

手机银行技术探讨

杨晓红 (山东财政学院计算机信息工程系 250014)

摘要: 本文提出了实现手机银行的两种技术方案,并分析了两种方案的可实施性和手机银行的安全性。

关键词: 手机银行 WAP STK

1 引言

Internet 和移动电话技术已经对我们的生活产生了前所未有的巨大影响。前者使我们能够方便且低成本地访问极大丰富的信息资源,后者则打破了通信对时间和空间的限制,两种技术的有机结合,提供了一种方便、快速、安全的移动商务平台,如手机银行和手机炒股,使网络能随身携带,使移动电话和其他无线终端用户能够迅速安全地获取互联网及企业内部网丰富的信息和其他通信服务。

金融业是现代社会的支柱产业之一,现代生活对金融业的服务形式和内容不断提出新的要求。基于无线互连技术的手机银行是一种全新的经营方式,与传统的银行柜台经营模式相比,它具有不受时间和地域的限制、主动式服务、交互性强、高效便捷、安全可靠、收费低廉的优点,随着手机的迅速普及,手机银行的未来应用前景是极为广阔的。

2 手机银行无线接入方案

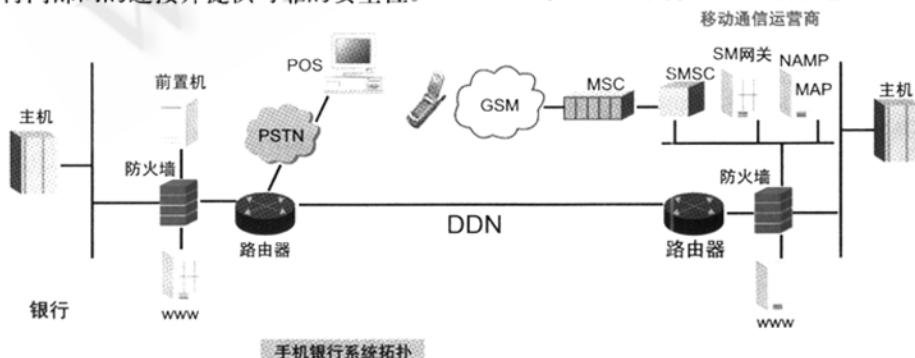
在当前技术背景下,手机接入方案主要有两种选择:WAP方式、GSM短信方式,两种方式与SIM卡技术结合,无须对现有银行企业内部网络架构和设备作大的改动,即可实现手机与银行内部网的连接并提供可靠的安全性。

SIM卡技术,在移动通信运营商端建立短信网关,与银行前置通过专线连接,移动运营商提供无线接入平台。手机银行交易流程为:银行前置实现接收短信网关转发的相关信息,进行业务受理,包括解密处理,用户认证,CRL检查,提交银行后台主机完成相关查询和交易业务处理,然后将处理结果加密后转发短信网关,通过短信中心发送到用户手机,手机用户解密后显示中文信息。

手机中SIM卡是基于智能卡技术,具有离线操作、能够加密解密等特性,为数据提供了可靠的安全性,同时其离线操作特性使手机银行成本低廉,容易为用户接受。

GSM短信方式要求手机支持STK(SIM Application ToolKit),STK是短信方式手机银行的关键技术之一。STK是一种小型编程语言的软件,可固化在SIM卡中,它的应用部分基于GSM规范,包括文件、数据结构、协议等规定,能够接受和发送GSM短信数据,是SIM卡和短信之间的接口,同时,STK应用软件可以通过OTA(Over the Air)机制下载到用户手机SIM卡上运行,使手机用户通过简单的中文菜单或编码命令交互式地进行各类功能选择和输入,轻松完成各类复杂信息检索和交易。

GSM短信方式实现手机银行业务,移动通信运营商应当提供的技术支持包括:为用户提供支持STK应用的SIM卡、写入银行RSA公钥和客户RSA私钥、写入或实



2.1 GSM 短信方式

这种方式利用移动通信公司的GSM短消息服务结合

时下载STK应用到SIM卡、确定各银行或券商等内容服务商英文简码或识别码(ID)的编码方案等。

GSM 短信方式的优越性在于: 银行和客户只需很少的设备投资(支持STK的手机只须更换一张SIM卡), 由于交易大多为离线操作, 故客户使用手机银行的费用低廉, 能覆盖全部柜台交易业务, 是目前情况下切实可行的方案。此方案的局限性在于SIM卡容量有限, 目前最大容量为32K, 64K卡正在实验阶段, 无法存放较复杂的应用, 而且一张卡只能存一个银行的应用, 这对于拥有多家银行帐户的用户来说是很不方便的; 此外, 它无法实现与Internet的真正连接以获取网上的信息资源。

2.2 WAP 方式

WAP (Wireless Application Protocol) 是一种新的无线互连通信协议, 其应用层包括无线标识语言(WML)、WMLScript和无线电话应用(WTA), WML是一种类似于HTML的浏览语言, 能实现浏览支持、数据输入、超级链接、文本、小图像及表格显示, WMLScript类似JavaScript, 使移动通信设备具有数据处理能力。

WAP手机银行的实现可以利用目前GSM语音通道(9600BTS)以CSD方式接入移动通信运营商端的RAS服务器, 通过WAP网关接入银行前置, 与STK不同的是, 这种方式可以通过WAP手机配备的微型浏览器, 真正实现手机上网, 使用户随时随地进行WWW浏览、收发E-MAIL和实时查看股市行情等。随着人们生活流动性的不断增大, 对实时信息服务需求的迅速增加, WAP方式将是未来手机上网的主流方式。

虽然WAP是一种理想的手机上网方案, 但目前在我国推广WAP上网仍然存在较大障碍, 最大原因是费用问题, WAP手机通过GSM网CSD信道连接, 在线操作, 信道利用率很低, 信道占用费高, 同时WAP手机价格也较贵; 其次WAP上网和通常所说的互连网有区别, WML网页格式与HTML不同, 必须为手机上网提供专门的网站, 因此在国内大多数地区WAP上网短期内难以形成大的发展。此外WAP手机的配置和使用还比较繁琐, 有待简化。

3 应用程序方案设计

无论GSM短信方式还是WAP方式实现手机银行, 固化或下载到用户SIM卡上的应用程序是银行与用户之间的接口, 它应当简单明了、操作方便, 使用户能够快速掌握, 并尽可能减少用户费用。可以采取两种方案设计应用程序。

3.1 命令编码方式

只要手机支持短信功能, 可不对SIM卡进行改造, 由银行和移动通信运营商共同对各种业务、名称进行编码,

用户通过输入编码命令完成交易。例如:

ZZ 转帐, ZH 帐号, 032-890013456

GP 股票, C 查询, 0001 深发展...

这种方法用户无须额外开支即可进入手机银行, 但需要记忆编码, 且输入信息较多, 易出错。

3.2 菜单方式

利用STK开发菜单式应用程序, 将其常用部分或全部加载到SIM卡上, 这样用户可以使用简单的菜单选择完成各种业务要求, 结合OTA技术, 可以实现对SIM卡菜单的动态增加、更新、删除。同时这种方法可以在应用程序中实现信息加密和数字签名, 提高交易的安全性。另外一种JavaCard技术能够在SIM卡上加载Java虚拟机程序, 手机用户可以动态实时地下载应用程序, 使手机真正像一台PC机。

这种方式用户需承担SIM卡更换费约200元左右, 花费不多, 获得超值服务, 应为首选方案。除上述两种方案外, WAP手机因具有很强的上网能力, 可以利用WWW浏览器和E-Mail完成业务处理。

4 手机银行的安全性

银行业务对数据安全要求极高, 手机银行在安全方面使用了多重加密机制, 以GSM短信方式为例, 首先银行帐户中设有交易密码, 可以进行用户身份认证, SIM卡中加载的应用程序可以在信息发送之前对其进行加密处理, 短信信道本身也有加密功能, 手机银行系统采用端对端的加密方式(发送端加密, 接收端解密)可以保证避免信息被非法截获, 另外短信息发送时间很短, 大部分时间是离线操作, 这些机制都能有效地确保手机银行的安全。

5 结束语

无线互连技术的发展使Internet应用进入了一个更深的层次, 为方兴未艾的电子商务注入了新的能量, 传统服务行业, 如银行、证券交易、航空订票等与这种新技术的结合, 将创建出新的经营模式, 更好地服务银行客户, 创造新的利润增长点。■

参考文献

- 1 湛力. 移动通信带来“无限银行”. 《网络世界》2000年 第24期
- 2 彭芳、盛安 “移动银行, 无线互连的一道大餐” 《网络 & 通信》2000年6月8日