 是公开信息，用作加密密钥，而 SK 需要由用户自己保密，用作解密密钥。加密算法 E 和解密算法 D 也都是公开的。虽然 SK 与 PK 是成对出现，但却无法根据 PK 计算出 SK。

公开密钥算法的特点如下：

- 用加密密钥 PK 对明文 X 加密后，再用解密密钥 SK 解密，即可恢复出明文，

  或写为：$D_{SK}(E_{PK}(X))=X$

- 加密密钥不能用来解密，即 $D_{PK}(E_{PK}(X))\neq X$

- 在计算机上可以容易地产生成对的 PK 和 SK。

- 从已知的 PK 实际上不可能推导出 SK。

- 加密和解密的运算可以对调，即：$E_{PK}(D_{SK}(X))=X$ 在公　开密钥密码体制中，最有名的一种是 RSA 体制。它已被 ISO/TC97 的数据加密技术分委员会 SC20 推荐为公开密钥数据加密标准。

3.1.1.3 数字签名技术

数字签名技术是实现交易安全的核心技术之一，它的实现基础就是加密技术。在这里对数字签名的基本原理做一个简要介绍。

以往的书信或文件是根据亲笔签名或印章来证明其真实性的。但在计算机网络中传送的报文又如何盖章呢？这就是数字签名所要解决的问题。数字签名必须保证以下几点：接收者能够核实发送者对报文的签名；发送者事后不能抵赖对报

文的签名；接收者不能伪造对报文的签名。

现在已有多种实现各种数字签名的方法，但采用公开密钥算法要比常规算法更容易实现。下面就来介绍这种数字签名技术：

发送者 A 用其秘密解密密钥 SK_A 对报文 X 进行运算，将结果 D_{SKA}（X）传送给接收者 B。B 用已知的 A 的公开加密密钥得出 E_{PKA}（D_{SKA}（X））=X。因为除 A 外没有别人能具有 A 的解密密钥 SK_A，所以除 A 外没有别人能产生密文 DSK_A（X）。这样，报文 X 就被签名了。假若 A 要抵赖曾发送报文给 B。B 可将 X 及 D_{SKA}（X）出示给第三者。第三者很容易用 PK_A 去证实 A 确实发送消息 X 给 B。反之，如果是 B 将 X 伪造成 X'，则 B 不能在第三者面前出示 D_{SKA}（X'）。这样就证明 B 伪造了报文。

可以看出，实现数字签名也同时实现了对报文来源的鉴别。但是上述过程只是对报文进行了签名。对传送的报文 X 本身却未保密。

3.1.1.4 数字证书

数字证书就是一份文档，它记录了用户的公开密钥和其他身份信息。WAP 证书采用最流行的 X.509 V3 系列证书，为适应无线环境，作了一些规定，使证书更简洁化。比如，在客户（移动设备）证书中的 Subject 域中通常只包含一个序列号。但证书使公钥与身份信息绑定的功能没有改变。

WAP 证书的数字签名方式采用 SHA_1 加 RSA 或 SHA_1 加椭圆曲线（ECC）DSA 的方式。后者是比较适合 WAP 的，因为它可以使证书和数字签名较小。WAP 证书的编码采用 X.690 系列定义的 DER（Distinguished Encoding Rules）编码。事实上，这种编码不是一种短长度的编码，比如一个 0 到 128 的整数，需要用三个字节进行编码，但它有一个好处是编码结果是唯一的，适合于数字签名环境。虽然，我们可以期望有一种更短长度的编码来代替 DER，但目前还没有看到这方面的进展。

3.1.2 X.509 与公开密钥基础设施

PKI 是一种遵循标准的密钥管理平台，它能够为所有网络应用透明地提供

采用加密和数字签名等密码服务所必需的密钥和证书管理。PKI 具有认证 机关(CA)、证书库、密钥备份及恢复系统、证书作废处理系统、客户端证书处理系统等基本成分。

ITU-T 的 X.509 建议书是对目录服务进行定义的 X.500 系列推荐书的一部分。X.509 是一个重要的标准，在 X.509 中定义的证书结构和鉴别协议已有广泛的应用。X.509 定义了一个由 X.509 目录向它的用户提供的鉴别服务框架。目录提供证书检索服务，每个证书中包含用户的公开密钥和 CA 私有密钥的对证书内容签名。X.509 同样定义了基于使用公开密钥证书的可选鉴别协议。

作为目前应用广泛的公开密钥基础设施（PKI）中的重要组成部分，X.509 也是 WAP PKI 的基础，当前其最新版本是 X.509V3。

3.1.3 智能卡与 WIM

智能卡（Smart Card）是集成电路卡的一种，它由 CPU、ROM、RAM、EEPRAM 等组成，内部具有卡片操作系统（COS），构成一个微型的计算机系统。智能卡是存取密钥的最佳媒体，卡内存有授权用户口令和密码，采用可靠的RSA/DES/ECC 加、解密技术，所有加、解密操作均在卡内实现，所有秘密信息均不暴露在卡外。智能卡系统具有完美的密钥存取管理机制，包括卡内密钥、通信密钥和传输密钥，对密钥的生成、存放和下载进行全过程管理。最终用户将密钥存放在智能卡中，卡可内置于手机（PTD）中，这就可以有效地防止密钥丢失、被盗。

智能卡还可以存储数据，比如一些会话过程中需要经常访问的数据（包括私钥和共享秘密等），它们通常用于建立长时间的会话。从共享秘密中派生密钥是一种节省会话建立时间，提高网络响应速度的有效方式。

WIM 规范是 WAP 1.2 中新增加的内容，它的目的是将安全功能从手机转移到抗损害设备中，这种设备可以是智能卡或者 SIM 卡。由于智能卡具有自己的处理器，因此可以在智能卡的芯片中实现加解密算法和哈希功能。WIM 卡可以为特定的加解密算法设计专门的加解密芯片，因此与通过手机上的软件实现加解密的方案相比，WIM 方案的显著优点之一是能够提供较好的运算性能。

安全可靠地实现在线支付功能是实现网上银行、网上购物、电子商务的前提。智能卡技术支持网上各种支付方案，包括电子货币支付（即电子信用卡支付、电子现金支付、电子钱包支付），电子票据支付（即电子支票支付、电子汇票支

付）以及通过清算中心自动进行电子资金转帐等。

3.2 电子支付手段

电子商务建立在计算机网络基础上，无论是公共网络还是专用网络都必须让用户方便安全地使用。金融机构涉及到资金的保管和处理，因而也总是罪犯攻击威胁的对象。为此金融机构在安全方面需要解决如下这些问题：防止数据被窃听、专用数据的保护、用户认证、数据完整性检验、安全访问能力、系统可靠性等等。总之，移动商务中的安全问题可以归结为两大类：通信安全和交易安全问题。

支付是电子商务活动的核心。国际通行的网上支付工具和支付方式主要有银行卡支付、电子现金、电子支票以及电子资金转账、微支付等，这些方式都以解决交易安全问题为最终目的。

3.2.1 信用卡支付标准（SET）

SET 是一种应用于开放网络环境下，以信用卡为基础的安全电子支付系统的协议，它给出了一套电子交易的过程规范。通过 SET 这一套完备的安全电子交易协议可以实现电子商务交易中的加密、认证机制、密钥管理机制等，保证在开放网络上使用信用卡进行在线购物的安全。由于 SET 提供商家和收单银行的认证，确保了交易数据的安全、完整可靠和交易的不可抵赖性，特别是具有保护消费者信用卡号不暴露给商家等优点，因此它成为目前公认的信用卡/借记卡的网上交易的国际标准。

3.2.1.1 SET 协议的支付流程

SET 规定了电子商务支付系统各方购买和支付消息传送的流程。图 1 为 SET 协议结构流程图。可见，电子商务支付系统的交易三方为：持卡人、商家和支付网关。交易流程为：

- 持卡人决定购买，向商家发出购买请求；
- 商家返回同意支付等信息；
- 持卡人验证商家身份，将定购信息和支付信息安全传送给商家，但支付信息对商家来说是不可见的；
- 商家验证支付网关身份，把支付信息传给支付网关，要求验证持卡人的支付信息是否有效；
- 支付网关验证商家身份，通过传统的银行网络到发卡行验证持卡人的支付信息是否有效，并把结果返回商家；

• 商家返回信息给持卡人，送货；
• 商家定期向支付网关发送要求支付信息，支付网关通知卡行划帐，并把结果返回商家，交易结束。

3.2.1.2 SET 协议中的密码学技术

SET 协议采用了对称密钥和非对称密钥体制，把对称密钥的快速、低成本和非对称密钥的有效性结合在一起，以保护在开放网络上传输的个人信息，保证交易信息的隐蔽性。其重点是如何确保商家和消费者的身份和行为的认证和不可抵赖性，其理论基础是著名的非否认协议 （Non-repudiation），其采用的核心技术包括 X.509 电子证书标准与数字签名技术（Digital Signature）、报文摘要、数字信封、双重签名等技术。如使用数字证书对交易各方的合法性进行验证；使用数字签名技术确保数据完整性和不可否认；使用双重签名技术对 SET 交易过程中消费者的支付信息和定单信息分别签名，使得商家看不到支付信息，只能对用户的订单信息解密，而金融机构只能对支付和账户信息解密，充分保证消费者的账户和定货信息的安全性。 SET 通过制定标准和采用各种技术手段，解决了一直困扰电子商务发展的安全问题，包括购物与支付信息的保密性、交易支付完整性、身份认证和不可抵赖性，在电子交易环节上提供了更大的信任度、更完整的交易信息、更高的安全性和更少受欺诈的可能性。

3.2.2 电子现金支付协议

电子现金（e-cash 或 digital currency）是以数字化形式存在的现金货币，具有多用途、灵活使用、匿名性、快速简便的特点，无需直接与银行连接便可使用，适用于小额交易。其主要好处是可以提高效率，方便用户使用。目前一些电子现金支付方式只需要软件，而另一些则需要新硬件--主要是智能卡，即主要有智能卡形式的支付卡或数字方式的现金文件。也可采用现金转卡或采用 Mondex 卡转卡的方式。其安全使用是一个重要的问题，包括限于合法人使用、避免重复使用等。不同类型的数字货币都有其自己的协议，用于消费者、销售商和发行者之间交换金融申请。每个协议由后端服务器软件--电子现金支付系统，和客户端的"钱包"软件执行。

3.2.3 电子支票

电子支票（e-check 或 e-cheque）支付目前一般是通过专用网络、设备、软

件及一套完整的用户识别、标准报文、数据验证等规范化协议完成数据传输，从而控制安全性。这种方式已经较为完善。电子支票支付现在发展的主要问题是今后将逐步过渡到公共互联网络上进行传输。电子资金转账（Electronic Fund Transfer，简称 EFT）或网上银行服务（Internet Banking）方式，是将传统的银行转账应用到公共网络上进行的资金转账。一般在专用网络上应用具有成熟的模式（例如 SWIFT 系统）；公共网络上的电子资金转账仍在实验之中。

3.2.4 微支付

微支付"（micropayments）的特征是能够处理任意小量的钱，适合于因特网上"不可触摸（non-tangible）商品"的销售。一方面，微支付要求商品的发送与支付要几乎同时发生在因特网上；另一方面，商品销售、处理与运输的"瓶颈"为保持成本低廉设置了障碍。为保持每个交易的发送速度与低成本，目前有很多厂商在致力于发展别的协议以支持 SET 和 SSL 所不能支持的微支付方式，其中之一是微支付传输协议（Micro Payment Transport Protocol，简称 MPTP），该协议是由 IETF 制定的工作草案。"微支付"的一个重要方面是其定义随着对象而变化，有许多系统声明其是"微支付"，允许支付小于现有货币面额的数额。如 IBM开发的"Micro Payments"、Compaq 与Digital开发的"Millicent"、CyberCoin 开发的"CyberCash"等。 联合电子支付联盟 JEPI（Joint Electronic Payment Initiative）：是由 World Wide Web 协会和 CommerceNet 领导的一个联盟，目的是对支付协商过程进行标准化。在买主一方（客户方），JEPI 是 WEB 浏览器和 wallet 使用不同协议的接口，在卖主一方（服务器方），JEPI 在网络和传输层之间，将下层激活的事务送给适当的传输和支付协议。

3.3 移动商务支付方案

在移动商务蓬勃发展的情况下，作为主流移动设备商的爱立信和诺基亚分别提出了自己的一整套移动商务解决方案。

3.3.1 Ericsson Mobile e-Pay 移动商务解决方案

Mobile e-Pay 支持使用移动电话来完成金融交易并与后端应用系统互联。Mobile e-Pay 的基本功能还包括算法转换功能——用于将固定网络协议转换成适应移动终端的功能，以及运营、管理和维护（OA&M）功能。Mobile e-Pay 的

可选的功能还包括提供支付方案和移动终端的浏览功能。

爱立信公司的 Mobile e-Pay 解决方案将移动通信网络、Internet、在线支付和安全技术有机地结合在一起，为移动电子商务提供了一个完整的解决方案。它的基本功能是使用移动电话来完成金融交易并与后端系统相联系，以及运营、管理和维护（OA&M）功能。

Mobile e-Pay 包括访问、支付和安全三大模块功能。访问功能完成各种访问请求的处理，它是进行移动电子商务的基础。支付功能主要是完成对服务提供商提供的商品或服务的付费。安全功能提供交易数据的认证、加密、数字签名和非否认服务，用以保证移动电子商务交易的安全。这三大功能共同构成了一个完整的移动电子商务方案。

Mobile e-Pay 支持的访问功能包括："拉"请求、"推"请求、移动网络、收据处理等。

Mobile e-Pay 支付模块允许提供商提供完整的支付方案，它为用户提供可通过移动电话访问的新电子钱包。因此，移动用户可以使用他们的移动电话作为支付商品或服务的基本设备。Mobile e-Pay 支持以下几种支付方法，标准支付接口、Jalda 支付 、信用卡支付 、Mobile e-Pay 预付账户、银行账户、借记卡支付。

Mobile e-Pay 提供了几种安全解决方案：PIN 安全、3DES SAT 安全、端到端 WPKI 安全等。

3.3.2 诺基亚 wallet 与 WIM 解决方案

诺基亚支付方案使移动终端具有支付能力，它主要对 WAP 网站上的电子内容的交易提供支付支持，同时也用来为其它商品和服务的交易提供支付支持。诺基亚支付方案包含几个主要部分：诺基亚支付服务器、虚拟钱包(Wallet)应用程序等等。此方案以虚拟钱包应用程序所管理的预付费帐户消费卡为基础，通过基于 WIM 的 WAPI.2 所确定的数字签名方案来授权每一笔支付交易。

虽然通过诺基亚支付方案所包含的一系列综合服务，可以很容易地搭建起移动商务支付平台，但是由于缺乏支持 WIM 的手机，诺基亚支付方案中有关基于 WIM 数字签名功能还无法实现。

第四章 简单支付协议设计

4.1 支付协议设计背景

小额支付业务为移动用户提供了一个通过手机进行交易支付和身份认证的途径。本文通过具体分析以下三种不同接入方式实现的小额支付应用解决方案，最终选取一种具有较高灵活性和安全性的方案作为电子支付协议的运行环境。

4.1.1 基于短消息的接入方式

短信具有简便、易用、通讯费用低廉等特点，已相当普及并仍在继续发展。目前大多数服务提供商均考虑采用此种接入方式来实现小额支付应用。从不同的系统设计考虑，基于短消息接入方式的小额支付主要包含以下三种方式：

4.1.1.1 普通短信

此类方案的设计是在考虑到移动 GSM 网络系统自身的安全性比较高，再加上需要用户输入个人密码回复确认，可以认为此系统结构是比较安全的。而且系统的架构比较简单，易于实现，对用户的移动终端设备也没有特殊要求，用户使用的手机只要能够收发普通短信即可使用。但是此方案的安全性只是基于用户的手机号码和用户的个人密码，没有传输层的安全机制，而且明文传输易于泄漏密码，很难实现较复杂和多交互的交易应用，由于短信的实时性和可靠性不是很高，因此普通短信的数据容量对该服务的限制也较大。图 4-1 为基于普通短信的小额支付方式。

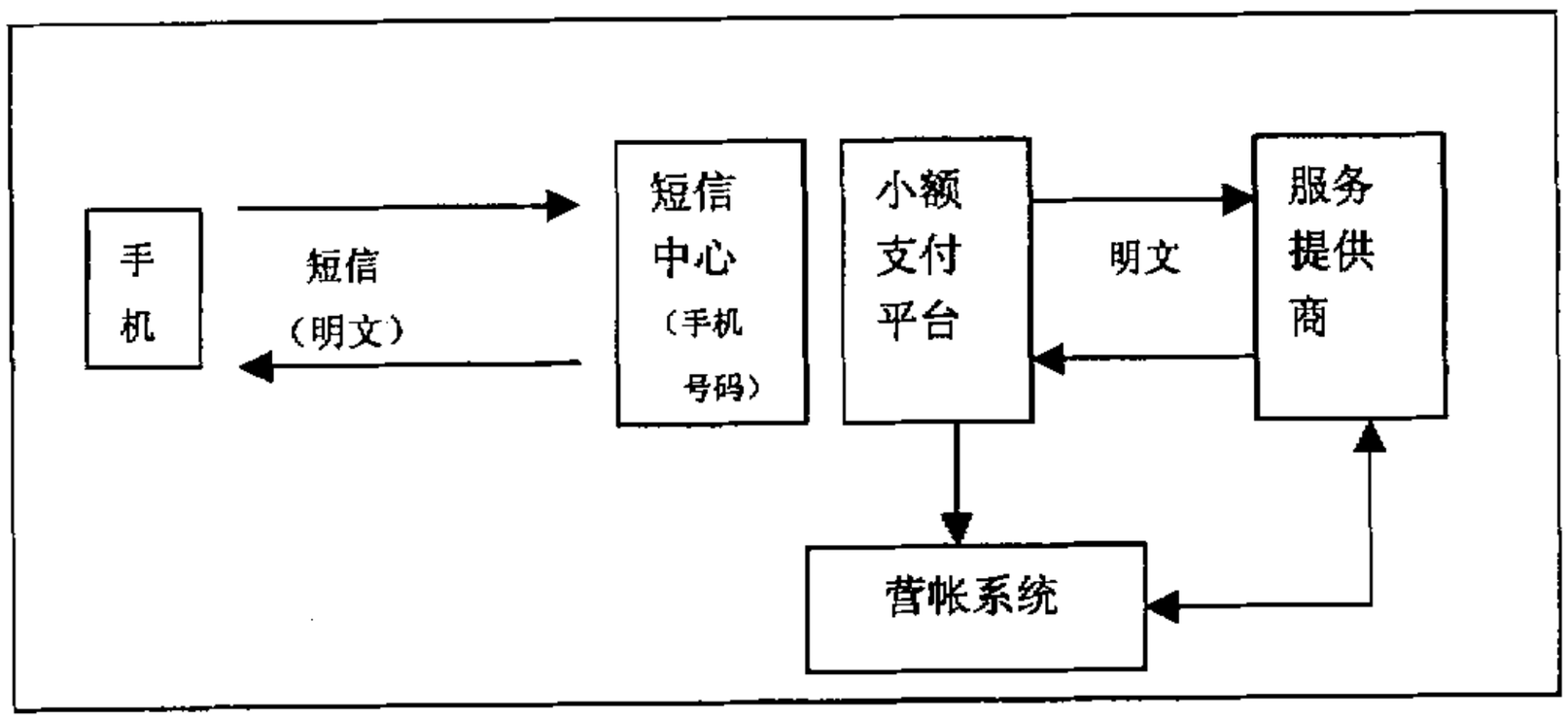

图 4-1 普通短信接入方式

4.1.1.2 STK 卡

此方案实现了较完整的传输安全机制，采用了 3DES 加密和 MAC 值校验，具有较友好的用户界面，应用程序的菜单等都是写入 STK 卡中的易于使用、同时还能实现较复杂的和有限交互的交易。因此目前此类方案已被许多无线交易系统所采用，特别是用于手机银行，手机证券等应用。用户使用该项服务时需要将原有的 SIM 卡换成 STK 卡才可以进行有限的移动交易，但由于目前市场上大量的 STK 卡尚不具备 OTA 更新菜单功能，用户不能灵活地选择所需服务，菜单更新困难，增加服务和改变服务时都需要通过移动运营商重新写入程序；且用户菜单开发困难，只能由卡商来完成，同时对称密钥体制对用户密钥管理要求很高，无论是采用固态密钥还是由主密钥加随机码运算而得的密钥都存在着保密问题。因此此类通过 STK 卡来实现的移动小额支付的解决方案始终没有能够推广开来。图 4-2 为基于 STK 卡的小额支付方式。

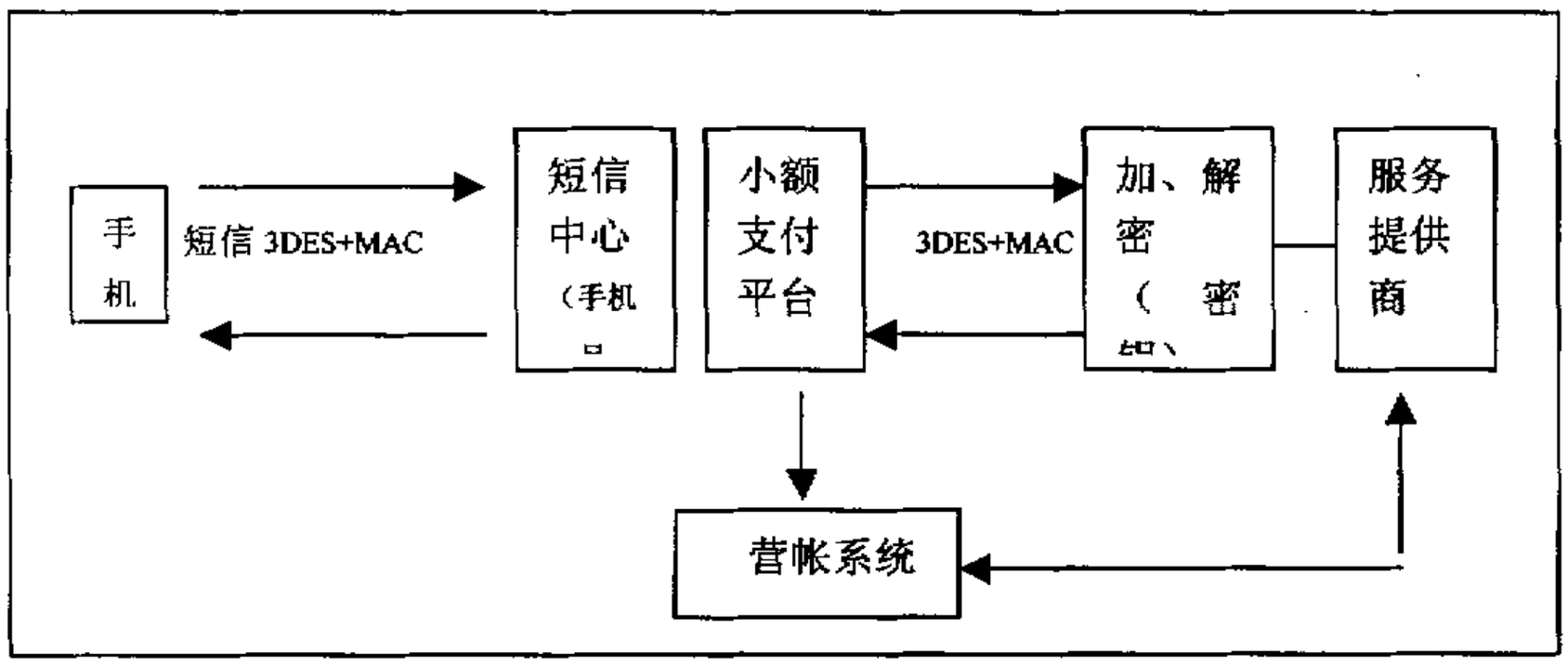

图 4-2 STK 接入方式

4.1.1.3 WPKI 卡

本类方案与前两个解决方案相比，增加了更加完善的安全机制，系统采用了 3DES 加密和 RSA 签名算法，并内置了 STK 指令的解析器和 OTA 空中下载更新功能，是一个完善的移动交易解决方案，也是目前唯一可以提供端到端安全交易的方案。通过 OTA 空中下载技术使得手机用户更加便利地添加和选择自己所需的服务，还可以实现复杂的多次交互式交易；对于服务提供商来说开发过程也相对简单。但整个系统架构较为复杂，其中涉及到密钥管理及需要 CA（证书发放机构）的引入。用户必须更换 SIM 卡方可使用此项服务，且目前 SIM 卡的功能和处理能

力也有一定局限。图 4-3 为 WPKI 卡的小额支付方式。

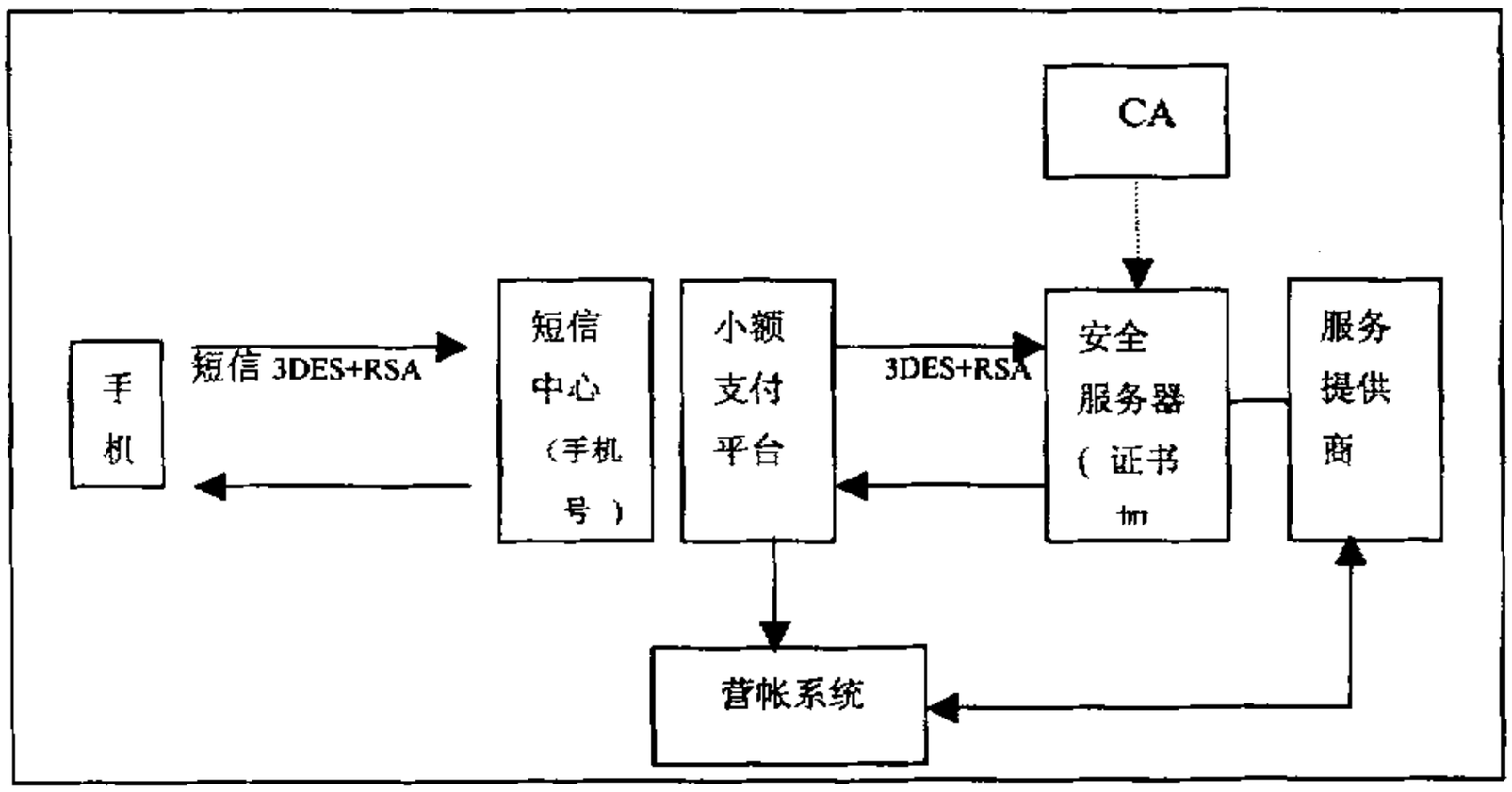

图 4-3 WPKI 接入方式

4.1.2 基于呼叫中心的接入方式

传统的呼叫中心系统已经非常成熟，它是基于硬件基础上的，具有较高的稳定性，服务的实时性也较好。目前移动运营商现有的充值卡业务均是基于呼叫中心系统之上的。因此此系统实现起来相对简单，系统几乎对用户的移动终端无任何要求，服务提供商可以很方便地对系统进行升级并不断给用户提供新的服务。但此系统的安全机制是完全依赖于移动语音通信的安全。此类解决方案仅适于开展预付费业务，且服务的操作复杂，耗时较长，通讯费用相对也较高。基于呼叫中心的接入方式如图 4-4 所示。

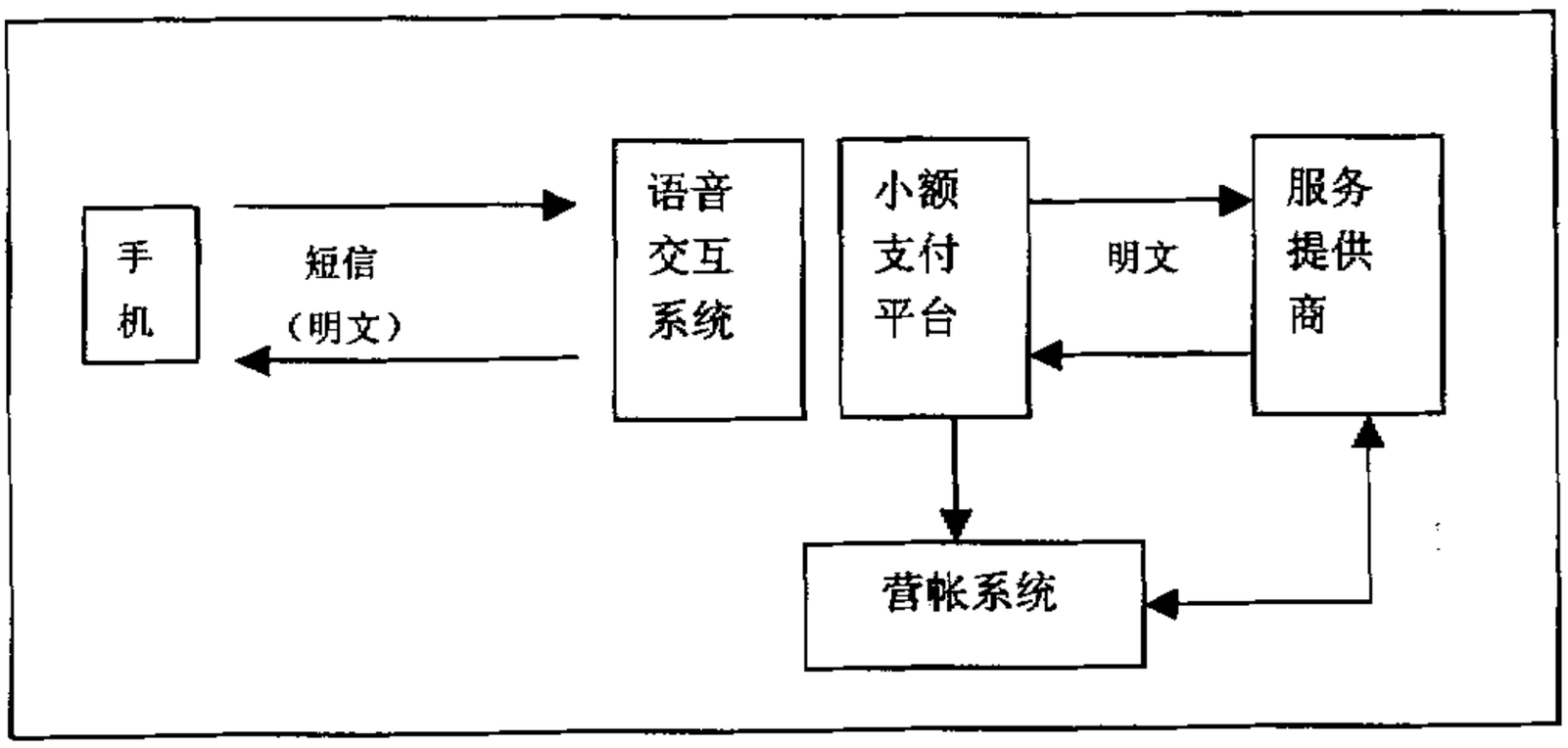

图 4-4 呼叫中心接入方式

4.1.3 基于 WAP 的接入方式

随着移动运营商网络的发展以及移动终端厂商技术的不断完善，WAP 技术在移动支付服务上已经可以提供很好的用户界面和完整的安全机制。该类方案在设计上采用将移动终端到 WAP 网关之间通过 WTLS 安全传输机制得以实现，同时系统还可以结合 WIM 卡提供用户证书的验证和对数据的签名功能。手机用户通过此系统可以实现复杂灵活和多次交互的交易。但此系统结构较为复杂，WAP 网关与服务提供商之间的接口需要采用 SSL 连接，而且大部分移动用户想要使用此服务时还需更换手机。目前 WAP 手机使用起来还不是十分方便，网络条件及速度也不十分稳定。基于 WAP 的接入方式如图 4-5 所示。

由于基于 WAP 接入方式的解决方案具有很高的灵活性和安全性，本论文中采用这种方式作为移动商务解决方案的运行环境。

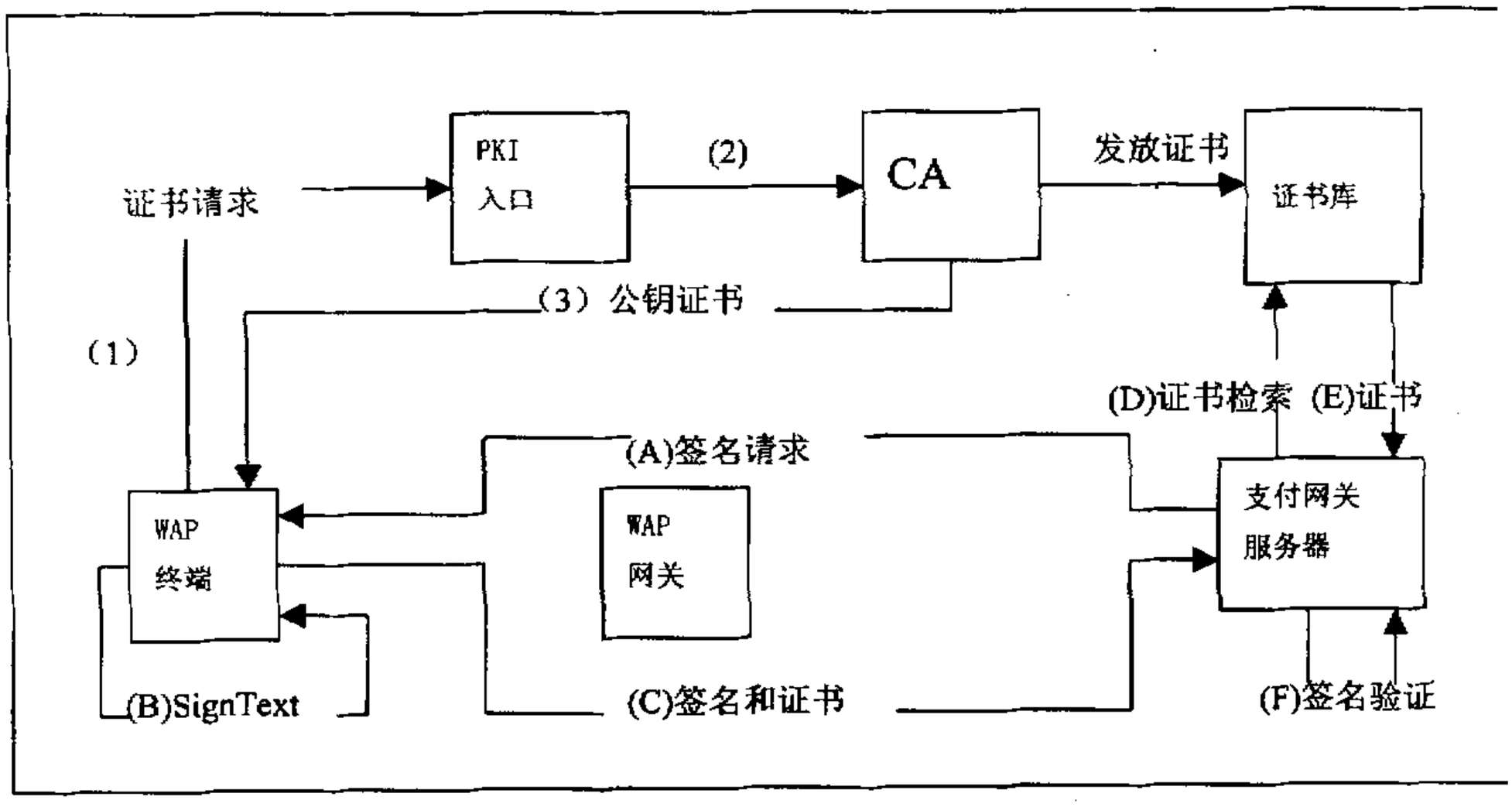

图 4-5 WAP 接入方式

4.2 电子支付协议设计

4.2.1 目的

移动电子商务系统是一种以移动通信网络为传输载体的交易系统，其功能是实现电子货币的支付和服务的兑现或承诺，其核心是电子支付系统。移动商务支付行为通过电子支付协议来实现，因此我针对移动通信中的一些特点（数据带宽窄、通信质量差等），提出了一种较为简洁的电子支付协议。

本协议所制定的支付流程，能够保证在用户（持卡人）（C）、商家（M）和银行（G）之间完成安全的电子支付行为。

4.2.2 流程

移动商务交易过程可细分为“浏览”、“选择”、“定购”、“支付请求生成”，“支付授权”和“委托支付”六个阶段。当用户经过“浏览”、“选择”和“定购”三个协议初始化阶段后，才真正开始激活本支付协议来完成“支付请求生成”，“支付授权”和“委托支付”阶段。

C 表示用户（持卡人），M 表示商家，G 表示网关（网关以银行代理的身份出现在移动商务支付过程中）；ID_m、ID_c 表示商家、顾客的身份标识符，Od 表示订单，Pd 表示支付帐单,Purchamt 表示交易数量；H(x)表示 Hash 函数， Td 表示交易数据，其内容包括 C、M、(ID_m，ID_c)、Purchamt、H(Od)、H(Pd)；RD 表示银行对交易认证并转帐的结果，(RD，H(Td))Kg^{-1}相当于发票，网关用其向商家和用户证明支付交易已经完成；而 Km、Km^{-1}为商家的公开和秘密密钥，Kc、Kc^{-1}为用户的公开和秘密密钥，Kg、Kg^{-1}为网关（银行代理）的公开和秘密密钥。协议执行流程如下：

- 初始化
  C—>M ： (C, M)
- 支付请求生成
  C—>M ： $(Od)Kc^{-1}$, Od
  M—>G ： $(TD)Km^{-1}$, $(TD)Kg$, $(Pd)Km^{-1}$, $(Pd)Kg$
- 支付授权
  G—>C ： Pd
  C—>G ： $(Pd)Kc^{-1}$
- 委托支付
  G—>M ： $(RD, H(TD))Kg^{-1}$
  G—>C ： $(RD, H(TD))Kg^{-1}$

图 4-6 电子支付协议

经过“初始化”阶段后，商家和用户已经分别获得了对方身份标识 ID，这就为电子支付协议建立了初步的执行环境。在“支付请求生成”阶段，用户将定购信息（Od）发送给商家，商家根据从用户得到的定购信息（Od）生成支付信息（Pd）和交易信息（TD）并将其发送至支付网关。在“支付授权”阶段，支付网

关将支付信息发往用户请用户核实，用户对支付信息核实无误后授权支付网关可以进行转帐行为。在“委托支付”阶段，支付网关已经分别得到了用户和商家的授权，因此在得到商家应用系统的委托支付请求以后，支付网关以银行代理的身份执行转帐行为，在支付行为成功完成后，支付网关将转帐结果以发票的方式发往用户和商家，以便用户（持卡人）和商家应用系统确认网关的已完成支付行为。

4.3 电子支付协议分析

4.3.1 Kailar 逻辑简介

4.3.1.1 Kailar 逻辑概述

Kailar 逻辑是 Rajashekar Kailar 提出的一种形式化逻辑证明方法，它的基本概念是可追溯性，即协议中源到目标的“动作”（发送一组数据）可以向第三方予以“证明”。与 BAN 逻辑不同的是，它不是研究协议中的“信任”关系，而是研究“可证明”(CanProve)的关系。证明分为强证明和弱证明。电子商务的目标可以表述为（C 是用户，M 是商家）：

- C CanProve (M 收到了付款)
- M CanProve (C 履行了付款)
- C CanProve（服务或承诺是有保障的）
- M CanProve（服务或承诺是有保障的）

4.3.1.2 Kailar 逻辑的记号、语义和语法

假设 A、B 是（客户或商家的）主机，K 是密钥，m 是消息

(1)A CanProv x ： A 可（强）证明 x

(2)A CanProv x to B ： A 可以向 B 证明 x

(3)A IsTrustedOn x: 表示 A 给出 x 是可信的

(4)A IsTrustedOn x by B:B 认为 A 给出的 x 是可信的

(5)K Authencates A: 表示可以通过公钥 K 来认证 A

(6)x in m ： x 蕴含在消息 m 中

(7)A say x: A 说过 x

(8)A Receives m signed With K^{-1}：A 收到了用 K^{-1} 签名的消息 m

(9)x => y： x 蕴含 y

(10)x∧y:x 并且 y

(11)（P；Q）|R：表示若 P 和 Q 同时成立，则 R 也成立

4.3.1.3 Kailar 逻辑的基本推理规则

K1:(A CanProve x;A CanProve y) |=A CanProve(x∧y)

K2:(A CanProve x; x=>y) |=A CanProve y

K3:((S(S 表示一组前提);C CanProve y)=>(A CanProve x)) |=
((S;C CanProve y to B)=>(A CanProve x to B))

K4:((S;C IsTrustedOn y)=>(A CanProve x)) |=
((S;C IsTrustedOn by B)=>(A CanProve x to B))

K5:(A Receives (m Signed With K-1); x in m; A CanProve (K Authenticates B)) => (A CanProve x to B))

K6: (A CanProve (B Says x); A CanProve(B Is TrustedOn x) |=(A CanProvex)

4.3.2 协议安全性分析

4.3.2.1 协议目标

由于本协议是电子支付协议，其目标只是完成电子支付，不涉及服务或承诺的兑现，因而可以表述为：

①C CanProve(RD,H(TD))，即 M 收到了付款；

②M CanProve(RD,H(TD))，即 A 履行了付款；

4.3.2.2 协议形式化（理想化）

① a. M Receive Od Signed With Kc^{-1}

b. G Receive TD Signed With Km^{-1}

c. G Receive Pd Signed With Km^{-1}

② G Receive Pd Signed With Kc^{-1}

③ M Receive (RD, H(TD)) Signed With Kg^{-1}

C Receive (RD, H(TD)) Signed With Kg^{-1}

4.3.2.3 初始假设

P1: C, M CanProve (Kg Authenticates G)

P2: C, G CanProve (Km Authenticates M)

P3: M, G CanProve (Kc Authenticates C)

P4: G IsTrustedOn Pd by C

4.3.2.4 协议分析

1. 由①a 和 P3 及 K5 可得： M CanProve(C says Od)
2. 由①c 和 P2 及 K5 可得： G CanProve(M says Pd), 由②和 P3 及 K5 可得： G CanProve(C says Pd), 这样 G 就可以实施转帐并且开出发票。
3. 由③和 P1 及 K5 可得： M CanProve(G says （RD, H（TD）)) 和 C CanProve(G says （RD, H（TD）)), 再由第一步中证明得到的 M CanProve(C says Od), 此时商家就可以向用户提供服务或某项承诺了。

这样就从逻辑角度“证明”了此电子支付协议可以实现预定的电子支付的目标，从而可知此简洁的电子支付协议是安全的。

4.4 电子支付协议描述

本节将根据上文中所描述的协议为基础，详细设计其中参与支付活动各方的具体行为，以及协议交互过程中使用到的协议数据单元和协议状态迁移情况。

4.4.1 概述

4.4.1.1 支付协议中的角色

1. 用户（持卡人、支付者）： 在移动商务环境中，支付者使用手机通过移动英特网与商家和支付网关交互。支付者拥有经认可的 CA 发行的数字证书。
2. 商家： 具有货物或服务提供给支付者的组织。

3. 金融机构（银行）： 可以为拥有合法资金帐户的商家和支付者提供资金转帐服务的组织。

4. 支付网关： 支付网关以金融机构代理的身份出现在移动商务环境中，实现核准和支付功能。

4.4.1.2 协议执行过程

本文电子支付协议的执行过程可以划分为生成支付请求、支付信息验证和支付请求委托三个阶段：

1．支付请求生成

①手机用户浏览商家 WAP 网站信息

②手机用户确定购买清单(OI)，并将其发给商家

③商家记录手机用户购买清单(OI)

④商家将购物支付记录(PI)以数字信封格式提交给支付网关

⑤支付网关校验商家身份信息

⑥支付网关记录手机用户的支付记录(PI)，初始化支付记录中的支付状态

2．支付信息验证

①商家要求手机用户支付帐单

②手机用户从支付系统获得支付记录(PI)

③支付网关修改支付记录中的支付状态字段

④手机用户用私钥对帐单签名，生成签名信息（格式参见 signcontent）

⑤手机用户将签名信息交给支付网关

⑥支付网关验证手机用户签名信息有效性

⑦支付网关保存手机用户签名信息

⑧支付网关修改支付记录中的支付状态字段

3．支付请求委托

①手机用户请求商家发货

②商家向支付网关查询支付记录状态

③商家请求支付网关向营帐系统提交支付合同

④商家向支付系统提交购买清单编号

⑤支付网关验证商家身份

⑥支付网关查询支付记录状态

⑦支付网关向帐务系统提交支付合同

⑧支付网关通知商家提交成功

⑨支付网关修改支付记录中的支付状态

⑩商家通知手机用户即将发送货物

4.4.2 协议数据结构

本小节以 ASN.1 对电子支付协议中定义的关键数据结构进行简要描述。

4.4.2.1 购物清单(OI)

支付者在浏览商家 WAP 网站过程中选定商品，商家应用系统生成相应的购物清单。购物清单作为商家生成支付请求的依据，在支付者完成支付行为后商家应用系统根据购物清单向支付者提供服务或者商品。

```
OrderInformation ::= SEQUENCE
    {
        orderNumber          INTEGER,        ---定购单号码
        merchantIdentifier   OCTET STRING,   ---商家 ID
        consumerIdentifier   OCTET STRING,   ---用户 ID (MSISDN)
        commodityName        OCTET STRING,   ---商品或者服务名称
        Price                REAL,           ---商品或者服务价格
        timeStamp            OCTET STRING    ---时间戳为 UTCTime 格式
    }
```

4.4.2.2 支付请求(PaymentRequest)

商家应用系统根据支付者提交的订购信息，生成支付请求发送至支付网关，请求在支付网关的协助下完成整个支付过程。支付请求中包含着和支付行为相关的所有必要信息，并且支付请求通过订购单号码与订购信息一一对应。

```
PaymentRequest ::= SEQUENCE
    {
```

```
    orderNumber          INTEGER,        ---定购单号码
    merchantIdentifier OCTET STRING,  ---商家 ID
    consumerIdentifier OCTET STRING,  ---用户 ID
    totalPrice           REAL,           ---支付金额
    timeStamp            OCTET STRING    ---时间戳为 UTCTime 格式
}
```

4.4.2.3 支付信息(PaymentInformation)

支付网关根据商家应用系统提交的支付请求生成对应的支付信息，随后支付网关将根据电子支付协议所规定的支付流程引导支付者和商家应用系统完成整个支付过程。支付信息通过订购单号码字段与商家应用系统中的订购信息一一对应。

```
PaymentInformation ::= SEQUENCE
    {
        orderNumber          INTEGER,        ---定购单号码
        merchantIdentifier OCTET STRING,  ---商家 ID
        consumerIdentifier OCTET STRING,  ---用户 ID
        totalPrice           REAL,           ---支付金额
        timeStamp            OCTET STRING    ---时间戳为 UTCTime 格式
        signedContent        OCTET STRING,   ---支付者签名，格式为
                                                WAP SignedContent
        status               StatusCode      ---协议执行当前状态
    }
StatusCode ::= ENUMERATED
{
    notSet (0),                  INTEGER,        ---未置
    new (1),                     INTEGER,        ---新记录
    authorizationPending (2),  INTEGER,  ---未验证
    authorized (3),              INTEGER, ---授权
```

```
        committed (4)                INTEGER,---委托
    }
```

4.4.2.4 签名内容（SignedContent）

支付者在核对支付信息无误后，使用自己的签名密钥对支付信息签名，授权支付网关进行支付交易，签名内容格式详细描述参见 WAP 协议。

```
signedContent ::= SEQUENCE
    {
        version          INTEGER,          ---版本信息
        signature        Signature,        ---签名
        signerInfos      SignerInfo,       ---签名者信息
        contentInfo      ContentInfo,      ---内容信息
        authenticated    Attribute,        ---认证信息
    }
```

4.4.2.5 支付信息状态查询/响应对

商家应用系统通过查询支付网关中指定支付信息的支付状态，然后根据支付网关返回的查询响应确定支付行为是否已经完成，从而进一步决定是否向支付者提供商品或者服务。

```
PaymentStatusRequest ::= SEQUENCE
        {
            orderNumber          INTEGER,          ---定购单号码
            merchantIdentifier OCTET STRING,  ---商家 ID
        }
PaymentStatusResponse ::= SEQUENCE
        {
            orderNumber          INTEGER,          ---定购单号码
            merchantIdentifier OCTET STRING,  ---商家 ID
            statusCode StatusCode                  ---支付状态
```

```
        }
StatusCode ::= ENUMERATED
    {
        notSet (0),                    INTEGER,        ---未置
        new (1),                       INTEGER,        ---新记录
        authorizationPending (2),      INTEGER,        ---未验证
        authorized (3),                INTEGER,        ---授权
        committed (4)                  INTEGER,        ---委托
    }
```

4.4.2.6 委托支付请求/响应

商家应用系统委托支付网关完成支付行为，支付网关向商家应用系统返回指令的执行结果。

```
PaymentCommitRequest ::= SEQUENCE
        {
            orderNumber          INTEGER,        ---定购单号码
            merchantIdentifier OCTET STRING,  ---商家 ID
        }
PaymentCommitResponse ::= ENUMERATED
        {
            notSet (0),          INTEGER,        ---未置
            new (1),             INTEGER,        ---新记录
            authorizationPending (2), INTEGER,. ---未验证
            authorized (3),      INTEGER,        ---授权
            committed (4)        INTEGER,        ---委托
        }
```

4.4.3 状态迁移图

本小节根据电子支付协议的执行流程，详细描述电子支付协议执行过程中的状态迁移。

1. “支付者”浏览商家网站，指示“商家应用系统”开始一个新的支付过程，“商家应用系统”生成交易记录并提交给“支付网关”，支付协议当前状态为“新记录”。
2. “支付网关”根据交易记录生成待签名数据提交给“支付者”，支付协议当前状态为“未验证”。
3. “支付者”用签名密钥对交易数据签名，将签名数据发送给“支付网关”，“支付网关”验证用户签名，“支付网关”通知“支付者”签名验证通过，支付协议当前状态为“授权”。
4. “支付者”通知“商家应用系统”授权成功，“商家应用系统”委托“支付网关”进行交易，协议当前状态为“委托”。
5. “支付网关”完成交易，协议当前状态为“存档”。
6. 在协议状态为“”、“”和“”时，“支付者”可指示“商家应用系统”撤消支付交易，协议状态转换为“未置”。

支付交易协议的完整状态迁移过程如图所示：

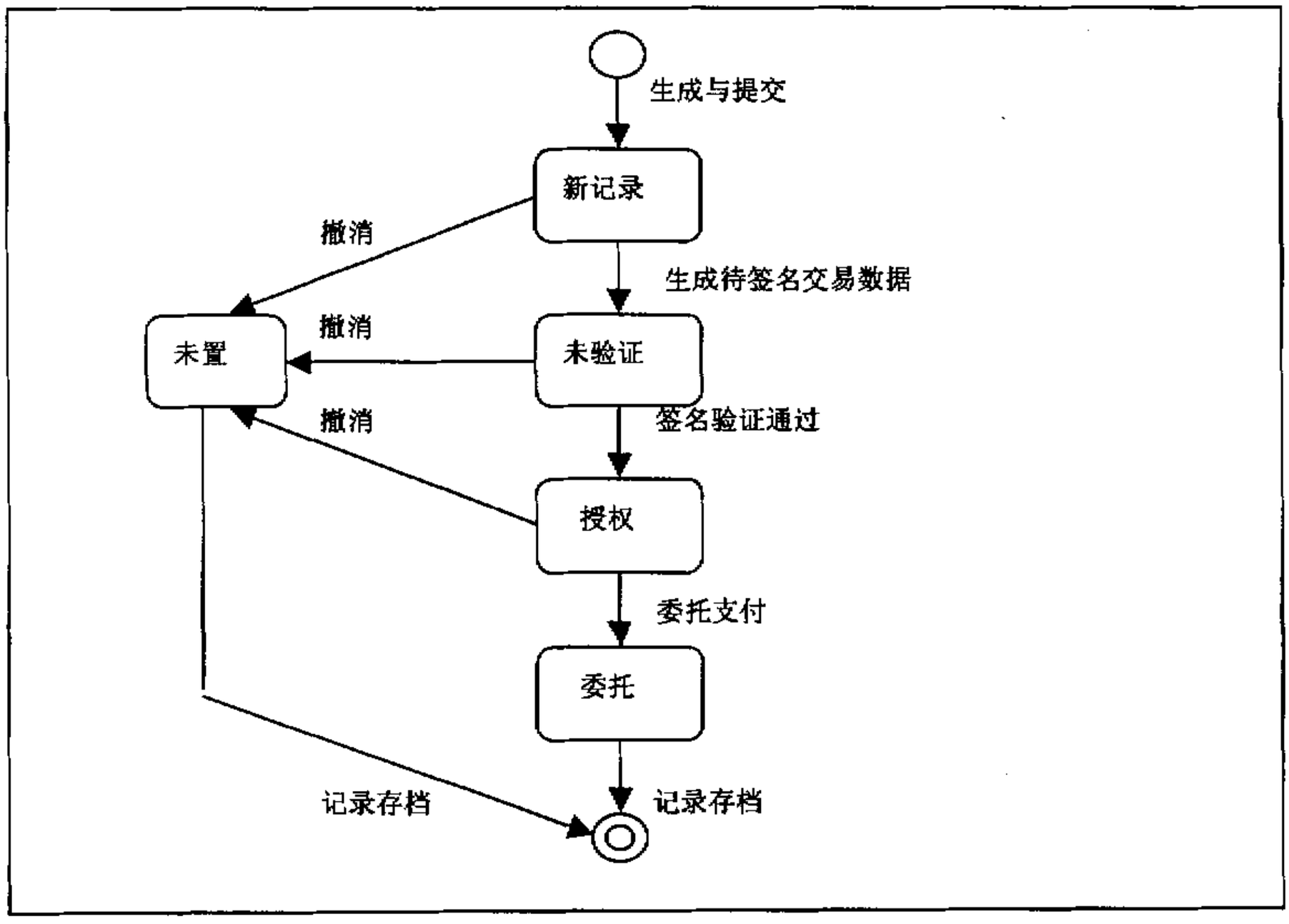

图 4-7 电子支付协议状态迁移

第五章 支付网关总体设计

本章对支付网关总体设计过程中的关键部分作详细介绍，包括支付网关的功能以及支付网关的总体设计方案。

5.1 支付网关的功能概述

本文的目标是设计实现一个安全支付网关系统。在以 WAP2.0 协议为基础的移动互联网环境中，该网关系统能够支持配备有 WIM 卡的 WAP2.0 兼容手机实现电子支付功能。

支付网关根据 MVC 设计模式思想采用层次化设计，每层保持各自相对的独立性，通过标准化接口进行层间通信，并为其它层提供服务。每层软件模块内部的改动(在保证与其它层软件模块接口不变的前提下)不会对其它逻辑层造成影响，这就为支付网关系统的开发提供了一种独立可扩的运行环境。

在一个完整移动商务体系中，共有三个关键角色与支付网关系统有交互行为，它们分别是商家、用户（支付者）、金融机构（银行等）。

支付网关系统不需要实现电子现金，而是要借助于信用卡或者借记卡等预付费方式来实现一种授权支付方式。支付网关以金融机构代理的身份，在得到用户（支付者）授权以后，完成商家与支付者帐户之间的资金交易。

根据用户（支付者）向其发出的定单信息，商家应用系统产生相应的支付信息，并将其发往支付网关系统。支付网关向手机用户（支付者）提交此支付信息，手机用户在对支付信息进行核实后，决定授权或者拒绝该支付交易。

所有已完成的支付记录数据永久存储于支付网关系统。由于支付记录中包含支付者授权信息，当商家或者支付者对支付网关的资金交易提出疑义时，可以将支付记录交由第三方进行公证。

商家应当能够向网关系统查询交易记录支付状态，从而决定是否向用户（支付者）提供它所要求的服务或者商品。

当用户（支付者）授权交易，并且支付网关系统对支付者的授权验证成功之后，商家有权指示网关系统进行资金流转交易。

支付网关系统能够验证用户（支付者）对支付信息的数字签名，在得到支付者对交易的授权后，进行资金划转。

当用户（支付者）仅仅向支付网关系统提供其数字证书的链接时，系统应当能够使用 LDAP 协议从外部证书库检索到用户（支付者）的数字证书，从而获得用户（支付者）的公钥来验证支付者对支付信息的数字签名。

支付网关以金融机构代理的身份参于整个支付过程，当得到支付者对交易的授权后，支付网关系统有权限从金融机构内部系统中得到支付者的信用情况，从而决定是否进行资金划转。

5.2 支付网关的设计和实现方案

本章简要阐述支付网关系统实现方案，包括支付网关需求分析、移动商务系统运行状态下的各个组成部分的逻辑关系，支付网关系统设计要点及其系统结构与功能。

5.2.1 需求分析

5.2.1.1 安全

系统安全模型应当遵守 WAP 论坛所制定的规范，在设计与实现时不需要考虑密钥长度，密钥的生成，证书的发放、取消，移动终端的实现和安全模型的实现。关于以上问题，论文做了以下假设：

- 移动终端内 WIM 所使用的签名密钥长度能够提供足够的安全性。例如，1024b 的 RSA 密钥或者 160bit 的 ECC 密钥。
- 签名密钥在 WIM 卡内生成，不会离开 WIM 从而保证了签名密钥的安全性。
- 证书发行者实时更新 CRL。

系统应当实现如下安全性设计标准：

- 非经授权的实体（用户或者商家应用系统）不允许进入网关系统或者访问系统数据。
- 只能通过系统提供的专门接口访问系统数据，系统不存在“后门”。
- 客户端与系统的通信链路经过加密处理 。

5.2.1.2 模块

系统分为多个独立模块，当以增加一个新模块的方式向系统添加新的功能时，不会影响到其它模块的运行。模块化的实现关键在于各个模块对外接口的设计，通过精心设计使各个模块间的接口具有“可插拔性”，在为系统增加新模块时不需要对整个系统进行编译。

5.2.1.3 性能

系统应当具有较好的运行性能。例如，在正常负载情况下，系统响应时间在用户可容忍范围之内。

5.2.1.4 维护

系统生成日志文件以便于进行系统管理。管理员至少能够通过日志文件来跟踪系统运行情况，并且能够通过一些简单的方法来解决系统运行中出现的问题。

5.2.2 系统结构及描述

5.2.2.1 系统体系结构

本文所提出的移动商务解决方案参照层次体系结构设计方法，关键模块均以JAVA技术开发实现。系统结构如下图所示，分为客户层、HTTP适配层、表示层、业务逻辑层、数据层和外部系统层共六层。由于移动商务系统核心组成部分为支付网关系统，因此本文以各个逻辑层次与支付网关系统的关系为参照物，对移动商务系统的各个逻辑层次予以命名。

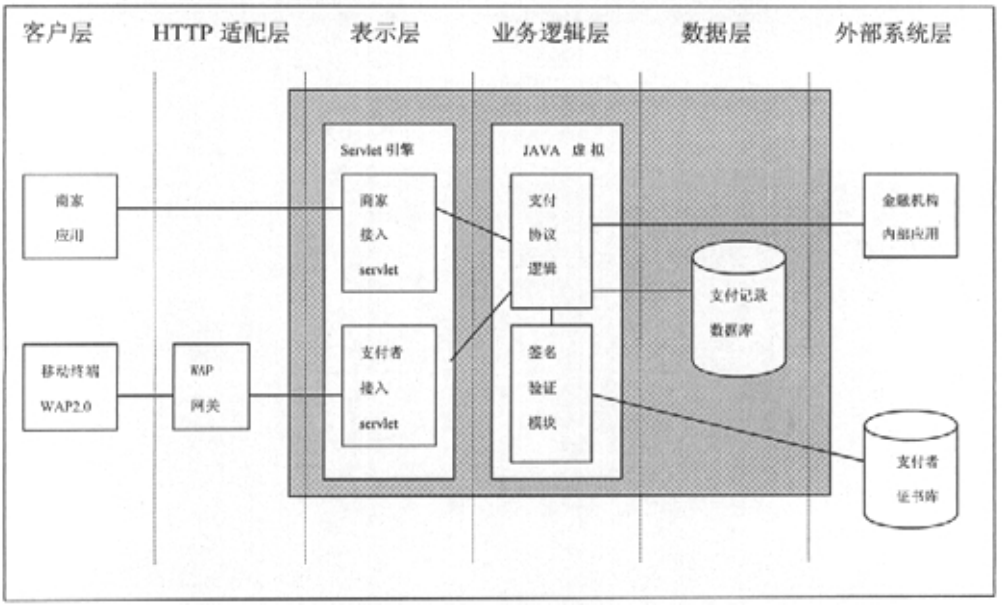

图 5-2 支付网关软件体系结构

层次化的设计结构有利于各个功能逻辑的封装，最大限度地隔离功能不同的软件模块，从而实现一个软件模块的内部改动不会影响到其它软件模块的实现（通过标准化不同软件模块之间的接口）。

在移动商务系统内，支付网关以金融机构代理身份为商家应用系统和移动终端提供支付服务，所以客户层包括商家应用系统和移动终端。支付网关的表示层与客户层的接口为 HTTP 协议。商家应用系统可以通过 TCP/IP 连接承载 HTTP 协议直接接入到支付网关，而不需要 HTTP 适配层功能；移动终端需要 WAP 网关将 WAP 协议转换为 HTTP 协议，因此对于移动终端来说，HTTP 适配层需要实现 WAP 网关的协议转换功能。

外部系统层功能包括金融机构内部应用系统和支付者证书库。支付网关在移动商务系统中的身份为金融机构代理，它的功能是依据电子支付协议保证电子支付过程的顺利进行，而真正的资金划转都由金融机构内部应用系统来完成，它们之间的接口由银行内部应用规定而非标准协议。支付网关验证支付者对交易数据的数字签名时，需要利用外部系统层提供的数字证书检索服务来获得支付者的数字证书，其接口使用 LDAP 协议。

支付网关系统分为三层结构，包括表示层、业务逻辑层和数据层。对支付网关结构和功能将在下文中详细讨论。

5.2.2.2 支付网关结构及功能

图中阴影方框内为支付网关系统结构图，系统设计以 MVC 设计模式思想为基础，将其分为表示层、业务逻辑层和数据层共三层。

1. 表示层

表示层以 HTTP 为接口协议为客户层提供接入服务，它包括“支付者接入 servlet”和“商家接入 servlet”两个模块。选择具有 servlet 引擎功能的 Web 服务器，采用 java servlet 开发模式简化了支付网关表示层的开发。

移动终端使用 WAP 微浏览器访问支付网关，“支付者接入 servlet”向移动终端发送 WML 页面，然后从移动终端送回的请求中得到参数内容，并将其发送到支付协议逻辑层，再将支付协议逻辑层的处理结果以 WML 页面的形式发送到移动终端。

确切地说，商家应用系统访问支付网关不需要表示层提供的 wml 页面，但为了简化系统结构和软件开发过程，支付网关表示层同样采纳 java servlet 开发模式向商家应用系统提供接入服务。“商家应用系统”以 HTTP 方式向支付网关表示层发送请求，“商家接入 servlet”从 HTTP 请求中获得参数内容，并将其发送至支付协议逻辑层，然后将支付协议逻辑层的处理结果以 HTTP 响应方式发回给商家应用系统。

2. 业务逻辑层

业务逻辑层按照电子支付协议规定的支付流程，在外部系统层的支持下，引导商家和支付者完成支付行为。

业务逻辑层包含很多功能模块，这些模块分别实现了支付协议逻辑功能、数字签名验证等功能。这些模块均以 EJB 方式实现，这样业务逻辑层就能够利用 J2EE Web Server 提供的分布式处理功能，实现支付网关处理能力的平滑升级。

3. 数据层

数据层提供关系数据库的数据存储及其访问功能。关系数据库中存储支付协议运行过程中产生的支付信息记录，以及支付过程完成后的历史支付交易记录。

支付记录中的状态字段永久保存协议当前运行状态，这样当支付过程发生异常中断时，业务逻辑层可以通过支付记录中保存的状态字段恢复协议的执行。

当支付者和商家对历史交易行为发生疑义时，可以将数据库中存档的历史交易记录交由公证的第三方进行裁决。

5.2.3 系统运行逻辑关系

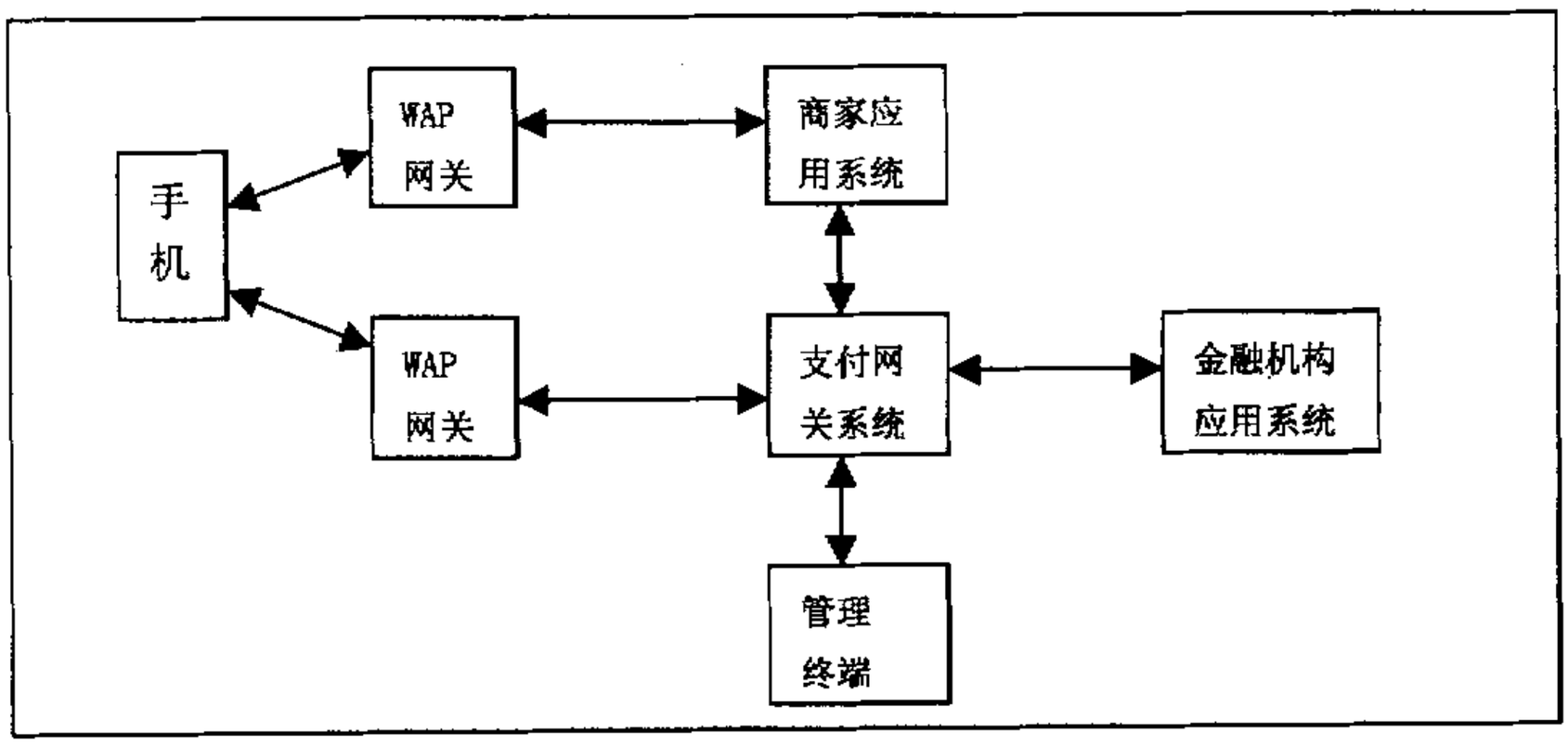

图 5-1 系统运行逻辑关系

本文中采纳四章中描述的 WAP 接入方式作为支付网关的解决方案（如图 4-5）。在基于 WAP 的移动商务环境中，各个组成部分的逻辑运行关系如图 5—1 所示。

支付网关系统需要与四种相关物理模块交互，它们分别是移动终端、商家应用系统、金融机构内部应用系统和管理终端。系统运行期间各个物理模块之间的交互数据格式在第四章《简单电子支付协议设计》中有详细叙述。

系统与移动终端通信（使用 WAP 协议），接收并验证用户的签名数据；与商家应用系统通信（使用 HTTP 协议），接收商家应用系统提交的支付相关数据，比如“支付生成请求”；与金融机构后端应用系统通信，完成支付者的信用查询以及帐户之间的资金划转（采用金融机构后端应用系统内部通信协议）；与管理终端通信（使用 HTTP 协议），向管理终端提供系统状态数据，接收管理终端的管理命令。

5.2.4 系统设计要点

我们可以将支付网关系统划分为三个层次设计来实现：表示层、业务逻辑层和数据层。系统设计要点为将业务逻辑层分为两大模块实现，分别是支付协议逻辑、签名验证模块。

1. 支付协议逻辑与表示层的两个软件模块（商家接入模块，支付者接入模块）之间存在标准化的接口，并且和业务逻辑层的另一个软件模块（签名验证模块）之间也存在一个标准化接口。支付协议逻辑模块引导商家和支付者顺利完成支付行为。

2. 签名验证模块是系统中的一个计算密集性模块，它的执行将会耗费大量的 CPU 时间，另外 WAP 规范中规定了几种可选的数字签名密码学算法，因此将签名运算功能作为一个独立软件模块分离出来有两个好处：使系统处理能力平滑提升；易于实现不同密码学算法的签名验证模块的动态载入。

3. 以成熟的分布式计算技术为基础，通过逐渐增加签名验证运算模块的数量并将其分布于不同计算机之上，利用负载平衡算法动态分配业务负载，从而使整个支付网关系统处理能力得到平滑提升。

第六章 支付网关系统实现

本章描述支付网关系统实现的一些细节。比如开发环境和开发工具的选择，开发过程中用到的一些密码学规范 PKCS 等；开发和测试环境的搭建，开发中使用到的软件设计模式等等。

6.1 支付网关系统体系结构

本节介绍支付网关系统体系结构及其实现过程中使用的软、硬件平台和开发工具。

6.1.1 支付网关物理结构

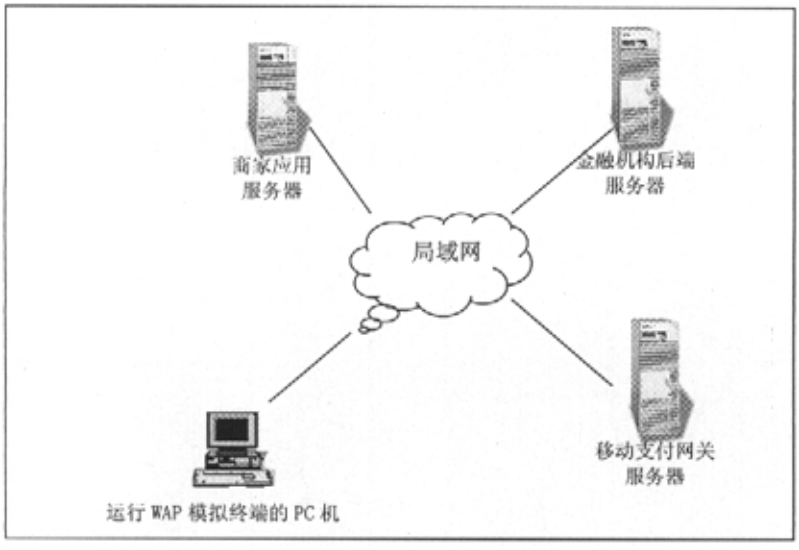

图 6－1 系统物理结构

网关系统物理结构如图 6-1 所示。运行于 PC 机上的 NMIT3.0 模拟 WAP 终端发起请求，分别访问商家应用系统 WAP 网站和支付网关系统。WAP 模拟终端、商家应用系统、支付网关系统和金融机构后端系统通过局域网相连。移动商务系统运行逻辑关系参见图 5－1。

6.1.2 软件和硬件平台

由于支付网关规模的可伸缩性较大，要求网关能够照顾到不同类型用户的要求，这样要求网关系统可以在不同的操作系统中运行，例如 NT、UNIX。进行本课题系统开发时我们采用了如下环境：

软件平台：　Windows 2000

数据库：　Oracle 8i for Sun Solaris

数据建模工具：　TODA v7

开发工具：　Jbuilder 4

编程语言：　JAVA

终端模拟工具：　Nokia Mobile Internet Tool v3.0

6.1.3 JAVA 平台

Java 不仅仅是一种语言，而且是一种区别于传统系统，遵循"网络就是计算机"信条的平台技术。Java 平台将面向对象系统扩展成包括程序和数据的网络计算机(NC)，而这个平台的核心就是 Java 虚拟机，许多使 Java 成为万能开发平台的属性都源于 Java 虚拟机的概念和实现。

从底层看，Java 虚拟机就是以 Java 字节码为指令组的软 CPU，字节码是 Java 虚拟机的指令组（很象 CPU 上的微码），开始执行前把所有字节码翻译成本地机器码，然后再将翻译后的机器码放在 CPU 上运行。

Java 具有很好的可移植特性。作为一种编程语言，JAVA 具有源代码可移植性；作为一个虚拟机，JAVA 具有硬件平台可移植性；作为一种虚拟的操作系统(OS)和图形用户界面(GUI)，JAVA 具有操作系统移植性。

Java 作为一种综合的开发平台，在客户端可以用于开发与运行硬件环境无关的客户端应用软件，在服务器端可以开发企业级服务应用。本文利用 Java 企业级应用开发环境的分布计算能力，为支付网关系统提供平滑扩容的能力。

6.1.4 WAP 网关与移动终端

NMITv3.0 具有内置的网关模块，具有解析 wml script 的功能，在系统实现时期，我使用其对系统进行模块测试而没有使用真正 WAP 网关。

目前市场上只有很少的几款手机真正支持 WAP2.0 中规定的 SignText 和 WIM 功能，所以我决定在系统实现过程中使用终端模拟器来完成模块测试。由于 NMITv3.0 实现了 WAP 规范中的 SignText 功能，并且具有内置的 WIM 卡及其签名和认证数字证书，因此最终选定 NMITv3.0 来模拟 WAP2.0 兼容手机。

6.2 关键算法和处理

6.2.1 WAP SingedContent

根据支付网关总体设计中对其功能的描述，支付网关的关键处理运算就是对支付者的数字签名进行验证，从而确定用户（支付者）是否授权支付网关处理特定的支付交易。

为了对 WAP SignedContent 进行验证，需要 j2se 中密码学运算类以及大数运算相关类的支持。由于 RSA 算法的专利权问题，J2SE 中并没有包含 RSA 算法的实现，因此就需要参考 RSA 密码学算法的原理，利用 J2SE 中提供的大数运算支持类来实现 RSA 数字签名的验证，并且利用 J2SE 中所提供的处理数字证书的相关类，从支付者的数字证书中获取他的公钥。

根据 WAP 论坛有关 WAP SignedContent 协议，支付者可以利用多种公钥密码学算法（例如 RSA、ECC）和报文摘要算法（SHA、MAC 等）来生成数字签名。为了简化开发过程和测试过程（NMIT3.0 采用和本文相同的设置），本文牺牲了软件的灵活性，将 WAP SignedContent 中的各个字段固定设置如下：

- Signature Algorithms ---RSA/SHA according to PKCS #1
- Signer Info Types ---X.509v3 Certificate
- Content Types ---data
- Authenticated Attributes ---GMT UTC time

6.2.2 MVC 设计模式

MVC(Model-view-controller pattern)模式由三部分组成。模型（Model）是一组表示应用系统商业逻辑的对象，它通常包括表示商业抽象的类（如：账号、采购等等）和现实世界的对象（如职员、客户等）；视图（View）是用一种向用户表达信息的具体方式，要理解视图的捷径是把视图想象成为一个具体的网页或者屏幕，它能够给用户提供一组互相有关的信息；控制（Controller）是应用系统处理具体流程和导向的核心部分。它把模型对象给出的信息翻译成视图可以理解的形式，并且处理系统流程的走向，例如视图在下一个回应中将会给用户什么样的反馈。MVC 的关键是商业模型的设计与实现可以独立于应用系统的结构设计与实现（控制）和界面的设计与实现（视图）。

MVC 模式可以与 J2EE 框架很好地结合，按照如下的方式将 J2EE 的元素映射到 MVC 的三个组成部分：

- Model: JavaBeans 和 Enterprise JavaBeans
- View: JavaServer Pages
- Controller: Servlets

这里 servlets 用作 controllers，用于接收 HTTP 的 POST 请求，并且负责将 POST 上来的数据传送给 model，然后选择用哪一个 JSP 页面来显示 model 处理的结果。这种系统结构通常又称为“Model II” JSP 结构。

在本文中以 MVC 设计思想设计和实现支付网关软件体系结构。支付网关中的三个逻辑层分别为表示层、业务逻辑层和数据层，分别对应于 MVC 设计模式中的视图、控制和模型。

6.2.3 负载平衡算法

支付网关接收到支付者的签名后的交易请求，需要对支付者签名进行验证。由于密码学算法的运算强度较高，所以在实现支付网关的密码学模块时，应当考虑到采用分布式环境来配置密码学模块。在支付网关运行过程中，当需要对支付者签名进行验证时，根据负荷平衡算法来选定特定的密码学模块进行处理。负载平衡算法用于平衡多个密码学模块之间的运算负荷，平衡的依据是历史纪录，算法的基本思想是根据历史纪录中的各个密码学模块的负荷量，选出最小负荷的密码学模块作为当前用户请求的处理器。

每一个历史记录对应一个密码学模块，历史记录中有一个计数器字段记录对应的密码学模块当前正在处理的签名验证的请求个数，支付网关控制模块根据历史记录来选择负荷较小的密码模块来验证支付者签名。

6.2.4 计费处理

由于 WAP 网关的配置情况将决定支付网关能否得到主叫号码， 所以当前用于区别用户的还是用户（支付者）帐户名，但在数据库中应当为主叫号码留了接口字段，在得到主叫号码后将按照主叫号码计费。

6.3 系统测试

系统功能测试主要验证系统各个组成部分的实现过程是否严格遵循了系统

设计规范。功能性测试的目的是验证系统数据处理过程的正确性，因此主要是从用例的观点来对系统进行功能测试，以下列举了本文的测试用例和结果。

6.3.1 测试用例：生成支付请求

商家应用系统应当能够生成一个包含所有支付相关信息的支付请求。

测试	结果
提交一个格式正确的支付请求	支付请求被接受
提交一个序列号重复的支付请求	支付请求被拒绝，系统报告支付请求序列号重复

6.3.2 测试用例：授权支付

用户（支付者）应能够连接支付网关系统从而授权支付网关处理支付事宜。支付网关系统接受一个格式正确的签名并且验证它。

测试	结果
提交一个正确签名	授权行为被接受
提交一个随机数据块作为签名	授权行为被拒绝，系统报告签名数据或者数字证书不正确

6.3.3 测试用例：委托支付

只有当用户（支付者）授权支付交易后，商家应用系统才能够委托网关进行支付交易。

测试	结果
委托支付交易（交易已经经过用户授权）	支付委托成功
委托支付交易（未经过用户授权）	支付委托失败，支付网关报告支付记录状态转换非法

第七章 结束语

随着中国移动开通 GPRS 业务，移动数据通信的带宽不断拓展，无线数据业务的能力日益增强。当越来越多的人拥有移动电话，而且越来越多的人越来越依赖互联网时，移动通信与互联网就不可避免地走到了一起。

移动互联网风潮一起，从欧洲、北美到亚洲，电信公司、网络公司、软件公司以及设备制造厂商无一例外地在移动互联领域投入巨额资金，不断推出新型的移动终端设备，以及切实可行的移动商务解决方案。

尽管移动商务的应用前景是乐观的，但我们必须看到，移动互联网和 WAP 技术仍有其局限性和急待解决的问题：无线通信线路的带宽受限，即使到了第三代速率也只能保证 384kbps，故而限制了移动数据应用的推广；WAP 的大发展需要方方面面的共同协作，如移动终端设备制造商、移动通信运营商、ISP、ICP、应用软件开发商以及固定网络经营者，协调难度比较大；WAP 信息资源不够丰富，信息内容对用户的吸引力并不是很大；手机的屏幕过小和操作的不便也会限制一些应用的开展。上网费用偏高，不利于发展用户。

由于移动互联网存在上述问题，移动互联网和 WAP 技术的应用与开发一度出现停滞，很多人也对 WAP 技术本身持怀疑态度。随着中国移动开通 GPRS 业务以及第三代移动通信系统的建立，上述局限性必然会得到克服，移动互联网的大潮必将到来。中国拥有世界上最大的 GSM 网，拥有世界上最大的潜在市场，中国移动互联网事业一定会随同世界大潮得到充分发展。

移动互联网在中国的发展具有特殊意义。因为美国等发达国家 PC 机用户数高于手机用户，中国则恰好相反，手机用户大于 PC 机用户数，中国用户群的特征决定了移动数据在中国可能会比在其他国家发展的更快。据预测，到 2005 年，中国的移动用户将接近 2 亿，这个市场基数是相当巨大的。

WAP 标准的最新正式版本是 WAP V2.0。WAP V2.0 将会采用 XHTML，并将 TCP 作为技术基础。WAP V2.0 具有很好的向前兼容性，可以和以前的版本很好地兼容。 据悉，WAP2.0 将会在原有的功能基础上，增加屏幕动画、流动多媒体和音

乐文件下载功能，此外还将具备彩色显示和实现基于位置的内容服务等功能。

WAP 已得到全球多数公司的认同，它与互联网的结合势在必行，并将在潜移默化中改变人们以往传统的生活工作方式，用户仅仅依赖 PC 上网的现状将得到改观。用户得益的不仅仅局限于简单地用 WAP 终端上网、收发邮件，更重要的是用户将享受到移动领域由此产生的各类增值业务，电子商务就是其中最具发展潜力和丰厚投资回报吸引力的业务之一，而 WAP 终端功能的增强以及第三代无线网络技术为它的进一步发展提供巨大契机，只要携带具有 WAP 功能的移动终端，用户即可随时随地享用证券交易、订票、网络银行、网上购物等各类业务，移动中的电子商务将真正地从单纯的概念跨入实施阶段，WAP 与电子商务紧密集合将为 21 世纪的人类生活展现更为美好的前景。

术语和缩略语

PTD	personal trusted device	可信的个人手持设备
ASN.1	Abstract Syntax Notation 1	抽象语法符号规则 1
B2B	Business to Business	商家对商家
B2C	Business to Consumer	商家对客户
BER	Basic Encoding Rules	基本编码规则
DER	Distinguished Encoding Rules	区分编码规则
ECDSA	Elliptic Curve Digital Signature Algorithm	椭圆曲线数字签名标准
FIPS	Federal Information Processing Standards	联邦信息处理标准
ICC	Integrated Circuit Card	集成电路卡
J2EE	Java 2 Enterprise Edition	JAVA 2 企业版
J2SE	Java 2 Standard Edition	JAVA 2 标准版
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
NIST	National Institute of Standards and Technology	国家标准与技术委员会
PIN	Personal Identification Number	个人识别码
PKCS	Public Key Cryptography Standard	公共密钥密码标准
RDBMS	Relation Database Management System	关系数据库管理系统
RSA	The RSA Pubic Key Cryptosystem	RSA 公共密钥密码体制
SSL	Secure Sockets Layer	安全套接层
URL	Universal Resource Locator	统一资源定位
WAP	Wireless Application Protocol	WAP 应用协议
WML	WAP Mark-up language	WAP 标记语言
WSP	WAP Session Protocol	WAP 回话协议
WTLS	WAP Transport Layer Security	WAP 传输层安全
PLMN	Public Land Mobile Network	公共陆地移动通信网

参考文献

[1]Wireless Application Protocol Architecture Specification, WAP Forum

[2]Wireless Application Protocol Architecture Specification, WAP Forum

[3]Wireless Application Protocol Wireless Transport Layer Security Specification, WAP Forum

[4]Wireless Application Protocol Wireless Telephony Application Interface Specification, WAP Forum

[5]Wireless Application Protocol Wireless Identity Module Specification, WAP Forum

[6]Wireless Application Protocol Public Key Infrastructure Definition, WAP Forum

[7]WAP Transport Layer End-to-end Security, WAP Forum

[8]《电子支付协议安全性的形式化分析》，信息工程大学学报，Vol.1 No.2，2002.6

致谢

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

最后，我还要感谢电子工程学院通信与网络实验室的所有老师和同学们给予我的关心和帮助。