ISSN 1000-1239/CN 11-1777/TP
50(2): 291-301, 2013

一种终端认证简化的在线移动支付模式与协议

王红新[1] 杨德礼[1] 姜 楠[2] 马 慧[1]
[1](大连理工大学管理科学与工程学院 辽宁大连 116024)
[2](大连民族学院计算机科学与工程学院 辽宁大连 116024)
(wanghongx@263.net)

An Online Mobile Payment Model with Simplified Terminal Authentication

Wang Hongxin[1], Yang Deli[1], Jiang Nan[2], and Ma Hui[1]
[1](*School of Management*, *Dalian University of Technology*, *Dalian*, *Liaoning* 116024)
[2](*School of Computer Science and Engineering*, *Dalian Nationality University*, *Dalian*, *Liaoning* 116024)

Abstract Mobile payment is an important and core application of information safety technology in mobile Internet, and the mobile terminal authentication is the important issue needing to be solved first in mobile payment. In order to meet the special requirement of mobile payment, such as mobile terminal resource constraints from portable needs and mobile terminal update acceleration from more and more rich personalized needs, the steps of terminal authentication need to be as simple as possible, the dependence on equipment needs to be as little as possible, and the customer's operation experience also need the authentication to be as simple as possible. So there should be a simplified and independent of equipment's terminal authentication. Therefore, a mobile payment model with simplified terminal authentication is introduced. The model is designed based on the "pre-trust" hierarchical certification model and the payment system framework with a character of "public-service-domain". To achieve the purpose of controlled system safety and simplified terminal authentication, a credit transfer chain starting from merchants is built, as well as an account addressing and management mechanism are designed. Meanwhile, related research review, system framework, authentication model and corresponding payment protocol are given. Furthermore, the security of the protocol is analyzed.

Key words mobile terminal authentication; public service domain; payment model; mobile payment protocol; payment security

摘 要 信息安全技术在移动互联网中最重要的应用是移动支付,移动终端认证又是移动支付首先要解决的问题.移动支付的特殊性要求移动终端的认证要尽可能简单并对设备的依赖性最小,为此提出终端认证简化的移动支付模式.该模式建立在基于"预信任"的分层认证模型与公共服务域为特征的支付系统架构上.通过建立商户为起点的信任传递链以及公共服务域中的帐户寻址与管理机制来实现系统安全可控及终端认证简化的目标.给出了相关研究综述、模式的系统架构、认证模式以及相应的支付协议,并对协议的安全性进行了分析.

关键词 移动终端认证;公共服务域;支付模式;移动支付协议;支付安全

中图法分类号 TP393

收稿日期:2012-01-08;**修回日期**:2012-09-20

基金项目:国家自然科学基金重大项目(70890080,70890083);国家自然科学基金项目(70672092)

支付是任何商业领域的助推器[1],购买的产品与服务都必须支付[2],移动支付是移动互联网与移动电子商务重要而核心的应用.

移动支付系统由下面的主体组成:客户(移动设备与卡持有者)、WPKI、商户(产品或服务的提供者)、银行与代理[3](如图 1 所示).其中代理可以是非银行第三方支付服务机构、MNO(mobile network operator)、支付网关、其他中间服务商或产生移动 AGENT 的服务器.

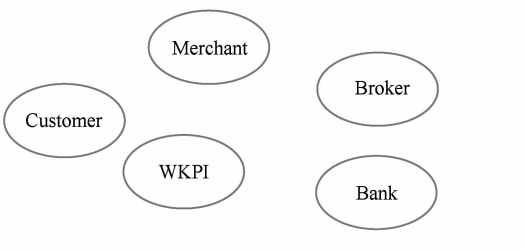


Fig. 1 Entities of mobile payment system.

图 1 移动支付系统主体构成

要在广袤的互联网空间实现交易者相互不能面对面地在线电子商务及支付,支付各主体之间的认证成为最重要的核心问题[1].只有实现正确的认证,才能保证资金从正确的付款方流向正确的收款方,而这正是支付活动正确完成的最重要标志.

支付主体间网上相互认证方案有多种,各自有不同的认证流程、认证次数与认证方法,它取决于支付系统架构、主体之间的关系、业务流程以及所采用的安全技术与协议.与桌面互联网环境不同,移动互联网环境下,由便携需求带来的移动终端资源受限以及客户越来越丰富的个性化需求带来的移动终端更新加速,需要终端的认证步骤尽可能简单,对设备的依赖尽可能少,客户的操作体验也需要认证的简化.为此,我们提出终端认证简化的移动支付模式(mobile payment model with simplified terminal authentication, MPSTA).

终端认证简化意味着后端安控的加强.MPSTA 以基于"预信任"的分层认证模型及各种安全技术解决商户以及各代理平台(中介)之间的认证与信任问题,解决支付信息安全传递问题;用"公共服务域"中的帐户寻址与管理机制保证不可否认性并防范支付风险.二者结合生成移动支付信任链及各主体间的约束机制,最终可达到支付安全可控及移动终端认证简化的目的.在 MPSTA 中,终端只与付款帐户(可选择的)所在支付机构认证一次且不必认证其他任何主体(包括商户);除存储私钥外,终端不必存储任何支付帐号及其他敏感信息.这种简化的且与具体支付机构具体设备无关的模式可以有效降低支付终端的运行开销及生产设计开销,并可以很好地防范支付欺诈与风险.

1 相关研究

已有大量对移动支付模式及认证模式的研究.如文献[4-9],因设置不同的支付代理或中介,给出不同银行网关方案而具有不同的支付系统架构,也具有不同的主体认证方式.在这些方案中,移动终端与各主体认证不只一次.在大多数方案中,终端不但要直接与支付机构(银行或非银行支付机构)认证,还要与商户认证[1,3]、与支付网关认证[8]甚至与其他中介平台或代理认证[7].支付流程在主体间是交叉的、反复的、网状的,而不是流线型的.有些方案如文献[3]为了使终端能与商户认证还增设专门的代理服务器.还有些方案如文献[10]将支付网关作为对所有主体的认证中心,所有主体间的信息交换须经过支付网关,每交换一次认证一次,流程复杂.典型的欧盟移动支付系统 SEMOPS[4],其移动支付架构使用户与商户只与自己的支付机构(开户银行或 MNO)直接相联并相互认证,但认证次数不止一次,且由于支付指令之外的商务信息也必须通过支付机构传递,给银行带来额外的信息处理负担也不符合信息保密要求.更重要的是这种架构难以包容新的中介服务.所有创新与增值服务除非由银行担当,否则不能实现,不利于支持网络商务的不断创新.

文献[1,4,11-13]对建立国家与地区级的公共移动支付数据服务进行了研究,对其必要性与可行性给出论述.应用的典型案例还是欧盟 SEMOPS,建立全国及多国共用的银行帐户寻址数据库 DC,结合国家与地区的银行间清算系统保证支付的通用性与数据安全.MPSTA 的"公共服务域"参考了这种结构并在其上进行了改进(见 2.1 节).

SET 协议[14]与 3-D Secure 协议[15]是目前应用最广泛的电子支付协议,由 Master 和 Visa 联合 Microsoft 等公司推出,用于世界各地的信用卡及互联网交易,中国银联也加入其中.但这两个协议还没有移动支付版本,且存在其他不足.尤其 3-D Secure 协议中,商户的认证依靠目录服务器,商户必须是信用卡公司的特约商户,这不适于更普适的基于帐户

(不限于信用卡)的电子支付.事实上目前大量已运行的互联网支付系统(支付宝、PAYPAL、苹果手机支付等),对商户的认证采用了分层认证模式,先是由商区/社区(如淘宝、苹果商务平台)完成对商户的第1级认证,再由支付网关对商区等中间平台完成第2级认证,这些认证又以线下信任为保障基础.这种机制强化了网上主体与现实信任的联系,使线上认证可与现实世界的制约机制联系起来,提高了认证的可靠性.MPSTA研究并提练了这种认证机制并在其上改进,使之可以适应更广泛的应用场景并适于移动支付.

关于认证密码机制与认证技术已有大量研究,最典型的网络认证建立在PKI与WPKI机制的基础上[16].所有的网上客户、商户、中间服务商均预先在CA(certificate authority)处经认证获得电子证书,线上认证靠验证对方的电子证书或电子签名实现.但这种方案带来了大量证书传递与验证开销.基于身份ID的密码技术可以避免常规公钥基础设施(PKI)中为公钥的检验去使用证书的问题[17],近几年得到广泛应用.移动通信的短信通道用于身份认证也在实践中广泛应用,部分银行与第三方支付平台(如中国工商银行、招商银行、PAYPAL、银联支付)已采用短信通道实现客户授权与认证,前提是必须保证短信源号码不可篡改.其他认证技术也在实践中使用,有些采用了除SIM卡外再在终端配置支付专用卡的方法(如EMPS[1]等),有些还采用手机U盘接口或磁条卡接口(长沙银联等),需要用户在手机上物理刷卡或插入U盘,给用户带来不便并增加了手机成本.

不少支付协议采用多种安全技术,除基于身份ID的密码方案[17]外,还有盲签名算法[18]、不可信前提下的传递机制[8]、保证不可否认性的交易证据提取、保留及争议解决机制[3,19].根据商务原子性理论[20],支付信息PI(payment information)需要与商务信息(如电子订单、电子合同)捆绑,而根据信息保密需求(要保证商户永远不知道信用卡信息;而金融机构永远不知道订单信息[3,10]),商务信息又需要与PI分离.要同时满足就需要将商务信息与PI分别打包又使之相互关联.这些研究都给我们很好的启发,也应用在MPSTA下的支付指令传递模型与支付协议中,使之较好地满足了电子支付安全的5个主要标准,即可认证性、授权性、完整性、保密性、不可否认性[16].

2 终端认证简化的在线移动支付模式

2.1 MPSTA基本架构

MPSTA基本架构如图2所示:

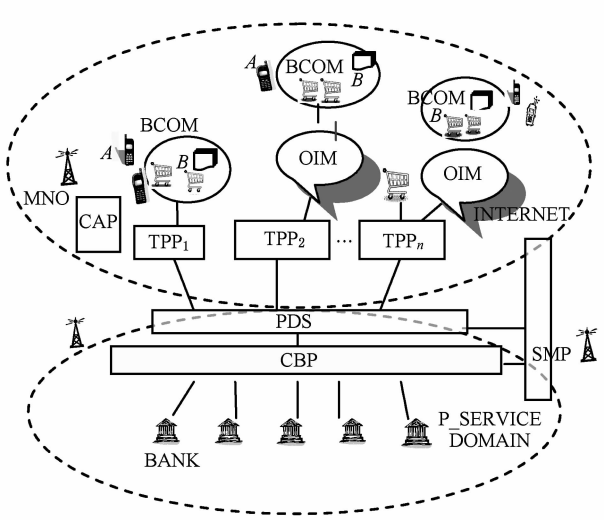


Fig. 2 Main structure of MPSTA.

图2 MPSTA基本框架

图2中,A为手机客户(付款人);B为商户(收款人),可以是任意产品或服务供应商;BCOM为商区或社区,即B所在的商业平台;TPP为有资质的非银行第三方支付平台,这里的"有资质",指经权威机构认证的具有良好信誉与所需能力的第三方支付服务机构,在中国即经央行批准的非银行支付机构;PDS为支付数据服务中心,提供银行帐户寻址服务.即可根据用户手机号、商户ID(或名称)与各银行帐号的绑定关系,将用户手机号及商户ID号转换成真正的银行帐户信息,如帐号、帐户名等;CBP为跨行支付平台,联通所有银行的银行间支付与清算平台(如国内的CNAPS,CUPN[21]);CAP为证书与密钥发行平台,提供第三方可信的证书发行与基于身份密码方案的密钥发放;SMP为争议管理平台,接受争议解决申请,调用在TPP与PDS存储的交易证据送专门的仲裁机构;OIM为其他中间代理,可以是一个或多个,它是可变化的,也是可包容各种电子商务创新服务的部分.

整个架构将移动支付分成互联网域与支付公共服务域PA.支付公共服务域由PDS,CBP及所有的银行组成,构成支付服务云.公共服务域参考了SEMOPS[4,11]的架构.只是不再要求客户与商户只能直接与自己开户银行联接,而是可以通过各种中介去间接与之相联,也为互联网上的商务创新与支付

创新留下充分空间.

PDS 成为互联网域与支付公共服务域 PA 的交界面,一面联接(且只联接)主要的第三方支付服务商 TPP;一面联接银行系统的跨行支付平台 CBP,解决所有应用(通过 TPP)与所有银行的多对多联接问题,也构成互联网与银行网络之间的安全屏障.

PI 传递路线按图 2 中各主体的关联路线,即从 $A \rightarrow B \rightarrow$ BCOM $\rightarrow$ OIM $\rightarrow$ TPP $\rightarrow$ PDS $\rightarrow$ CBP $\rightarrow$ BANKS.

2.2 实现目标的主要设计思想

要实现终端认证简化的目标,主要思路是将安全控制后移[22],同时采用各种方案使终端与各主体以及各主体间的信息交换次数降到最低,使认证关系与信息传递路径成为单向单线型链条而不是复杂的交叉结构.在这种链条中,不只是终端客户,所有参与主体都只与相邻的节点认证一次.主要有以下 3 种方法:

2.2.1 以基于"预信任"的分层认证模型建立单向线型 PI 传递链与单向认证链

支付处理可分为两大任务,一是支付(信息)的产生与传递,二是支付授权与执行[23].在开放网络中传递 PI 需要对传递主体进行认证,支付授权也需要对支付主体认证.一般协议将上述两大任务中的认证放在一起交替进行,由于信任关系与认证权力的不同(如 3-D Secure 中 ACS 要求商户由目录服务器认证,付款人只能由付款行认证,而授权只由商户向收款行发起)加上 PI 传递中相邻节点需相互认证使各主体的认证出现交叉、往复与复杂化.考虑移动终端的特点与当前电子商务中商户认证的特点,我们将终端客户的认证、授权与商户及其他主体的认证分开,将其剥离出来,使整个支付过程由两个阶段两条路径组成,一是 PI 生成与传递路径,二是付款人认证与授权路径(空中路径,见 2.2.3 节).第 1 路径的起点为商户,终点为支付机构(非银行支付时为 TPP_I,银行支付时为 PDS),通道为地面网,主要任务仅是 PI 传递以及对商户的认证.对商户的认证不再靠专门的服务器(如 3-D Secure 的目录服务器)或终端与银行(如 SET 协议、SEMOPS 协议)而是商务信任关系的上级.上级再向上一级传递,一层认证一层,一层信任一层,直到支付机构.PI 一直传递在有"预信任"关系的链条中,加上 2.2.2 节的方案,使商户真实性与 PI 的安全性得到保障,也使 PI 传递链成为单向线型传递链,各主体间的认证关系成为单向.

MPSTA 将"预信任"定义为:本次交易前主体间预先存在的信任关系,它包括线下认证以及相应的信任机制约束机制.

"预信任"关系是电子商务普遍存在的关系,如现实中商户大多数处于商区(社区)中,商区对商户具有事前线下认证与约束关系(如淘宝对其商户);商区及中介服务与某些第三方支付机构有线下认证与约束关系(如淘宝与支付宝);TPP 与 DPS,DPS 与 CBP 更是如此,它们之间是安全的地面专线网或安全的银行专网.充分利用这种关系可以使网络环境中的认证得到简化,这一结论已经在多篇论文[17,24-25]中得到阐述,也在互联网支付的实践中得到检验.

MPSTA 基于"预信任"的分层认证模型指:认证沿着 PI 传递链,只在有"预信任"关系的主体中传递,随着传递链的层次关系一层认证一层.传递链中每相邻的两个主体在现实世界中都具有信任与制约关系,信任关系最终以电子证书的方式预存在这些相互信任实体的服务器中.

即 MPSTA 将认证分为事前实体相互认证与事中电子认证,如图 3(其中,IB 表示付款行,AB 代表收款行):

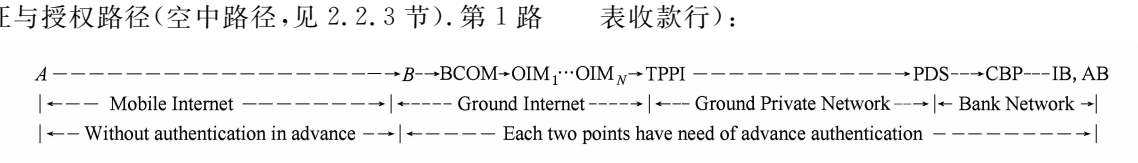


Fig. 3 Authentication chain of MPSTA.

图 3 MPSTA 认证链

线上认证的最终目的是保证虚拟空间交易各方的真实性,将其与真实空间的身份联系起来,使交易行为具有可追溯性、责任可区分性[10,16].MPSTA 基于"预信任"的分层认证模型正是满足了这一点.

MPSTA 的信息传递链如图 4 所示(带有钥匙的空中路径也是第 2 路径),各主体认证方向与路径如图 5 所示.PI 生成后整个传递链是单向的,认证关系也是线型的,而不是交叉或网状的.传递路径中每一步只需前一节点对后一节点认证,直到支付机构转过来对客户认证,构成一个认证闭环.

认证链中每一个节点既是认证者(对信息发送节点)也是被认证者(对于信息接收节点),每笔支付

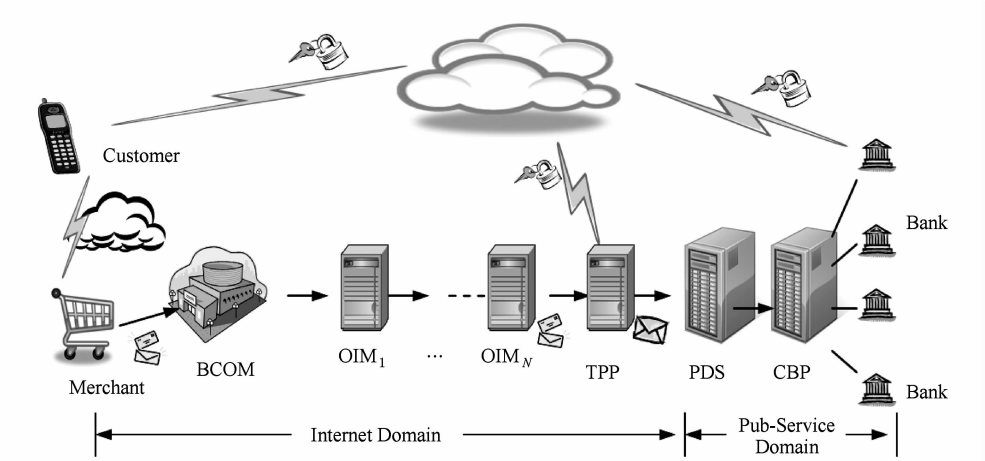


Fig. 4 The transfer path of payment information.

图 4 支付信息传递路径

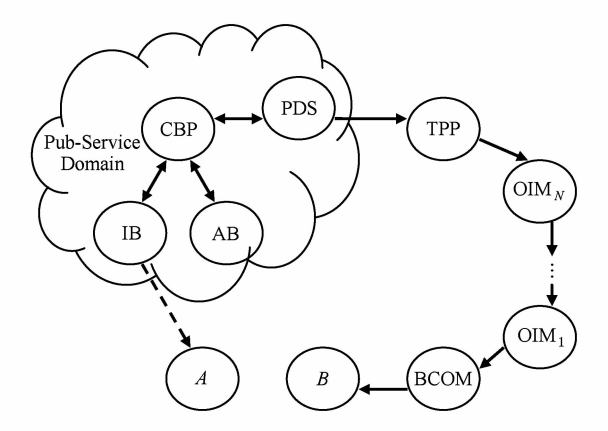


Fig. 5 Authentication relationship of every part.

图 5 各主体认证关系图

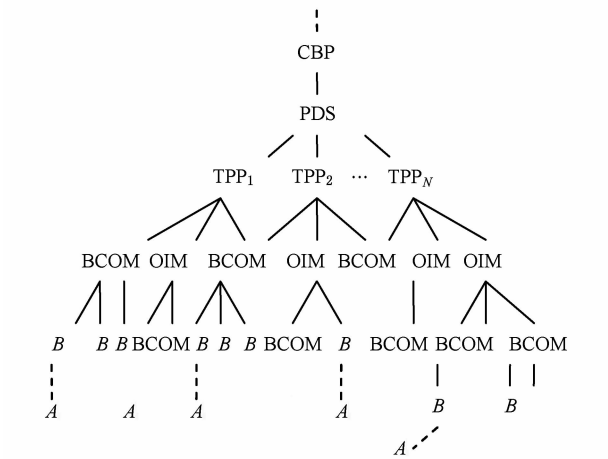


Fig. 6 Relationship of authenticating in hierarchy.

图 6 分层认证关系

中每个传递节点只执行一次认证.客户与商户之间不必相互认证.

分层认证机制还可形成支付系统认证空间逐级缩小的结构,用户一旦选择了商户,整个后续的搜索空间就变得有限与清晰.每个上一级节点只对信任圈中的下一级节点认证且搜索空间逐级缩小.如商区只对所属商户进行认证,中介对所接入的商区认证,TPP 对各种中介服务认证,最终使 PA 中的 PDS 只须对有资质的 TPP 进行认证(最多百来个),大大减轻了 PDS 的接入压力与认证压力,达到安全可控的效果(如图 6 所示).

与一般认证模式相比,有"预信任"的分层认证模式还由于信任关系的预存省去了证书传递及追朔证书链的步骤,使线上认证得到进一步简化.

2.2.2 以"公共服务域"中的帐户寻址与管理机制防范支付风险

"公共服务域"处于整个支付传递链的后端,除担负支付的最终实现外还对前端传递链起检测与监督作用.每笔涉及银行的支付都在 PDS 与 CBP 留下记录.PDS 的帐户寻址功能既可使互联网域中不必传递银行帐号等敏感信息(只传递手机号及商户 ID,利于保密,便于用户操作),又使每个商户的收款帐户处于可监控状态(只有经银行或 PDS 临柜认证的商户才可在 PDS 注册,只有注册的商户才能得到银行系统的互联网支付服务),从而完善了 PDS 代表的公共服务域对 PI 传递链信任的建立(在对 TPP_1 信任的基础上).这个信任是商户生成的 PI 信息可以进入银行系统并传递到付款行的关键.

建立国家级的公共服务域还因其公信力带来系统可信性与可接受性[26],使支付协议与流程的设计得到最大程度的简化.

公共服务域还对跨银行服务提供了最大的便利.只要将载有选择不同银行、不同支付方式的支付指令送到 PA,则无论选择了哪一个银行,哪一种

支付方式都可以得到有效传递与执行.

2.2.3 以基于手机绑定帐户的两因素认证模型简化终端认证操作

“在计算机领域,用户的身份认证被定义为3个方面:有什么、知道什么以及是什么”[27]. 如信用卡认证中,用户持有的信用卡解决“有什么”,口令对应“知道什么”,客户手写签名回答了“是什么”或“你是谁”[28]. 由于手机的私用性、号码的唯一性及信息接收的可定向性,将其与银行帐户绑定就可以起到信用卡类似的作用. 信用卡与手机认证的关系如表1所示:

Table 1 Authentication Factors Comparison in Credit Card Payments and Mobile Payment

表1 信用卡支付与手机支付认证要素比较

Payment Model	What You Have	Action to Connect Account	ID to Connect Account	What You Know	What You Are	Stolen or Lose Coping
Cards Payment	Cards	Swing Card	Magnetic Stripe	Password	Autograph	Report the Loss One by One
Mobile Payment	Mobile Phone	SMS or WAP	Mobile Phone Number	Password or PIN	Autograph on Screen	Report the Loss Synchronously

一般情况下,三因素也可简化为两种[28-29]. 据此,MPSTA主体认证采用下述方法:

1) 对终端用户的认证

MPSTA用短信通道实现支付机构对终端用户的认证. 支付机构发短信到帐户绑定的手机(有什么),用户在回复短信中输入密码(知道什么),还可以在智能机彩信中回送手写签名(是谁). 而客户靠识别短信显示的支付机构特服号码确认短信的来源. 短信通道也可以应用动态口令技术、令牌技术、验证码技术.

由于对终端客户的认证是在第1阶段PI传递完成后才开始,此时付款行已经收到了PI信息,因此付款人认证与授权可一次性完成.

2) 其他各主体的认证

有什么:加密软件、加密卡或其他(因为除客户外的主体都有预信任关系且都处在地面网中,可以实现预先的各种安全配置与约定). 知道什么:会话密钥、签名密钥. 是什么:IP地址及其他.

各主体只要在支付发生时用预存的对方(相邻的信息发送方)公钥进行签名验证. 每两两认证主体的密码方案与CA中心均可不同,只要双方预先协商确定.

客户与商户协商结果(订单与PI)的传递采用基于身份ID的密码方案. 用户手机上只存自己的私钥与基于公开密钥算法的电子签名验证模块. 私钥用于客户对订单与PI的签名以及解密商户传来的信息. 商户传递自己的公钥给客户,客户只使用但不验证,也不到CA查询其可信性.

3 支付流程与协议

以手机网络购物为例.

3.1 基本符号表示

本文综合文献[1,10]等协议的形式化描述和分析方法.

X:主体 X.

M:主体间发送的消息.

KX:主体 X 的公钥.

KX^{-1}:与 KX 对应的私钥.

$[M]_K$:用密钥 K 对 M 进行非对称加密后的密文.

$Sign_X(M)$:用 X 的私钥对消息 M 进行数字签名;这表示完成了下述过程:X 用自己的私钥对 M 的摘要(散列函数 $H(M)$)进行加密.

$Verify_X(Sign_X(M))$:用 X 的公钥对 X 的签名验证. 是签名的反过程. 这表示完成下述过程:用 X 的公钥解密 $Sign_X(M)$,得到 M 的散列值 $H(M)$;再对原始信息 M 取散列值得到 $H(M)'$,如果 $H(M)$ 与 $H(M)'$ 相等,则说明数据传输正确并且信息确实是由 X 发来的.

$Evid(M)$:将 M 作为证据. 它等于 $[F, M]_{KA}$. 其中 $F=[Sign_B(M)]_{KA^{-1}}$,是 A 与 B 的双签名. 用 KA 加密 F 与 M,使之被封装起来,传递与存储中不能被任一方打开,只有争议时在 A 的参与下才可以打开.

$KX[M]$:用 X 的公钥对 M 解密.

$Store[X]_Y$:在 Y 节点存储信息 X.

PPO:初始支付指令,$PPO=\{NO; ANM; BID; PID; SUM\}$. 其中,$NO$ 为交易编号;ANM 为付款人 A 的手机号;BID 是收款人-商户的标识,具备唯一性,由简称及商户ID组成;PID 为用户 A 所选择的要完成付款任务的支付服务机构ID. 支付机构范围包括CNAPS所覆盖的所有银行(国内、国外)以及央行批准的所有非银行第三方支付服务机

构,ID 是全国统一编码(已有);*SUM* 为支付金额.

PX:客户订单(本文也指其他商务合约),*PX*={*NO*;*CNAME*;*CINF*;*CP*;*CNUM*;*ANM*,*BID*}.其中,*CNAME* 为商品名称;*CINF* 为商品信息可以含外观、型号、品牌等;*CP* 为商品单价;*CNUM* 为商品数量;*NO*,*ANM* 与 *BID* 与上同.商品可以是多种.

PPI:银行可执行支付指令,*PPI*={*IN*;*RN*;*SUM*}.其中,*IN* 为付款人银行帐号;*RN* 为收款人银行帐号;*SUM* 与上同.

以上 *PPO* 与 *PX* 中的 *NO* 相同,保证两者的关联性.*NO* 为 *PPO* 生成时刻的函数.

协议假定:对移动用户 *A* 的认证采用基于身份 ID 的密码算法[17],即各商户可以根据用户的手机号及标识生成用户 *A* 的公钥;用户 SIM 卡存有用户自己的私钥(而不必存储任何客户帐号与银行证书等敏感信息);用户与 SIM 卡绑定,与手机号绑定(不是与手机设备绑定);手机制造商或运营商有技术措施保证 SIM 卡的唯一性、不可复制性,保证 SIM 卡中的密钥不可非法读出,保证短信来电号码不会被篡改.

3.2 流 程

1) 客户 *A* 在手机上与商户 *B* 的网页交互,形成订单(如将所有欲购物品放入购物车),一旦最终决定支付,在选择"银行支付还是第三方支付","哪个银行""哪个第三方支付"以及"哪个帐户"(用别名)后,按下支付确定键.

2) 商户网页接收支付确认,根据"购物车"生成订单 *PX* 与初始支付指令 *PPO*,分别签名后送 *A*.同时向 *A* 送出 TPP 的公钥(非银行支付下 TPP 由用户选择,否则由 *B* 选择)以及 PDS 的公钥(银行支付时).

3) *A* 接收信息,解密、验证并核对订单与支付信息(*PX* 与 *PPO* 将在移动设备上显示出来),确认则对 *PX* 进行 Evid 操作,用 KTPP(当非银行支付)或 KPDS(当银行支付)加密 *PPO*′(*PPO*′=[$Sign_A$(*PPO*),$Sign_B$(*PPO*),*PPO*])构成加密信封,再与 *PX* 证据一起用 TPP 公钥加密构成 2 级加密信封,签名后送 *B*;否则不签名,选择"修改",交易再开始回到第 1)步.

手机存储 *PPO*,可用于以后对银行支付通知的自动核对.

4) *B* 验证是 *A* 所发,将信封盲签名后转发商区 BCOM. *B* 同时向 BCOM 发送 ID_{TPP},对后续整个传递链提示传递目标;发送自己的标识 *BID*,便于支付机构对盲传递信息的验证(防止手机端对收款人的更改).

5) BCOM 验证 *B*,将 *B* 的信息盲签名后转发到自己信任的、且可以有路径到达 TPP 的节点 OIM_1.

6) OIM_1 验证 BCOM,而后将信息盲签名传递到自己信任的下一个有路径到达 TPP 的 OIM_2,以此类推,每一次传递都是后一节点验证前一节点,再签名后再向后一级传递.

7) 最后一个中介 OIM_N 将信息传递到 TPP. TPP 验证 OIM_N,存储 *Evid*(*PX*)作为交易的证据,以备后用.当 *Y*=TPP,则 TPP 用私钥解密 *PPO*′,转入支付程序并保存 *PPO*′,验证 *BID*,否则下一步.

8) TPP 对$[PPO']_{KY}$盲签名送 PDS,同时加编支付指令序号 PN,以备信息反馈.

9) PDS 验证 TPP,打开 *PPO*,验证 *PPO* 中的 *BID* 是否与传送来的 *BID* 相同(不同则中止支付);根据 *NO* 进行重放检验;需要时(大额交易或特别交易)将商户信息送 CAP 审核;将 *PPO* 转换为正式支付指令 PPI(即将 *PPO* 中的手机号、银行编号与商户名翻译成真正的银行帐号.或者仅将商户名翻译成真正的银行帐号而将客户手机号直接送相应的银行,由各银行自己根据手机号找到绑定的帐号);将 *BID*(在付款行提示用户 *A* 授权时用)与 PPI,PN 送 CBP;*PPO*′备份留存 PDS.

10) ……

从第 10)步开始是 CBP 及银行之间的支付处理过程(即支付指令的执行阶段,充分利用原来

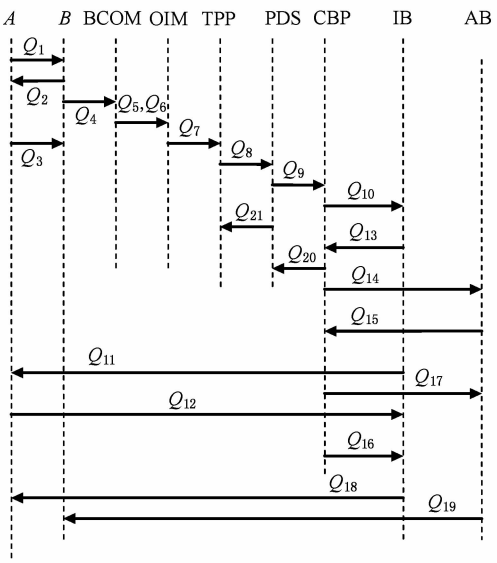


Fig. 7 Information flow of protocol.

图 7 协议信息流图

CNAPS 中的功能,如图 7 中的 Q_{10},$Q_{13}\sim Q_{17}$ 所示)以及银行与客户、商户之间的交互过程(Q_{11},Q_{12},$Q_{18}\sim Q_{21}$).其中两点很重要:

一是付款行 IB 在执行付款指令前必须向付款人 A 要求授权(要密码及支付确认, Q_{11},Q_{12});这个过程通过用户与开户机构直接的安全通道(短信或 WAP),而不是原来的支付指令传递路径.

二是支付完成后由消费者 A 的开户行 IB 向 A 及时反馈支付情况(Q_{18}、短信或票据),商户 B 的开户行 AB 向 B 及时反馈收款情况(Q_{19},短信或票据).同时由 CBP 向 PDS,再由 PDS 向 TPP 反馈支付完成情况以备后用(Q_{20},Q_{21}).

3.3 协议描述

1) $A\rightarrow B$:A 确定好购物车内容,决定支付.

2) $B\rightarrow A$: $Q_2=[Sign_B(PX),Sign_B(PPO),KB,KC,PX,PPO,KTPP]_{KA}$. /* 银行支付时 KC=KPDS,非银行支付时 KC=0 */

3) $A\rightarrow B$: $Q_3=[Sign_A(Q'_3),Q'_3]_{KB}$,其中: $Q'_3=[Evid(PX),Y,[Sign_A(PPO),Sign_B(PPO),PPO]_{KY}]_{KTPP}$. /* 当银行支付时,$Y$=PDS,当非银行支付时,$Y$=TPP */

4) $B\rightarrow$BCOM: $Q_4=[Sign_B(Q'_3),Q'_3,BID,ID_{TPP}]_{KBCOM}$;

5) BCOM$\rightarrow$OIM$_1$: $Q_5=[Sign_{BCOM}(Q'_3),Q'_3,BID,ID_{TPP}]_{KOIM_1}$;

6) OIM$_1\rightarrow$OIM$_2$: $Q_6=[Sign_{OIM_1}(Q'_3),Q'_3,BID,ID_{TPP}]_{KOIM_2}\cdots$;

7) OIM$_N\rightarrow$TPP: $Q_7=[Sign_{OIM_N}(Q'_3),Q'_3,BID]_{KTPP}.Store[Evid(PX)]_{TPP}$,/* 当 Y=TPP 时,TPP 转去执行自己的支付程序,否则继续 */

8) TPP$\rightarrow$PDS: $Q_8=[Sign_{KTPP}([PPO']_{KY}),[PPO']_{KY},BID,PN]_{KPDS},Store[PPO']_{PDS}$/* 此时 KY=KPDS */

9) PDS$\rightarrow$CBP: $Q_9=(PPI,BID,PN)$.

10) ……

协议中,PDS 与 CBP 及银行间的认证采用 CNAPS 的认证方法,不再赘述.

当交易双方有异议可向 SMP 平台申请争议解决.

在以上流程中,客户 A 的各银行付款帐户以及商户 B 的收款帐户均需预先在 PDS 或银行临柜进行认证与注册.商户获取手机号可通过 MNO 所提供的通用服务.

4 MPSTA 性能分析

本节主要从终端认证简化与安全性目标角度进行分析.

4.1 满足终端认证简化的目标

1) 终端用户只被支付机构认证一次,且认证与支付授权一次完成.终端不必验证任何主体的证书(故不必与任何 CA 打交道),也不与支付机构之外的任何其他主体认证.与其他协议相比,MPSTA 有更少的终端认证次数(见表 2).表 2 中"Certificate"指认证过程需要传递证书.一次证书验证只计一次,还没有包括证书链认证次数(而通常追溯证书链需要 2~4 次认证[16]).

Table 2 Terminal Authentication Model Comparison in Some Mobile Payment System(Single Transaction)

表 2 终端认证模式比较(部分支付协议或支付系统,单次交易)

Model	Terminal Auth Times	Terminal Authentication Object	Terminal to Be Certified Times	Terminal to Be Certified by	Authentication Methods	Cryptography Scheme	Terminal and Others Interaction Times	Authentication between Other Nodes	Application Case and Related Literature
SET	2	merchant, gateway	2	merchant, gateway	certificate, signature	PKI	4	bidirectional, cross	[14,30]
3-D Secure	2	merchant, issuer	3	merchant, issuer	signature, password	PKI	6	bidirectional, cross	[15]
SEMOPS	2	banks or MNO	2	banks or MNO	certificate, signature,PIN	PKI	5	bidirectional, merchant to customer by MNO	[1,4,11]
FINEID	2	merchant, banks	2	merchant, banks	certificate, signature,PIN	PKI	5	bidirectional	[1,16]
SET Improved	2~3	merchant, TTP,agent	2~3	merchant, TTP,agent	certificate, signature	PKI	4~6	bidirectional	[3,14,30-31]

Continued

Model	Terminal Auth Times	Terminal Authentication Object	Terminal to Be Certified Times	Terminal to Be Certified by	Authentication Methods	Cryptography Scheme	Terminal and Others Interaction Times	Authentication between Other Nodes	Application Case and Related Literature
3-D Improved	1	banks	2	merchant, banks	signature, password	PKI	3	bidirectional, unidirectional	[8-9]
SEMOPS Improved	1～2	merchant, banks	2	merchant, banks	signature	PKI	3～4	bidirectional	[13,32]
others	2-3		2～3		signature, certificate		3～8	all through gateway, bidirectional	[5-6,10,16]
Proposed Model	0	0	2	issuer merchant	SMS, password (dynamic)	ID based encryption, PKI	3	unidirectional	

2) 用短信通道认证操作简便,支付过程不必输入帐号,用户的移动支付体验得到提升.

3) 终端认证对移动设备的依赖很小,手机只需存储基于身份密码方案的私钥及开销很小的签名验证模块,无需预先存储任何支付机构的软件,使手机对支付服务的适应性增强,减少生产与设计成本.

4) "预信任"使第 1 路径上各传递主体单向认证并减少证书传递与证书链追溯,使其他主体的认证也同时得到简化.

4.2 满足安全性目标

以一个购买飞机票的案例对协议进行检验、模拟,证明协议可以实现安全性目标:

1) 保密性. 商户只能看到客户的手机号,看不到帐号,更看不到也接收不到客户密码(密码与 PI 分时分路传递);订单只有客户商户可见到,银行看不到;银行帐号只有 PA 域可见到;由于 PI 传递中采用了盲签名,各中间传递机构无论对订单还是支付指令都既看不到也不可能修改.

2) 完整性. 信息的整个传递过程采用了数字签名,而对数字签名验证本身就保证信息的完整性. 因为有"$Verify_X(Sign_X(M))$ is successful if and only if $KX[Sign_X(M)]=H(X)$",若信息传递中完整性(篡改或丢失)出了问题,签名的验证也一定不成功.

3) 可认证性. 线下信任关系与分层认证机制以及线上的逐级签名认证保证了商户、各中间服务商、TPP 与银行之间的可认证性. 对客户的认证通过手机与帐户的绑定关系以及支付时的授权(口令)认证.

4) 授权. 虽然为了简化客户操作,每次支付发起时并不要求客户注册,但每笔支付实现的最后时刻,支付机构必然通过直接安全通道要求客户授权,要求用户给出密码,保证支付安全.

5) 不可否认性. 由于 PI 产生、传递的每一步都有数字签名,所有参与主体的行为都可追溯,都能区分责任. 另外,SMP 的设置;订单证据 $Evid(PX)$ 在 TPP 的保留;支付发起证据 PPO' 及支付结果数据在支付机构的保留可保证争议发生时的可追朔性. 例如:当商户 B 否认错发了货品(质量、数量与订单不符),客户 A 可向 SMP 申请调出在 TPP 的订单证据,即

$$[[Sign_B(PX)]_{KA-1},\ PX]_{KA} \rightarrow \text{arbitrator}.$$

仲裁者在 A 的配合下解密,而后验证是否"$KA[[Sign_B(PX)]_{KA-1}]$ is equal to $[H(PX)]_{KB}$",如果是,仲裁者可以将得到的订单 PX 与 A 收到的货单进行核对,证明 A 的申述是否正确.

4.3 可较好地防范支付风险

支付指令三要素为付款人、收款人、金额[23]. 一笔支付的风险主要来自对这三要素的非正常更改,即:第 1 类:篡改付款人(转嫁应付款项,如某人盗取他人手机,想用他人帐户为自己付款);第 2 类:篡改收款人(将他人应收款项转移到自己帐户上或与自己有利益关系的帐户上);第 3 类:金额更改(为各种目的或增或减交易金额). 这些都可能出现在支付过程的任何环节,即终端、商户端与各中间传递环节,每个环节中又分主观性篡改(主体行为)及客观性篡改(黑客或故障).

MPSTA 的各种安控措施可防范各环节可能发生的这 3 种风险,如表 3 所示.

表 3 中符号表示如下:A——要求付款人口令或手写签名;B——支付指令经客户检验(在手机屏幕显示);C——商户转客户信息包时加 BID,供 TPP 或 PDS 检验收款人;D——终端、商户签名并加封的支付指令传至 TPP 或 PDS 保留;E——每步传递只在有线下信任基础的节点中进行并盲签名;F——收款帐户须在 PDS 登记,系统外帐户收不到款,系统内收款帐户行为有记录;G——每笔支付在

可信第三方 TPP 与 PDS 都有记录;H——银行或 TPP 的授权短信及短信通知、TPP 存储的订单证据.

Table 3 Risk Prevention Measures of MPSTA

表 3 MPSTA 的支付风险防范

Risk Category	Risk Point	Prevention Measures
1	terminal	A
1	merchant	B;D;A
1	other nodes	E
2	terminal	C;D;F
2	merchant	B;D;F
2	other nodes	E
3	terminal, merchant, other nodes	G;H

5 结论与展望

本文提出了一种终端认证简化的在线移动支付模式——MPSTA,通过建立基于"预信任"的分层认证模型及"公共服务域"为特征的总体架构使移动支付的终端认证得到很好简化. 在 MPSTA 中,终端只与付款帐户所在的支付机构认证(且只一次)而不必认证其他任何主体(包括商户);移动终端只需要存储并管理自己的私钥,不必存储任何支付帐号及其他敏感信息. 模式对提高移动支付市场适应性、提升用户体验及应用满意度有积极作用,对移动设备成本节省有积极作用. 同时对支付系统资源共享及统一测控也提出了新思路. 与现有的其他移动支付模式研究相比,本文的主要特点为:

1) 建立基于"预信任"的分层认证模型,并以线上线下信任相结合的认证方案解决移动支付各主体线上认证及终端认证简化问题;

2) 提出公共支付服务域 PA 的思路与方案,以解决支付安全问题,并解决支付资源共享问题以及跨银行支付问题;

3) 综合运用各种安全技术解决支付指令传递中的认证与安全问题,并使认证程序得到简化.

MPSTA 模式还存在一些局限性,如对移动终端中的签名算法及验证签名算法还未进行多种方案严谨比较以得到最佳方案,这也将是我们下一步研究的重点.

参 考 文 献

[1] Marko H, Konstantin H. Elenatrichina utilizing national public-key infrastructure in mobile payment systems [J]. Electronic Commerce Research and Applications, 2008, 7(2): 214-231

[2] Dahlberg T, Mallat N, Ondrus J, et al. Past, present and future of mobile payments research: A literature review [J]. Electronic Commerce Research and Applications, 2008, 7(2): 165-181

[3] Ou CM, Ou C R. SETNR/A: An agent-based secure payment protocol for mobile commerce [J]. International Journal of Intelligent Information and Database Systems, 2010, 4(3): 212-226

[4] Karnouskos S, Vilmos A, Hoepner P, et al. Secure mobile payment-architecture and business model of SEMOPS [C] // Evolution of Broadband Service, Satisfying User and Market Needs. European Institute for Research and Strategic summit. Berlin: Spinger, 2003: 1-8

[5] Chong C, Chua H N, Lee C S. Towards flexible mobile payment via mediator-based service model [C] // Proc of the 8th Int Conf on Electronic Commerce. New York: ACM, 2006: 295-301

[6] Kousaridas A, Parissis G, Apostolopoulos T. An open financial services architecture based on the use of intelligent mobile devices [J]. Electronic Commerce Research and Applications, 2008, 7(2): 232-246

[7] Lei Y H, Quintero A, Pierre S. Mobile services access and payment through reusable tickets [J]. Computer Communications, 2009, 32(4): 602-610

[8] Mildrey C, Jose' Mara S, Javier L. Secure multiparty payment with an intermediary entity [J]. Computers and Security, 2009, 28(5): 289-300

[9] Li Xi, Hu Hanping. A security method for mobile payment [J]. Application Research of Computer, 2008, 25(5): 1546-1549 (in Chinese)
(李曦, 胡汉平. 一种安全的移动支付方法[J]. 计算机应用研究, 2008, 25(5): 1546-1549)

[10] Kungpisdan S. Accountability in centralized payment environments [C] // Proc of the 9th Int Symp on Communications and Information Technology. Piscataway, NJ: IEEE, 2009: 1022-1027

[11] Karnouskos S, Hondroudaki A, Vilmos A, et al. Security, trust and privacy in the secure mobile payment service [C] // Proc of the 3rd Int Conf on Mobile Business. Los Alamitos, CA: IEEE Computer Society, 2004: 12-13

[12] Mohammadi S, Hediye J. A study of major mobile payment systems' functionality in Europe [C] // Proc of the 11th Int Conf on Computer and Information Technology. Piscataway, NJ: IEEE, 2008: 605-610

[13] Deepti K, Timothy A G, Ashok J, et al. Mobile payment architectures for India [C] //Proc of National Conf on Communications. Piscataway, NJ: IEEE, 2010: 1-5

[14] Shedid S M, El-Hennawy M, Kouta M. Modified SET protocol for mobile payment: An empirical analysis [J]. International Journal of Computer Science and Network Security, 2010, 10(7): 289-295

[15] Visa Public. Verified by visa acquirer and merchant implementation guide [R/OL]. 2011. [2012-06-19]. http://usa.visa.com

[16] Martinez-Pelaez R, Rico-Novella F J, Satizabal C. Study of mobile payment protocols and its performance evaluation on mobile devices [J]. International Journal of Information Technology and Management, 2010, 9(3): 337-356

[17] Sun J Y, Zhang C, Zhang Y C, et al. SAT: A security architecture achieving anonymity and traceability in wireless mesh networks [J]. IEEE Trans on Dependable and Secure Computing, 2011, 8(2): 295-307

[18] Fan C I, Liang Y K. Anonymous fair transaction protocols based on electronic cash [J]. International Journal of Electronic Commerce, 2008, 13(1): 131-151

[19] Gan Zaobin, Xiao Shicheng, Li Kai, et al. Secure E-commerce payment protocol based on four parties [J]. Computer Science, 2011, 38(10): 39-44 (in Chinese)
(甘早斌, 肖仕成, 李开. 基于四方的安全电子商务支付协议研究[J]. 计算机科学, 2011, 38(10): 39-44)

[20] Jean C L. An atomicity-generating protocol for anonymous currencies [J]. IEEE Trans on Software Engineering, 2001, 27(3): 272-278

[21] People's Bank of China. Department of Payment &-settlement China Payment System Development Report [M]. Beijing: China Finance Publishing House, 2007 (in Chinese)
(中国人民银行支付结算司. 中国支付系统发展报告[M]. 北京: 中国金融出版社, 2007)

[22] Lu Xiaobing, Pan Xinping. What is an opportunity for the third party payment [J]. Financial Computerizing, 2008 (9): 34-37 (in Chinese)
(卢晓冰, 潘辛平. 第三方支付发展的新契机[J]. 金融电子化, 2008 (9): 34-37)

[23] Su Ning, et al. Payment System Comparison Research [M]. Beijing: China Finance Publishing House, 2005 (in Chinese)
(苏宁. 支付系统比较研究[M]. 北京: 中国金融出版社, 2005)

[24] Overby E. Process virtualization theory and the impact of information technology [J]. Organization Science, 2008, 19 (2): 277-291

[25] Zhang Jiao, Zhang Yujun, Zhang Hanwen, et al. A fast inter-domain authentication method combining trust mechanism in mobile IPv6 networks [J]. Journal of Computer Research and Development, 2008, 45(6): 951-959 (in Chinese)
(张娇,张玉军,张瀚文, 等. 结合信任机制的移动 IPv6 网络快速跨域认证方法[J]. 计算机研究与发展, 2008, 45(6): 951-959)

[26] Changsu K, Wang T, Namchul S. An empirical study of customers' perceptions of security and trust in e-payment systems [J]. Electronic Commerce Research and Applications, 2010, 9(1): 84-95

[27] Brainrd J, Juels A, Rivest R, et al. Fourth factor authentication: somebody you know [C] //Proc of Conf on Computer and Communications Security. New York: ACM, 2006: 168-178

[28] Aloul F, Zahidi S, El-Hajj W. Two factor authentication using mobile phones [C] //Proc of IEEE/ACS Int Conf on Computer Systems and Applications. Piscataway, NJ: IEEE, 2009: 641-644

[29] Yang Guomin, Wong Duncan S, Wang Huaxiong, et al. Two-factor mutual authentication based on smart cards and passwords [J]. Journal of Computer and System Sciences, 2008, 74(7): 1160-1172

[30] Huang Shaoyin, Chen Yong, Gao Chuanshan. SETBOC—A new secure electronic transaction protocol based on one-way certification technique [J]. Journal of China Institute of Communications, 2003, 24(12): 170-176 (in Chinese)
(黄少寅, 陈勇, 高传善. SETBOC———一种新型的基于单向身份认证的安全电子交易协议[J]. 通信学报, 2003, 24 (12): 170-176)

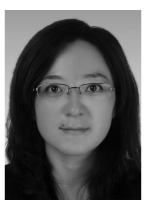
[31] Ren Lili, Wang Chengjun, Fang Yuankang. On applying set protocol in network payment [J]. Computer Applications and Software, 2010, 27(10): 105-107 (in Chinese)
(任莉莉, 王成军, 方元康. SET 协议在网上支付中的应用研究[J]. 计算机应用与软件, 2010, 27(10): 105-107)

[32] Liu Jun, Liao Jianxin. A new universal model for mobile payment system and its protocol [J]. Chinese High Technology Letters, 2006, 16(6): 560-565 (in Chinese)
(刘军, 廖建新. 一种通用移动支付模型及其协议的研究[J]. 高技术通讯, 2006, 16(6): 560-565)

Wang Hongxin, born in 1954. PhD candidate. Senior engineer. Her main research interests include mobile payment and information safety (wanghongx@263.net).

Yang Deli, born in 1939. Professor and PhD supervisor. His main research interests include system engineering, business intelligence, and mobile business (somdyang@dlut.edu.cn).

Jiang Nan, born in 1964. PhD and professor. Her main research interests include information safety (983116087@qq.com).



Ma Hui, born in 1983. PhD. Her main research interests include e-business and business intelligence (rccmm@dlut.edu.cn).