② 商家接收订单，生成初始应答消息，数字签名后与商家证书持卡人联系。

③ 持卡人对应答信息进行处理，选择支付方式，确认订单，签发付款指令，将订单信息和支付信息进行双重签名，它对双重签名后的信息和用支付网关公钥加密的支付信息签名后连同自己的证书发送给商家（商家看不到持卡人的账户信息）。

④ 商家验证持卡人证书和双签名后，生成支付认可请求，并连同加密的支付信息转发给支付网关。

⑤ 支付网关解密后获得用户卡信息，向发卡行请求验证持卡人的账户信息，并生成支付认可消息，数字签名后发给商家。

⑥ 商家收到支付认可消息后，验证支付网关的数字签名，生成购买订单确认信息并发送给持卡人。

⑦ 至此交易过程结束。商家发送货物或提供服务并请求支付网关将购物款从发卡银行持卡人账户转账到收单银行商家账户，支付网关完成转账后，生成取款应答消息发送给商家。

20.6　3-D Secure

SSL 协议能解决交易两端信息传输的安全问题，但无法满足电子交易支付的个性化需求；SET 协议能有效解决电子交易支付的安全性，但因其协议过于复杂、成本过高而始终无法得到广泛应用。2001 年 VISA 推出了一种能够弥补 SSL 和 SET 不足的“VISA 验证”服务，这项服务采用全球互通付款的“3-D Secure 技术”，可有效减少信用卡在网络被盗刷的风险，对持卡人、特约商家及发卡银行都是皆大欢喜的多赢结果。

3-D Secure 是 3 Domain Secure 的缩写，是 VISA 为提高电子商务支付的有效性而提出的一种认证技术，它主要采用 SSL 加密技术和商家服务器插件 MPI（Merchant Server Plug-In）技术来实现。在在线交易中，它既能查询并鉴别持卡人的身份，又能够保护支付卡信息在网络中传递的安全性。

3-D 是指三方域模型，由三个域组成，即发卡域（Issuer Domain）、收单域（Acquirer Domain）和协作域（Interoperability Domain）。由于 3-D 是由 VISA 提出的，所以在协议定义中与 VISA 服务的各个部分（如 VISA 网络、VISA 目录等）联系紧密。

发卡域主要负责用户注册以及在交易中验证注册用户并为合法用户授权。发卡行系统主要通过一个充当中介的中间目录服务器与 3-D 特约商家联系，它必须有能力同时处理多个用户通过浏览器访问互联网进行交易的操作。而持卡人不需要任何特殊的软件，他们一旦注册，就可以通过标准浏览器进行交易活动。发卡域具体包括以下几个部分：

① 持卡人（Cardholder）：持卡人是在线交易的买方。在线交易结算时，直接或通过电子钱包提供卡号、卡的有效期以完成交易。当弹出认证 Web 页面时，持卡人提供认证信息（如密码或个人确认消息）即可。

② 持卡人浏览器（Cardholder Browser）：持卡人的浏览器充当了商家服务器插件（位于收单域）和访问控制服务器（位于发卡域）之间的消息传递通道。

③ 附加的持卡人组件（Additional Cardholder Components）：其他一些可选的持卡人端的软硬件设备，如智能卡需要的专用读卡软件和读卡器。

④ 发卡行（Issuer）：发卡行是指为持卡人建立一个账户并发放银行卡的金融机构。

⑤ 访问控制服务器 ACS（Access Control Server）：主要有两个功能，一是验证请求支付的某一个卡号是否在被允许参与 3-D 服务的范围内（通过注册取得参与 3-D 交易的权利）；二是对某一笔交易的持卡人进行认证或在认证无效时提供认证的证据。

收单域负责定义一个过程，以保证参与 3-D 交易的商家所有操作符合收单行的规定。收单行还要为合法交易提供具体的交易处理。收单域主要包括以下几个部分：

① 商家（Merchant）：通过已安装的交易软件处理交易过程，包括获取支付卡卡号、调用 MPI 引导进入支付认证过程、认证后向收单行提交授权请求等。

② 商家服务器插件 MPI（Merchant Server Plug-In）：创建和处理支付认证消息，并为商家交易软件返回相应的控制消息，验证这个控制消息里的数字签名。

③ 验证过程（Validation Process）：确认从 ACS 返回消息的数字签名，此过程也可以由 MPI 或其他机构完成。

④ 收单行（Acquirer）：金融机构成员。在 3-D 服务中，主要是与商家建立契约关系并为它们承兑支付卡，判断商家是否有资格参与 3-D 服务。

协作域利用一般的通信协议联系发卡域和收单域，并且共享 VISA 目录和 VisaNet 网络服务，使得整个支付流程能够顺利进行。协作域主要包括以下几个部分：

① 目录服务器（Directory Server）：每一次支付过程都通过该目录服务器接收商家查询某支付卡卡号的请求消息，判断这个卡号是否在合法的交易卡号范围内。将持卡人账户认证信息提交给适当的 ACS。ACS 的响应可以直接返回给商家，也可以由目录服务器接收认证响应消息，并由它返回给商家。

② 商业认证机构（Commercial Certificate Authority）：为使用 3-D 服务的实体发放特定的证书，包括 TLS/SSL 客户端和服务器证书等。

③ 方案认证机构（Scheme Certificate Authority）：为使用 3-D 服务的实体发放特定的证书，包括数字签名证书、支付方案所需的根证书等。

④ 认证历史服务器（Authentication History Server）：每一次支付过程都通过它接收向 ACS 发出的支付认证请求消息和认证结果（不管认证是否成功），并存储和记录这个消息。当收单行和发卡行发生争执时，可通过该服务器的数据记录进行仲裁。

⑤ 授权系统（Authorization System）：在支付认证通过后，授权系统（如 VisaNet）开始执行它的传统功能。从收单行接收授权请求，将这些请求提交给发卡行，将发卡行的响应返回给收单行，提供发卡行和收单行之间的清算服务。

根据规范，3-D Secure 的工作流程分为以下 10 个步骤：

① 购物者浏览商家网站将商品放入购物车，最后请求购买结算（此时商家已经获取所有必需的数据，包括卡号 PAN（Personal Account Number）和用户设备信息）。

② 商家通过 MPI 将 PAN 和可用的用户设备信息发送到目录服务器。

③ 目录服务器向匹配的 ACS 发出查询请求，验证 PAN 和设备信息是否合法（如果这时没有可用的 ACS 进行响应，则目录服务器会为 MPI 创建一个响应消息并跳到步骤⑤）。

④ ACS 向目录服务器发出响应消息。

⑤ 目录服务器将 ACS 的响应（或步骤③中自己创建的响应）回送给 MPI。如果 PAN

（和可用的设备信息）是合法的，那么 3-D 过程就继续进行下去；如果没有证据来证明 PAN（和可用的设备信息）是合法的，则 3-D 处理过程就终止。

⑥ MPI 通过购物者设备（如 PC 浏览器）将支付认证请求送到 ACS，ACS 生成认证消息 Web 页面并发到持卡人浏览器中。

⑦ 持卡人在认证消息框中输入认证信息，并提交给 ACS。

⑧ ACS 利用持卡人输入的信息鉴别购物者的身份，然后 ACS 会生成认证响应结果消息并签名。

⑨ ACS 通过购物者设备将认证响应结果消息返回给 MPI，同时 ACS 将其中特定的数据送到认证历史服务器并记录下来。

⑩ MPI 验证认证响应消息的签名，并将获得授权的交易信息提交给商家的收单行。最后，收单行和发卡行通过它们之间的授权系统（如 VisaNet）进行结算，并将结果返回给商家。

3-D Secure 工作流程示意图如图 20-11 所示。

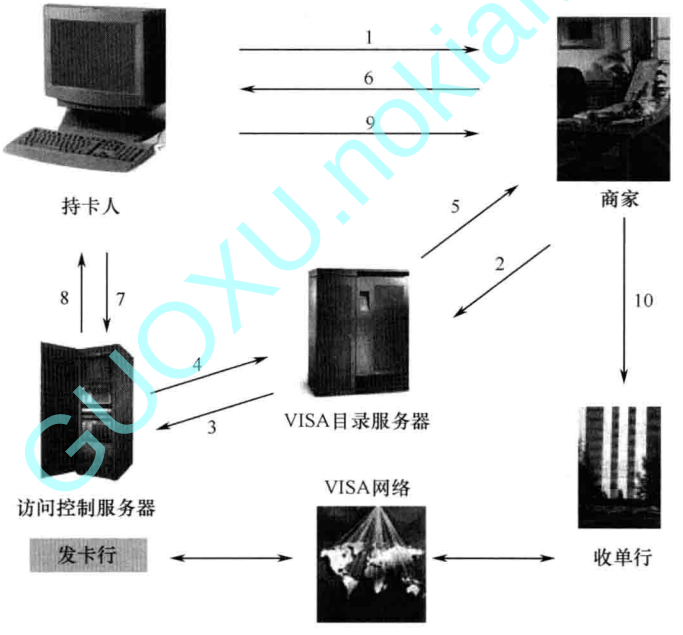

图 20-11　3-D Secure 支付流程示意图

20.7　WAP

WAP（Wireless Application Protocol）为无线应用协议，是一项全球性的网络通信协议。WAP 使移动互联网有了一个通行的标准，其目标是将互联网中丰富的信息及先进的业务引入到移动电话等无线终端中。WAP 定义了一种通用平台，将互联网上 HTML 描述的信息转换成用 WML（Wireless Markup Language）描述的信息，直接显示在移动电话的显示屏上。WAP 只要求移动电话和 WAP 代理服务器的支持，而不要求现有的移动通信网络协议做任何的改动，因而可以广泛应用于 GSM、CDMA、TDMA、3G 等多种网络中。

1. 访问模型

（1）WWW 访问模型

WWW 模型提供了易伸缩、功能强大的访问模型，如图 20-12 所示。应用和内容通过标准的格式进行提供，应用端通过浏览器进行浏览。

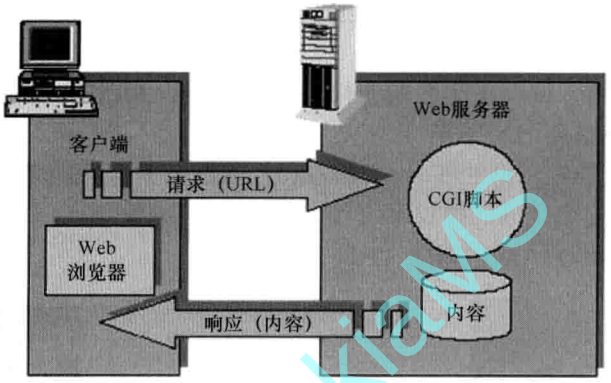

图 20-12　WWW 访问模型

WWW 协议定义了 3 种类型的服务器：

① 源服务器：资源驻留和功能创建服务器。

② 代理服务器：当客户机对服务器发起请求时，对客户机扮演服务器的角色，对服务器扮演客户机的角色。代理服务器通常处于无法直接通信的客户机和服务器之间，在 WWW 协议中，代理服务器必须既执行服务器又执行客户机的功能。

③ 网关：处理不同服务器之间的交换。

（2）WAP 访问模型

WAP 访问模型如图 20-13 所示，与 WWW 访问模型相似，这种相似性为应用开发者提供了极大的便利，包括熟悉的编程模型、已经证明过的结构和利用现有工具的能力（如 Web 服务器，XML 工具等）。为了适应无线环境的应用，已经对其进行了优化和扩展。

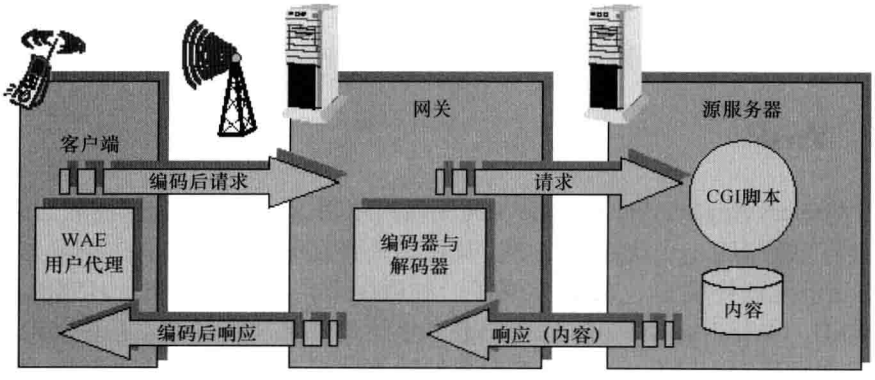

图 20-13　WAP 访问模型

WAP 定义了一组在移动用户终端和网络服务器之间通信的标准组件，包括：

① 标准命名模型：完成 WAP 内容的定位。

② 内容类型：所有的 WAP 内容以与 WWW 兼容的方式提供。

③ 标准内容格式：与 WWW 格式兼容。

④ 标准的通信协议：移动设备之间是兼容的。

WAP 的内容和协议是针对手持无线设备市场经过优化的，通过代理技术实现无线领域与 WWW 的连接，WAP 代理具有下列功能：

① 协议网关：完成从 WAP 协议栈（包括 WSP、WTP、WTLS 和 WDP）的请求到 WWW 协议栈（HTTP、TCP/IP）的转换。

② 内容编码和解码：将 WAP 的内容转化为紧凑编码格式以减少网络数据传输量。

通过使用代理技术，移动终端用户可以浏览大量的 WAP 内容，应用开发者也能开发出大量与具体终端无关的应用服务。同时，WAP 代理允许内容和应用驻留在 WWW 服务器上，并且采用成熟的 WWW 技术来开发应用。标准的模型包括 WAP 客户机、WAP 代理以及 WAP 服务器。但 WAP 体系结构可以支持其他的配置。比如，把 WAP 代理的功能包含在 WAP 服务器中，这样就可以实现客户与服务器之间安全的端到端连接。

2. 协议栈模型

WAP 是一个全球性的标准。1997 年 6 月，爱立信、诺基亚、摩托罗拉和 Unwired Planet（即现在的 phone.com）成立了 WAP 论坛，为基于 Internet 的各种服务在移动终端上的应用制定工业标准。同年 11 月，首次公布了该标准的结构。

1998 年 1 月，WAP Forum Ltd 成立，负责监督 WAP 标准的制定。WAP 论坛开始吸收新成员加入，以促进 WAP 在全球无线通信领域的应用和发展。1998 年 5 月，WAP 论坛推出了 WAP 协议的 1.0 版，1999 年 9 月，这一版本被更新的 1.1 版所取代，WAP v1.1 在 WAP v1.0 的基础上，增强了其兼容性和可互操作性，并参考 W3C（万维网联盟）新公布的 XHTML 协议对 WAP 协议的 WML 部分做了修改。随后，WAP v1.2 于 1999 年 12 月发布，增加了 WAP PUSH 结构这部分内容，在 WAP v1.1 的基础上，对 WTA（无线电话应用）部分做了一些补充，并增加了 WAP 可支持的承载网类型。

WAP v2.0 于 2001 年 8 月正式发布，它在 WAP 1.x 的基础上集成了 Internet 上最新的标准和技术，并将这些技术和标准应用到无线领域。这些新技术和标准包括 XHTML、TCP/IP、HTTP/1.1、TLS 等。在这些新技术的支持下，新增加了数据同步、多媒体信息服务、统一存储接口、配置信息提供和小图片等新的业务和应用，同时加强了无线电话应用、Push 技术和用户代理特征描述等原有的应用。这些新的业务和应用将会带来一种全新的使用感受，并极大地激发人们对无线应用服务的兴趣，从而推动移动互联网的发展。与 WAP1.x 相比，WAP 2.0 协议取消了 WSP、WDP，代之以 HTTP 和 TCP/IP。这种无线数据传输技术的改进带来了传输速率及传输可靠性的有效提高。

WAP v1.x 的协议栈模型如图 20-14 所示。WAP v1.x 安全性依赖于 WTLS 协议，通过 WTLS 实现传输层数据的机密性、完整性和通信双方的身份认证。WAP v1.1 并不提供不可否认的安全保护，即没有实现数字签名，无法做到不可抵赖性。WAP v1.2 通过 WMLSCrypt 提供签名机制来实现不可抵赖性。