基于信任传递的移动商务虚拟身份认证机制研究

王　亮◎著

经济管理出版社
ECONOMY & MANAGEMENT PUBLISHING HOUSE

本书出版得到王关义教授北京市属高等学校长城学者培养计划专项资助
（项目编号：CIT&TCD20140319）

基于信任传递的移动商务虚拟身份认证机制研究

王　亮 著

经济管理出版社
ECONOMY & MANAGEMENT PUBLISHING HOUSE

图书在版编目（CIP）数据

基于信任传递的移动商务虚拟身份认证机制研究/王亮著．—北京：经济管理出版社，2016.10

ISBN 978-7-5096-4616-8

Ⅰ.①基… Ⅱ.①王… Ⅲ.①电子商务—电子签名技术—研究 Ⅳ.①F713.363 ②N918.912

中国版本图书馆 CIP 数据核字（2016）第 225892 号

组稿编辑：陈 力
责任编辑：陈 力 舒 林
责任印制：黄章平
责任校对：王淑卿

出版发行：经济管理出版社
（北京市海淀区北蜂窝 8 号中雅大厦 A 座 11 层 100038）
网 址：www.E-mp.com.cn
电 话：（010）51915602
印 刷：北京玺诚印务有限公司
经 销：新华书店
开 本：720mm×1000mm/16
印 张：10.25
字 数：150 千字
版 次：2017 年 3 月第 1 版 2017 年 3 月第 1 次印刷
书 号：ISBN 978-7-5096-4616-8
定 价：42.00 元

前　言

移动商务作为一种以移动网络和移动设备为基础的电子商务模式，近年来在庞大用户群基础上和相关部门支持下迎来了井喷式发展，移动商务也在人们的日常生活中扮演着越来越重要的角色。移动商务的灵活性和便捷性更符合新时代电子商务的需求，但是也带来了一系列移动环境下特有的安全问题，而身份认证是解决这些安全问题最重要也是最直接的手段。通过认证移动商务参与者身份，可以确定与该身份相匹配的访问控制策略和授权，从而保证移动商务活动的安全运行。

在很多与支付和安全有关的移动商务场景下，均涉及“多方”而非“双方”参与，这些参与方可以是消费者、商家系统、支付平台或银行系统。在这种“多方参与”环境下，现行的主流身份认证机制是以跳转和多次认证为基础的，即消费者可能需要连续多次输入账号或口令等认证信息。随着移动技术的发展，移动网络和移动终端与普通桌面环境的性能差距正在逐渐缩小，而输入输出方式上的差距仍然存在。复杂的多次认证过程不仅大大降低了效率，同时也很容易主观或客观地降低用户的风险防范意识而遭受钓鱼、仿冒等攻击或个人隐私信息的泄露。因此，在“多方”参与的移动商务环境中，减少敏感信息输入和交换次数，是提高身份认证效率和安全性的重要方法。

上述问题可以用一种虚拟身份认证即“代理”形式解决，即消费者事先与支付平台或银行达成某种契约并预留安全令牌。在移动商务网站中进行结算行为时，消费者无须登录支付平台或银行系统，而是将预留安全令

牌通过加密处理发送给网站，网站作为代理将此安全令牌发送给支付平台或银行系统，经过验证，移动商务网站和支付平台之间即可进行无须消费者参与的结算活动。利用这种机制，可以使消费者不必在每次交易中登录支付平台或网上银行，整个移动商务过程会得到精简，交易效率和交易体验都会大大提高，受到钓鱼或仿冒攻击的风险则会大大降低。但是，这种机制也带来了新的安全问题，主要集中在如何防止来自移动商务网站的冒充重放和如何防止来自消费者的交易抵赖上。因此，本书主要内容就是构建上述虚拟身份认证机制并解决其带来的安全问题。

本书以多方参与的移动商务身份认证为研究对象，将着眼点从性能方面的改进转移到流程方面的优化，以安全基础上的便捷轻量化和信任传递基础上的虚拟身份认证机制为研究主线，按照“可行性研究—概念设计—逻辑设计—仿真实现”的研究思路，首次提出“基于信任传递的移动商务虚拟身份认证模型”，并充分考虑移动商务中的用户需求和安全需求，在模型基础上建立了多种基于当前主流身份认证技术的可行性方案、框架和实现流程，最后进行仿真系统开发和结果分析。基于上述工作内容，本书主要贡献和创新有：

(1) 系统地研究了移动商务身份认证的相关理论和技术，对典型身份认证机制的问题进行了分析，提出了移动商务中安全与流程复杂度的关系，构建了移动商务安全框架，在框架基础上分析移动商务的安全需求和面临的主要威胁，最终提出移动商务安全策略。

(2) 首次提出针对多方参与移动商务的“基于信任传递的虚拟身份认证”概念模型。首先通过问卷调查获取一手数据，分析模型的用户接受度，以确定其可行性和应用价值；然后定义信任域、信任联盟、契约、安全令牌、直接信任、间接信任等概念，基于概念提出了模型工作原理及各个工作环节中的输入、输出、存储和过程；最后根据信任的传递构建了虚拟身份认证机制。该模型将多方参与的身份认证过程简化为双方参与的身份认证过程，同时提出信任的建立、授权、存储和维护规则，以保证虚拟

身份认证过程的安全。

(3) 从实际应用角度对概念模型进行了实例化并形成了多种逻辑设计方案。逻辑设计方案分别采用不同的主流身份认证技术，一方面保证逻辑设计方案的可用性和兼容性，另一方面通过对比得出采用不同身份认证技术的逻辑方案的特点和适用环境。包括：基于动态口令的 DPVA 虚拟身份认证方案、基于数字签名的 DSVA 虚拟身份认证方案和基于可信第三方认证中心的 CAVA 虚拟身份认证方案。最后利用信息系统仿真方法分析、设计和开发了原型系统，用于验证逻辑方案的可实施性、功能和性能。

目　录

图表目录

1 绪 论

随着电子商务活动逐渐由桌面领域向移动领域渗透，移动支付在人们日常生活中的使用频繁程度也越来越高。移动支付的灵活性和便捷性更符合新型电子商务的需求，但是也带来了一系列安全问题。

身份认证是解决移动商务安全的最重要也是最直接问题，通过验证移动商务参与者身份，可以确定与该身份相匹配的访问控制策略和授权，从而保证移动商务活动的安全运行。

1.1 研究背景和意义

近年来，移动商务市场规模飞速增长。2014 年，我国移动智能终端用户规模达到 10.6 亿，环比增长了 231.7%。而在移动商务应用中，购物、缴费、订票和投资理财等涉及支付和信息安全的应用比例越来越大。根据国家工业和信息化部提供的相关数据，2013 年，中国移动商务参与者已达 367.6 万人，移动支付总成交金额已达 1006 亿元。2014 年底，支付宝（Alipay.com）公司也发布了其当年的支付业务情况报告。报告显示：移动支付业务已占其总支付业务的半数以上。在 2014 年 11 月 11 日，通过移动设备进行支付的业务就有 1.97 亿笔。由此可见，移动支付已经有了相当大的用户基础和使用量，并且正在飞速扩张。

虽然移动商务具有无比广阔的发展前景，但如其他快速扩张的新兴事物一样，快速发展必然产生一系列不可预知的新的问题，“安全问题”就是这一系列问题中最重要的问题之一。从广义讲，移动商务属于电子商务的一个分支，和桌面电子商务相比，移动环境更加开放，手机和平板电脑等移动终端在软硬件扩展防护功能上更加局限，因此移动商务不仅要面对从桌面商务继承过来的安全问题，还要面对其自身所特有的安全问题。安全问题中最基本的元素是身份认证，通过密码学理论和实践，身份认证技术可以正确识别商务参与者身份。移动商务活动的主体是参与者，验证主体身份并赋予相应的权限是保证商务活动顺利进行的重要条件，如果没有完善的身份认证机制，安全的管理和控制将无法完成。

当前，移动支付的身份认证参与者主要包括消费者、商家、支付平台和银行，如图 1-1 所示，其交易流程可以简化描述为：

（1）消费者使用移动设备浏览商家网站并产生订单。

（2）商家利用加密和数字签名等技术将订单号、订单信息发送给支付平台进行交易请求。

（3）第三方支付平台验证商家信息并解密来获取订单信息。

（4）订单信息确认后，第三方支付平台向顾客发起支付请求。

（5）顾客确认订单信息后登录支付平台，通过支付平台与银行接口登录到银行支付系统并完成支付。

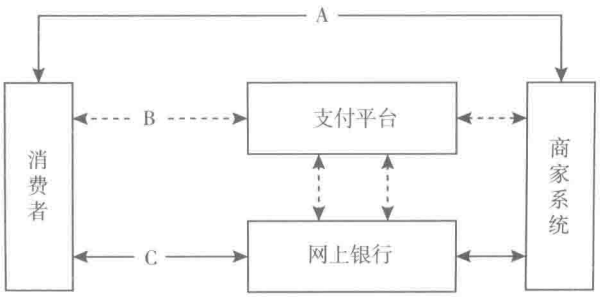

图 1-1　移动支付参与者

由图 1-1 可知，消费者在完成交易过程中，可能会经历 3 次登录过程，分别是：

A：消费者登录商家网站。

B：消费者登录第三方支付平台。

C：消费者登录银行支付系统。

这种烦琐的支付流程不仅不利于移动商务本身对于便捷性的要求，更可能会在复杂的过程中产生信息泄露、钓鱼攻击等严重的安全问题。由此可见，如能解决移动支付过程中的跨域单点身份认证问题，即使移动支付参与者之间建立起传递信任关系、将多方参与的身份认证过程在用户端视角上简化为双方参与的身份认证过程即可解决上述安全问题。

本书旨在利用信任和信任传递理论，构建一个基于信任传递的虚拟身份认证模型，并分别设计多种环境下的虚拟身份认证方案。此方案改进了多方参与的移动商务身份认证流程，消费者首先与支付平台和网上银行系统达成某种契约并预留安全信息。消费者在商家系统中进行购物结算行为时，无须登录支付平台或网上银行，而是将预留安全信息通过加密处理发送给商家系统，商家系统将此安全信息发送给支付平台或网上银行，经过验证后，支付平台或网上银行确认该支付请求是由消费者产生的，从而达成交易。

在改进流程中，由于消费者无须在每次交易中登录支付平台或网上银行，整个移动商务过程会得到精简，其交易效率和交易体验都会大大提高，受到钓鱼和仿冒攻击的风险则会大大降低。

1.2 国内外研究现状

1.2.1 无可信第三方的身份认证

无可信第三方的身份认证泛指仅仅通过交易双方的协商、信息交换和判